ABSTRACT

SOME IMPROVEMENTS TO SOCIAL AUTHENTICATION AND BOT DETECTION SCHEMES AND THEIR APPLICATIONS IN IOT

by Jacob J. Krzciok

The field of security is constantly evolving. One area of focus that has seen very little industry change in recent years is the area of fallback authentication. Industry standards continue to use insecure methods such as security questions and out-of-band services. Social authentication is a new type of fallback authentication which could improve security in many systems. In this thesis we first review various methods of trustee-based social authentication (TBSA) and analyze them for security flaws. We then propose two different methods, knowledge verified and CAPTCHA-aided TBSA, to help solve the issues tied to recently proposed TBSA methods. Furthermore, we combine these two methods to propose a novel scheme called knowledge verified CAPTCHA-aided TBSA. Lastly, we describe the benefits and the applications of applying these methods in the field of Internet of Things (IoT). The implementation of knowledge verified TBSA, CAPTCHA, and video notarization backed by deepfake detection provide a robust and secure method of authentication that rivals any method of fallback authentication currently implemented in IoT and the rest of the industry.

SOME IMPROVEMENTS TO SOCIAL AUTHENTICATION AND BOT DETECTION SCHEMES AND THEIR APPLICATIONS IN IOT

A Thesis

Submitted to the
Faculty of Miami University
in partial fulfillment of
the requirements for the degree of
Master of Science
by

Jacob J. Krzciok
Miami University
Oxford, Ohio

2023

Advisor: Khodakhast Bibak
Reader: Suman Bhunia
Reader: Vaskar Raychoudhury

This Thesis titled

SOME IMPROVEMENTS TO SOCIAL AUTHENTICATION AND BOT DETECTION SCHEMES AND THEIR APPLICATIONS IN IOT

by

Jacob J. Krzciok

has been approved for publication by

The College of Engineering and Computing

and

The Department of Computer Science & Software Engineering

Khodakhast Bibak

Suman Bhunia

Vaskar Raychoudhury

Table of Contents

List of Tables

List of Figures

Dedication

I would like to dedicate this thesis to both of my parents Bret and Deborah Krzciok. Without their support I never would have achieved what I have so far or what I hope to achieve. Both of them have been great role models of hard work and dedication. I would also like to dedicate this to my brother and sister, Joseph and Emily Krzciok who have always been great motivators for me in my pursuit of higher education. Thank you all for being my biggest supporters and helping to make me who I am today.

Acknowledgments

I would like to thank my advisor Dr. Khodakhast Bibak for helping me to pursue my interests in the field of security. I could not have completed my thesis without the countless hours of meetings we have had to teach me about research. He has pushed me to improve my writing and understanding of all things in academia. Additionally, I would like to thank Dr. Suman Bhunia and Dr. Vaskar Raychoudhury for being members of my committee and providing me with the suggestions I needed to complete my thesis.

Throughout my time at Miami many people have inspired, helped, and motivated me in many ways. I would like to especially thank Jack Beerman, Kareem Ghumrawi, Brian Bergem, Tim Finucan, Eddie Michael, Ben Chatwin, Ryan Sego, Sam Curran, Cole Grosshans, Rebecca Prangley, Bryanna Renuart, Annie Kreikemeier, and Nicolas Wamsely. You all have made my time at Miami an experience I will never forget.

Chapter 1

Introduction

The majority of websites have some form of login page to allow their users to have a more personalized experience while using resources, such as online banking, social media accounts, and online retail purposes. To make sure sensitive data is protected from malicious users, a password is required for future access into the account. This has allowed for the rapid development of personalized information and accessibility on the internet.

In today's age the average person has a large amount of passwords to keep track of in accessing a variety of different accounts. Rackspace has done research that found the average person has seventy to eighty passwords [1]. If a person's main focus is security then ideally each of their passwords should be different as well. This explains the statistic that 84% of people have forgotten a password in the past twelve months [2]. When the primary form of authentication fails people are required to use fallback authentication methods. The main types of fallback authentication are security questions and out-of-band services. Each of these come with their own set of flaws.

To combat this there has been a push towards other methods of fallback authentication. The evolution of social networks and the ability to track social networks has led to the study of social authentication as a possible method. Each of these new methods come with their own set of security flaws that need to be addressed. To improve the security of current methods of trustee-based social authentication (TBSA) the use of bot detection and knowledge-based social authentication (KBSA) are discussed. Each of them are advancing rapidly and can be applied in ways to fill holes in the security of TBSA.

Each of these tools can be implemented into many areas. One area that has come to the light in recent years is social cybersecurity. This is a form of cybersecurity focused on social behaviors of groups, as opposed to the individual [3]. There are currently not many security schemes that focus on this aspect and even less in the realm of Internet of Things (IoT). This area of security alone brings many challenges that need to be faced in order to create a truly secure environment. One of the biggest vulnerabilities to the security of a system is the people who directly interact with it [3]. A scheme that focuses on social cybersecurity provides extra protection to individuals using knowledge of how people behave and interact with security and privacy (S&P) protocols [3]. IoT is one of those areas that could greatly benefit from the introduction of social cybersecurity that implements social authentication

and bot detection.

In recent years, extensions of IoT have been of great interest to researchers [4][5][6]. An extension of IoT is formed by a set of geographically-distributed, special-purpose cyber-physical or cyber-enabled things connected using special-purpose protocols on top of internet to achieve a specific goal. To mention a few of these extensions, one may refer to Internet of Vehicles [7] and Vehicular Things [8], Internet of Medical [9] and Health-Care [10] Things, Internet of Bodies [11], Internet of Vessels [12] or Internet of Energy [13].

These extensions have been studied from different technological aspects [14][15]. Different objectives have been considered by IoT extension designers and researchers. Among these objectives, one may refer to performance [16], Quality of Service (QoS) [17], Quality of Experience (QoE) [18], timeliness [19], reliability [20], scalability [21], fault tolerance [22] and energy efficiency [23]. However, security is probably the most challenging design objective for IoT extensions [24], [25], [26], [27], [28].

Extensions of IoT are spread from the bottom of the sea [29] to space [30]. This is shown in Figure 1.1. Such a proliferation makes it pertinent to study these extensions from different perspectives. Related challenges as well as current and future trends need to be thoroughly investigated, in order to understand how new security schemes (i.e., fallback authentication) can be implemented in a secure and usable way.

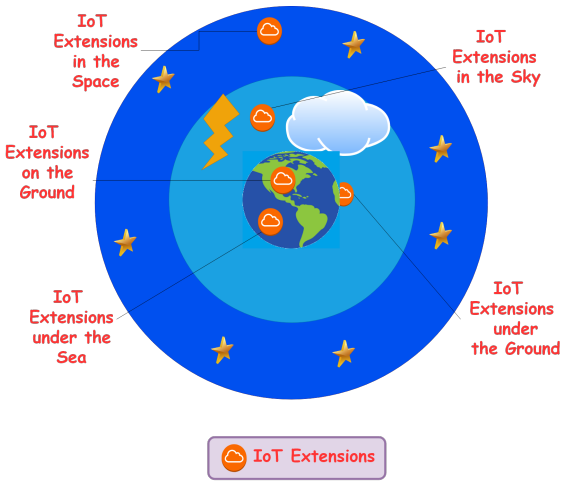

Figure 1.1: IoT Extensions Spread Everywhere.

In this thesis, Chapter 2 discusses fallback authentication, the current industry standards, and security schemes in IoT to help in developing new forms of fallback authentication. Chapter 3 provides a survey of the most up-to-date versions of TBSA, where each method is explained and then analyzed for vulnerabilities. Chapter 4 analyzes methods of KBSA and CAPTCHA as potential solutions by providing a survey of the most advanced methods, how they would interact with TBSA, and a detailed plan for implementation. In Chapter 5, we design a novel and fully functional form of TBSA that uses the proposed solutions and discusses its uses in social cybersecurity and the importance of trustee selection. Chapter 6, further analyzes the scheme design for the applications and benefits of applying it in the realm of IoT. Finally we conclude with Chapter 7 to restate our findings and future work directions.

1.1 Contributions

In this section each contribution is presented with a brief explanation of what was done to complete it. Chapters 3 through Chapters 6 each discuss a different contribution to this thesis. Large portions of this thesis are currently under review.

State-of-the-Art Methods of TBSA and Analyzing them Against Current Attacks and Vulnerabilities

This contribution, illustrated in Chapter 3, required research into literature from many top tier journals that discussed TBSA, such as ACM, Usenix, and Princeton. For each scheme a brief explanation of the scheme was given, to provide the background to each security flaw. Their similarities and differences were highlighted to show how each scheme adapted over time. Furthermore, each scheme was analyzed for security flaws, attacks, and vulnerabilities. Vulnerabilities and attacks were mentioned in other literature as well as discovered through the observation of scheme design. Each of these techniques allowed for a full analysis of each scheme and allowed for better understanding of TBSA systems and possible solutions. This is illustrated in Figure 1.2.

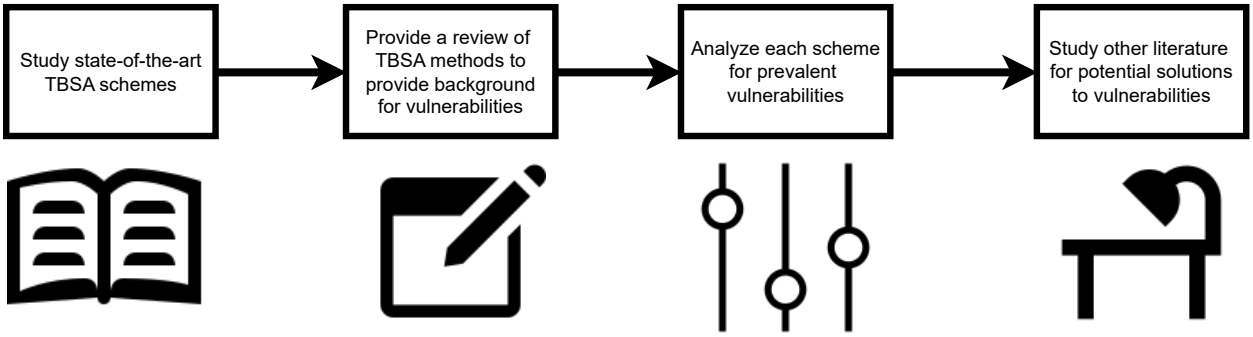

Figure 1.2: Contribution one flowchart.

Propose Knowledge verified and CAPTCHA-aided TBSA as Solutions to Security Problems with the Current TBSA Schemes and Examine them for the Best Implementation Methods

Before the start of Chapter 4, the security flaws discussed in Chapter 3 needed to be fully analyzed in order to determine methods of improvement. Through this analysis the solutions of knowledge verified and CAPTCHA-aided TBSA were discovered. A brief background of both were provided to help the reader in understanding the solutions. State-of-the-art methods of KBSA and CAPTCHA were studied to find the best schemes for implementation. After this a detailed analysis of the most secure and efficient ways to implement these methods is provided, followed by a detailed design and the improvements it provides overs the schemes discussed in Chapter 3. This is illustrated in Figure 1.3.

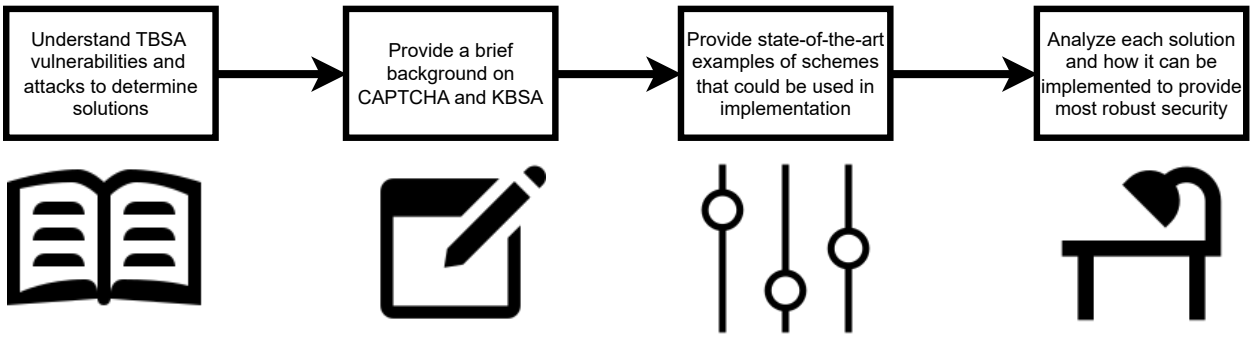

Figure 1.3: Contribution two flowchart.

A Novel TBSA Scheme in Order to Make a Secure and Usable Form of TBSA that is Fully Based on Social Relationships

This contribution, discussed in Chapter 5, started with research into TBSA and other security schemes in order to understand what goes into designing a novel security scheme. This was followed by designing the scheme based on the proposed solutions in Chapter 4. A detailed design is provided and then further studied for weaknesses that are discussed in similar schemes mentioned in Chapter 3. Once the design is finalized a discussion of Trustee selection and social cybersecurity is given to fully analyze the scheme and its applications. This is shown in Figure 1.4

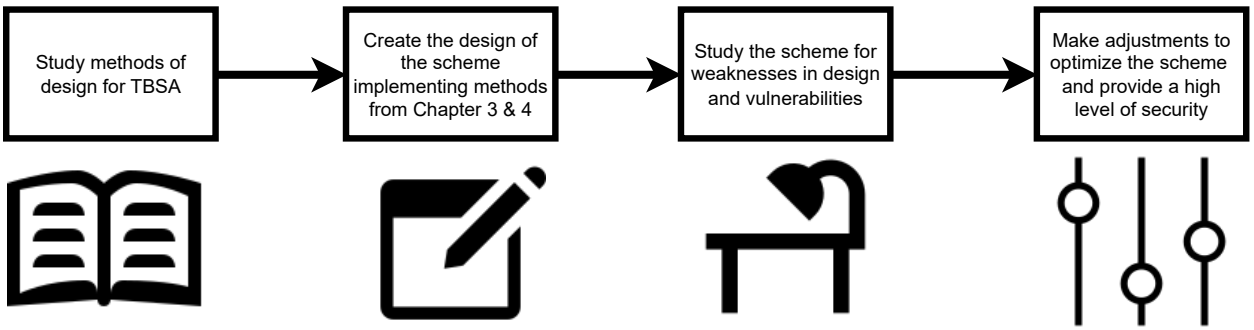

Figure 1.4: Contribution three flowchart.

Applications in IoT and More

Chapter 6 discusses the last contribution. In this chapter Knowledge verified CAPTCHA-aided TBSA is studied for its applications in IoT and other areas. Other security schemes in IoT are studied and discussed in order to show the role that our proposed scheme presents. The design is analyzed using the objectives of IoT as well as comparisons against other methods of fallback authentication. This is not only used to highlight the effectiveness of the scheme but to show case the ability of it to prevent security breaches in very sensitive areas of IoT. This is then concluded with a recap as to how Knowledge verified CAPTCHA-aided TBSA can provide huge benefits over traditional fallback authentication.

Chapter 2

Background & Related Work

2.1 Authentication

As web applications and technology have developed over the last decade, the need for authentication has grown substantially. There are many different forms of authentication that are used in a variety of different settings. For example, the authors of [31] use a multi-layer framework based on edge computing to allow for new devices to join a trusted network of devices. The scheme uses a four-way handshake based on clusters of nodes in the edge network. Another example of authentication mentioned earlier was proposed in [32] for uses in smart terminals. A user interacts directly with a terminal that monitors behavior to find irregularities in combination with the typical forms of authentication, such as a password.

The focus of this work is going to be on user interactions with devices in IoT. The most common form for user authentication relies on a password that a user is responsible for remembering. The issue is that as more applications and technologies require passwords the more likely a user is to forget a specific password. In a survey conducted by SAP inc., more than 84% of users have forgotten a password at least once during the last year [2]. This means that over the last year 84% of users have had to use a form of fallback authentication to regain access to their account.

2.2 Fallback Authentication

Fallback authentication is when a user can not complete the primary form of authentication. In most cases the primary authentication tends to be a password. Fallback authentication has been an important tool in account recovery. This allows users to still gain access to their system or account if they forget their password. The two types that are currently used in the majority of authentication schemes is security questions and out-of-band services. Both of these methods have been shown to have weaknesses that attackers may be able to take advantage of.

2.2.1 Security Questions

Security questions are when a user has a preset list of questions they need to answer to access their account. These have been studied extensively in the past. The general consensus is that security questions can be guessed correctly by someone who knows the user relatively well [33]. Some security questions have been shown to be easy to look up, such as "what is your mother's maiden name?" can be found with some simple research on social medias such as Facebook. Security questions may be an easy way to reset a user password, but studies have shown that they are also easy for attackers to guess [34]. Questions such as "what is your favorite food?" can be guessed about 20% of the time with a single guess for people in the United States [35]. Security questions for the most part are being phased out as an option all together in modern systems and are no longer approved by security professionals [33].

2.2.2 Out-of-Band Services

Out-of-band services are currently the most popular choice for fallback authentication. During the creation of an account a user predetermines a phone number or email they will have access to if they happen to forget their password. For a user to reset their password, they will receive a text message or an email with a code that allows them to reset the current password. The principles of out-of-band service relies on the idea that a user is the only one able to access the reset email or phone number and that at the time of reset they still have access to these services.

This scheme tends to fail after a long period of time as users change phone numbers or get new email addresses. A user does not always remember to change these in their account settings. Additionally, when a user gets a new email or phone number their old address and number may be recycled by the company that assigned them. This not only makes it impossible to reset their password but can also give a malicious actor access to a method of reset for another user's account password. Additionally if a malicious actor can steal a phone they have the ability to reset an account password very easily. While this is one of the more common ways for a user to authenticate themselves after primary authentication fails, their are still easy ways for the method to be taken advantage of.

2.2.3 Social Authentication

With both of the most common fallback authentication methods being less secure, there is a necessity for a new form of fallback authentication. Social authentication has become a possible direction for a more secure fallback authentication. Social authentication has been taken in many different directions [36], [37], [38], [39], [40], [41], [42], [43], [44]. The ability of social authentication to work as intended is tied to a user being able to recognize information based off of their social relations while an attacker can not [45]. This can be done in many different ways, but the two major areas are trustee-based and knowledge-based.

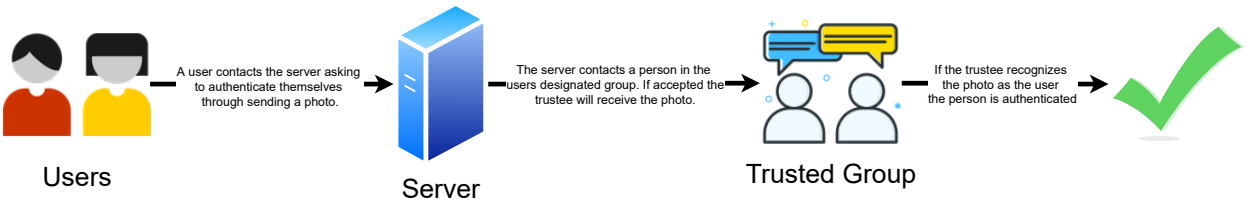

Figure 2.1: Basic explanation of social authentication.

TBSA

Vouching-based social authentication, also known as TBSA, is a form of social authentication that directly contacts people in a user's trusted network for authentication purposes. In most schemes this is used as a form of fallback authentication due to its inconvenience of contacting members of a user's network. In many cases this requires a user to obtain a vouching code from a member of a user's trusted network. One such example of this is proposed by the authors of [37]. This is a method of authentication that allows for a user to be verified by another trusted person. As shown in Fig. 2.1, a user contacts the server to authenticate themselves. The server then is able to contact members of the user's trusted group to see if they will verify a user. If the trustee accepts, the trustee will receive either a video chat to reject or accept, or a vouching code to return to the requesting user. The authors of [2] test this method using a conceptual model to test the willingness of users to participate in such a form of authentication. The study recruited 30 participants and consisted of a pre-survey, an experiment and a post-survey. The study concluded that 90% of the participants were comfortable with using TBSA. This shows that there is a willingness to use this form of authentication as a fallback method.

Aside from being used as a fallback method for authentication, TBSA has been used in conjunction with common forms of authentication, such as passwords, to form a two-factor authentication. Brainard et al. [36] propose a method that works in tandem with a PIN to reduce the ability of a system to be compromised by attackers who are able to compromise a trustee. While this limits some of the vulnerabilities there are still some that need to be addressed for this concept to be usable in the industry.

Knowledge-Based

Knowledge-based authentication is using information that is specific to a person or group to create questions to be answered for authenticating purposes. Security questions are the most common form of this authentication method. There are two promising ways that knowledge-based social authentication has been used.

The first way knowledge-based social authentication has been used is through the use of photos. Yardi et al. [41] designed a system for use with the social network Facebook called Lineup. The proposed scheme takes photos from accounts the authenticating user is friends with. It collects photos and the tags that are associated with the photos. Using the photos as prompts the authenticating user must identify the people in the photo. This works on

the ability of the user to be able to recall the people that are shown in the photos. It is not used as a primary form of authentication but as an extra barrier to login when suspicious activity is detected. This scheme has been shown to be ineffective due to the amount of facial recognition algorithms available today. Polakis et al. [46] creates an attack using publicly available knowledge to prove that the Lineup is no longer a viable option due to improved AI. The authors then offer the use of bot detection, removing suggested answers, and adding noise to photos as ways to slow down attackers attempting to take advantage of the system.

Another form of knowledge-based social authentication uses a similar model of collecting information from Facebook's network. Instead of using photos the authors of [40] use data collected on users by Facebook. The data used is called node attributes and consists of information such as employment, location and schools attended. The data of authenticating users' friends is also collected. Using these sets of data the authors were able to propose a scheme that automatically creates a set of questions based off of node data, pseudo-edge data, and edge data. Node data is information that relates directly to a person in the authenticating users network. Pseudo-edge data is information that relates to a group of friends. Finally, edge data refers to interactions between users. Through user testing the authors found that the information collected and used to form questions showed promising directions for a fully functional form of social authentication.

2.3 Bot Detection

Many social authentication and IoT schemes are vulnerable to attacks by bots that use facial recognition or deep learning to gain a broad understanding of a social network. This makes bot detection an important tool for improving the S&P in social authentication. It helps to prevent mass attacks on authentication schemes by requiring a person to perform a modified Turing test to determine an individual is not a bot. A user must perform a task of some kind that is not able to be performed by a bot. This is different than a typical Turing test due to the fact that the judge is a computer and not a person. One example of this used in our daily lives is CAPTCHA which stands for Completely Automated Public Turing test to tell Computers and Humans Apart. It was designed by L. Von Ahn [47] in 2004 and since has been implemented and improved by a variety of companies such as Google.

2.3.1 CAPTCHA

CAPTCHA was designed in 2004 using images of a combination of letters and numbers modified to be slightly harder to recognize by computer vision algorithms [47]. One important aspect of the original design is to have publicly viewable code and data as it should not be possible to design an attack whether an adversary knows the design or not. The security of the system should rely on the task being too complex for a bot to complete.

The original design has since been proven to not be secure [48]. The development of computer vision algorithms have advanced greatly since 2004. Many computer vision schemes can now accurately differentiate numbers and letters as well as a human is able to. Many

different forms of bot detection have been created to make it more difficult for AI to combat it. CAPTCHAs have been designed in a variety of ways relying on different senses. The original was designed as a visual text-based task to be answered with text but there are other examples such audio, pattern recognition, and image-based.

2.3.2 reCAPTCHA

Google has multiple versions of CAPTCHA they have created. The first version of re-CAPTCHA used books being digitized into a database to form two word pairs. The first word was a control word already recognized by the optical character recognition software while the other word was not. If the user got the control word correct then the software would compare the unrecognizable word to the most common words in the verification database. If it matched then the verification would be complete. As deep learning and AI methods improved, this form of reCAPTCHA was proven to be ineffective and discontinued.

The second version called reCAPTCHA v2 makes a user complete a challenge that a bot would not be able to do [49]. The user must click on a check box to allow google to run a risk analysis algorithm in order to determine if they were a bot or not based on a user's internet activity. If the algorithm determined a user had suspicious activity then the user must complete additional challenges such as clicking on photos of cross walks from a group. If a user passes these tasks then they are given access.

The third, and final, version called reCAPTCHA v3 works entirely in the background [49]. It monitors activity of a user on a site that has the software enabled. Then when the script is run, either when the site loads or when a button is pushed, it generates a score of the user determining whether they are a bot or not. If the score determines they are a bot then a site can run a second form of authentication to prevent a perceived bot from having access. This method and reCAPTCHA v2 are both available for sale by Google and are currently being used on millions of sites.

2.3.3 VTT CAPTCHA

Visual Turing Test (VTT) CAPTCHAs are an area of bot detection that uses the visual reasoning of an image. This form of CAPTCHA has been proposed by the authors of [48] as a promising form. VTT CAPTCHAs usually show a large group of objects at different distances, sizes, colors and orientations. A person is then given a prompt (eg. Click the object under the letter f) that they need to complete. If completed correctly the user is allowed to continue through. The authors of [48] perform tests on current VTT CAPTCHAs using an novel attack that is able to break typical questions a majority of the time. To improve the effectiveness of this CAPTCHA the authors found that their attack struggles when there are a large number of objects, an increased number of occlusions, an increased number of similar objects and the attack has the most issues if the prompt uses common sense knowledge. Common sense prompts are things that are more abstract concepts that are easily understood by humans. These types of questions accounted for 45% of the errors

in the attack proposed. This shows that VTT CAPTCHAs can be promising with some improvements.

2.3.4 aaeCAPTCHA

The authors of [50] propose a unique form of CAPTCHA called audio adversarial CAPTCHA (aaeCAPTCHA). To prevent the use of automatic speech recognition the scheme uses audio adversarial examples to perform as a CAPTCHA. A user must identify what is said to gain access. Through rigorous testing using state of the art speech recognition technology the authors show that this improved version of audio CAPTCHAs can provide adequate bot detection. The authors conducted a user study in order to prove the usability. This is one of the most advanced audio CAPTCHA techniques currently presented in research.

2.4 Social Cybersecurity

Cybersecurity is an important aspect of IoT devices and networks. Most current security schemes focus on the individual user. An individual accesses their own account using an individual based form of authentication. The issue is that many times in home, work, and other social environments, many people are accessing the same information and or need access to the same devices and accounts. This interaction with multiple users and security protocols is called social cybersecurity.

With current security mechanisms in place, people use poor practices in order to share the information they need. Users will share passwords or other forms of authentication which can negatively impact security. For example in a home environment, multiple people all share the same password and username for a Netflix account. If someone in that trusted group decides to also share that password with a significant other the network gets larger for the rest of the group, further reducing security. The issue is that there are no checks in place with most current systems to be used securely in a social aspect. This currently applies to IoT devices and networks as well. Current standards in security need to be modified in order to take into account these social interactions.

The authors of [3] take an in-depth look at social cybersecurity analyzing the social interactions of sharing information digitally, managing members of a social authenticated group, controlling online reputation, and helping others with security and privacy (S&P) problems. The authors further break down the categories of interaction such as relationships, family, social groups (work and friends) and the public. Breaking this down helps us understand the different ways people interact to better help create models to protect security and not inhibit their interaction with a system. For the purposes of IoT managing access to networks and devices is important. Many people will need to access these systems in ways that do not negatively impact the security.

Sharing digital information is important in every interaction of social groups. Many work groups must share passwords for access to different resources required for their job. For example, colleagues must access the same IoT network of devices to monitor patients'

information. To do this colleagues in many cases share passwords in unsafe ways and can disrupt logs of who accesses patient data incorrectly. This can hurt a patient's right to privacy. It is important for there to be a way for to share account access and digital information without reducing the security of the system.

We have not found any systems that effectively allow for social cybersecurity to be protected while not inhibiting a users normal behavior. To do this a scheme must be able to easily and securely authenticate a group of people for the same account, allow for effective management of members, and encourage positive S&P practices [3]. Social cybersecurity has led to an area of authentication known as social authentication which is able to authenticate people based off of social relationships and information. This can be a useful tool in designing a social cybersecurity scheme for IoT purposes.

2.5 Internet of things (IoT)

In this thesis, we first classify extensions of IoT based on the geographical locations where they are deployed, e.g. under the sea, under the ground, on the ground, in the sky or in space. We study security challenges in the design of each extension. Moreover, we discuss security mechanisms used in each extension. Lastly, we present a taxonomy on existing IoT extensions. This study is unique in its broad perspective in the sense that we cover all types of IoT extensions, all security challenges and all security mechanisms. This section and the following sections have been submitted and are under review for publication.

2.6 Existing Surveys

In this section, we briefly study existing relevant surveys in order to highlight their shortcomings, which motivate the work of this review. We classify existing surveys into the following categories.

- Surveys that focus on a single type of IoT extension, without discussing security challenges or mechanisms. These surveys are studied in Subsection 2.6.1.
- Surveys that cover a group of IoT extensions, without focusing an security-related issues. These surveys are studied in Subsection 2.6.2.
- Surveys focusing on security-related issues in IoT extensions. Although this category contains some surveys covering different security-related aspects, none of them studies all existing types of IoT extensions. Subsection 2.6.3 discusses this category of IoT extensions.
- Surveys focusing on the role of AI in IoT extensions, without investigating security considerations. None of the existing surveys falling into this category covers all kinds of IoT extensions or studies the role of AI in the future of these extensions. These surveys are reviewed in Subsection 2.6.4.

In our reviews, we did not identify any survey related to the role of AI in the security of IoT extensions. Especially, none of the existing surveys covers all types of AI models or all types of IoT extensions. Moreover, none of them anticipates the role of AI in the future of secure IoT extensions.

2.6.1 Surveys Focusing on a Single IoT Extension

This subsection reviews surveys that study a specific type of IoT extensions without a focus on security-related considerations. The extensions studied in these surveys can be classified as follows.

- **Extensions Deployed under the Ground:** Surveys on these extensions are reviewed in Subsection 2.6.1.
- **Extensions Deployed on the Ground:** Surveys related to this class are studied in subsection 2.6.1.
- **Extensions Deployed in the Sea:** We discuss surveys focusing on these extensions in Subsection 2.6.1.
- **Extensions Deployed in Space:** Surveys on this class are reviewed in subsection 2.6.1.

Extensions Deployed under the Ground

The recent literature comes with some surveys focusing on Internet of Underground Things. For example, state-of-the-art sensing and Cloud integration components used in this IoT extension were studied in [51] along with related challenges. The authors of [51] reviewed the applications of this extension as well. Moreover, in [52], the authors studied the role of Internet of Underground Things in soil fertility monitoring. They first highlighted the impact of soil fertility monitoring on qualitative and quantitative improvement in food production as the well as reduction in greenhouse gas emission. In the next step, they presented a survey on underground sensing technologies as well as communication protocols used in this type of IoT extension.

Extensions Deployed on the Ground

Several surveys have focused on different types of IoT extensions deployed on the ground, including Internet of Bodies, Internet of Audio Things, Internet of Vehicles, Internet of Autonomous Vehicles, Internet of Medical Things, Internet of Wearable Things and Internet of Bio-Nano Things. These surveys are reviewed in the following.

Internet of Bodies

The Internet of Bodies can serve to a wide range of services and applications for a broad spectrum of sectors. These services include, but are not limited to medicine, safety, security, health and entertainment. Despite this critical importance, there are only a few surveys focusing on Internet of Bodies. One such survey has been reported in [53]. In this research, the authors argued that given the recent crisis caused by COVID-19, Internet of Bodies can revolutionize public health and safety infrastructures in today's world. They reviewed the communication and networking requirements of this IoT extension along with related standards and protocols. These researchers presented a survey on channel modeling issues for various link types in Human Body Communication (HBC) channels. These channels are of critical importance due to the heterogeneous and lossy dielectric properties of the human body.

Internet of Audio Things

In this kind of IoT extension, audio things, such as acoustic sensors, are connected over an infrastructure capable of allowing local or remote, multidirectional communications. The authors of [54] presented an overview on this IoT extension. They established an ecosystem for this extension consisting of interoperable devices and services related to human-human and human-machine interactions. These researchers investigated design and implementation challenges in this field and developed directions for future research in this area.

Internet of Multimedia Things A survey related to this type of extension has been reported in [55]. The authors of [55] stated that the underlying protocol stacks in Internet of Multimedia Things need to fulfill stringent requirements in terms of quality of Service (QoS), latency, reliability, bandwidth and storage, which are raised by multimedia data. Moreover, thy highlighted interoperability as a challenging task in Internet of Multimedia Things due to the existence of heterogeneous multimedia sensors. They presented a survey on the challenges faced by seamless, interoperable communication in this type of IoT extension. The authors also studied Cloud as a promising paradigm for eliminating the storage requirements in these extensions.

Internet of Vehicles (IoV)

Internet of Vehicles is one of the best-studied extensions of IoT. There are several surveys on different aspects of IoV. For example, a review on existing methods for recommending driving strategies, appropriate routes and entertainment contents in IoV has been presented in [56]. As another example, one may refer to [57], where the authors present a survey on Business Models (BM) adapted for Fifth Generation (5G) network slicing with a focus on applications in IoV. This technology is capable of creating virtually-isolated and logically-parallel networks, enabling a large range of complex services. Another survey on the applications of 5G standards and infrastructures in Vehicle-to-Everything Communications (V2X) and IoV has been reported in [58]. The evolution of traditional V2X technologies to IoV platforms has been studied in relevant research [59].

Moreover, the authors of [60] highlighted the shortcomings of existing cellular communication technologies such as Fifth Generation (5G) and short-range wireless communication standards such as Dedicated Short-Range Communication (DSRC) in supporting the high volume of data generated by IoV sensors. They presented a survey on advances in Millimeter-wave (mmWave) technology with a focus on applications in IoV. In [61], the adoption of blockchain as a system platform for supporting the information exchange requirements of IoV has been studied. They noted that the underlying information exchange platform of IoV needs to be immutable, transparent, and secure in order to support the intended objectives of an Intelligent Transportation System (ITS). There are also other surveys briefly discussing different technological challenges of IoT [62].

Internet of Autonomous Vehicles

A survey on Internet of Autonomous (Driverless) Vehicles has been presented in [63]. This survey compares traditional client-server communication models with centralized models. The authors of this survey demonstrate how this IoT extension will move from network-centric communication models to user-centric ones in the future. They also discuss the role of Value-Added Services (VASs) in Internet of Autonomous Vehicles.

Internet of Medical Things

The authors of [64] stated that frequent topology changes due to user mobility and posture alteration increases the complexity of routing and resource allocation in Internet of Medical Things. They reviewed individual and group health monitoring architectures based on Internet of Medical Things that allow users to freely move around. They discussed the enabling technologies for each of the studied architectures. Moreover, they investigated existing solutions for route breakage in this kind of IoT extension.

Internet of Wearable Things (IoWT)

Wearable things include smart clothes, smart jewelry, smartwatches, and similar personal mobile devices. IoWT lies in the intersection of IoT and the technologies related to these devices. The battery-powered nature of these devices raises energy efficiency as a critical requirement in IoWT. A comparative, systematic literature review along with taxonomy on energy-efficient solutions proposed for IoWT-based scenarios has been presented in [65]. This survey discusses related performance parameters as well as existing solutions for improving energy efficiency in IoWT.

Internet of Nano Things

The literature comes with surveys on different aspects of Internet of Nano Things. For example, a survey presented in [66] studies this IoT extension with a focus on applications in healthcare environments. Another relevant research presents a survey on routing protocols in Internet of Nano Things [67].

Extensions Deployed in the Sea

Some extensions of IoT are deployed under the sea, e.g. Internet of Underwater Things, or on the sea, e.g. Internet of Ships (IoS). These extensions have been studied in a few surveys, which are discussed below.

Internet of Underwater Things

Internet of Underwater Things have been studied from different perspectives. For example, the survey presented in [68] discusses current advances, challenges and open issues in this IoT extension, with a focus on applications in smart oceans. Moreover, a five-layer system architecture for Internet of Underwater Things has been proposed in this survey. The proposed architecture consists of a sensing layer, communication layer, networking layer, fusion layer and application layer. Another relevant survey has studied Internet of Underwater Things from a big data analytics perspective [69].

Internet of Ships

A survey on IoS has been presented in [70] along with related architectures and elements. This survey also discusses emerging applications of IoS. Moreover, some potential future opportunities such as satellite communications as well as some potential challenges such as data collection, management and analytics have been studied in this survey.

Extensions Deployed in Space

Internet of Space Things as well as Internet of Drones fall into this category. Surveys on these extensions are discussed in the following.

Internet of Space Things

There are only a few surveys in this area. Among these surveys, one may refer to the one presented in [71]. This survey reviews existing research on connectivity and computing technologies in IoT for non-terrestrial, space environments. Moreover, it presents an overview on the area along with key challenges as well as a look-ahead of the future opportunities.

Internet of Drones (IoD)

There is a survey on applications, deployments, and integration of IoD [72]. This survey discusses some enabling technologies that support IoD in different scenarios. Optimization-based methods, Neural Networks (NNs) and blockchain are among these enabling technologies.

2.6.2 Surveys Focusing on a Group of IoT Extensions

To the best of our knowledge, the only survey covering a group of IoT extensions has been reported in [73]. In [73], the authors have tried to study the current trends and predict the future of IoT extensions. They have anticipated that a hyper space will be formed

consisting of physical space (traditional IoT), social-inspired space (Internet of People) and brain-abstracted space (Internet of Thinking). They refer to this hyperspace as Internet of X.

2.6.3 Surveys on the Security of IoT Extensions

Different security aspects of different IoT extensions have been investigated in some survey research works. Relevant surveys are discussed below.

Secure Internet of Vehicles

Different security aspects in different variants of Internet of Vehicles have been studied in existing surveys. For example, the authors of [74] have studied Social Internet of Vehicles from a location privacy perspective. A similar survey has been conducted on 6G-Enabled Internet of Vehicles [75]. As another example, in [76], the authors have studied authentication protocols in Internet of Vehicles along with related testbeds and challenges.

Secure Internet of Medical Things

There are some surveys related to secure Internet of Medical Things extensions. As an example, we can mention the one reported in [77], where the authors have highlighted the critical role of this extension, as safety-critical platforms, in the monitoring of patients suffering from chronic diseases. The authors of [77] presented a literature review on research works focusing on secure data collection, transmission, and storage in Internet of Medical Things. Furthermore, they studied some related attacks and some mitigation techniques. There is another relevant survey where risk assessment methodologies capable of being used in Internet of Medical Things have been studied and classified [78].

Secure Internet of Intelligent Things

The authors of [79] presented a tutorial on techniques for designing generalized blockchain-based schemes for authentication and key management in Internet of Intelligent Things. They discussed some prevailing consensus algorithms used for this purpose. These researchers also highlighted some related challenges as directions for future research in this area.

Secure Internet of Drones

In [80], the authors presented a taxonomy on drones used in Internet of Drones. They studied the severity of security and privacy threats associated with each type of drone. They tried to develop an architecture for secure Internet of Drones. Moreover, they established a taxonomy on attacks that hit this type of IoT extension. They reviewed existing attack mitigation techniques as well.

Secure Internet of Bio-Nano Things

The authors of [81] presented a review on bio-cyber interface technologies in Internet of Bio-Nano Things (e.g. bio-electronic devices, implantable Radio Frequency Identification(RFID) chips and electronic tattoos). They proceeded to study some security vulnerabilities of these technologies along with related mitigation strategies.

2.6.4 Surveys on the Role of AI in IoT Extensions

There are a few surveys somewhat related to the role of AI in IoT extensions. In the following, we review surveys of this type.

AI-Assisted Internet of Medical Things

The authors of [82] noted that Cloud computing, Edge computing (EC) and AI can be impactful in assisting Internet of Medical Things. They investigated how Cloud computing can facilitate the storage of data collected by medical sensors, how edge computing can support code caching in edge nodes, and how AI can assist big data analysis in this type of IoT extensions.

AI-assisted Internet of Vehicles

A survey has been presented in [83] that focuses on the role of AI in IoV environments supported by EC. In EC-enabled IoV, AI tools can help dynamic, real-time decision making in Road-Side Units (RSUs), which play the role of edge nodes. AI-based methods can improve learning capacity and assist dynamic resource allocation in edge nodes. The authors of [83] reviewed common IoV edge service frameworks in order to explore the applications of AI in service offloading and edge server placement.

2.6.5 Summary

Table 2.1 summarizes existing relevant surveys in order to make it easy to compare them with our work in this thesis.

In Table 2.1, the first entry in each row cites one of the surveys studied above. The second column contains a "Yes" if the survey covers all kinds of IoT extensions. It contains a "No" otherwise. The third column indicates whether or not the survey studies all security challenges and mechanisms. The fourth column contains a "Yes" only for surveys that provide a taxonomy. In the fifth column, a "Yes" indicates a survey that presents a future roadmap. Lastly, the sixth column indicates whether or not the survey cited in the first column discusses the role of AI in the future of secure IoT extensions.

Table 2.1: Summary of Existing Surveys

Survey	**Year**	**All Ext.**	**All Sec.**	**Tax.**	**Roadmap**	**AI**
[51]	2020	No	No	No	No	No
[52]	2022	No	No	Yes	No	No
[53]	2022	No	No	No	Yes	No
[54]	2020	No	No	No	Yes	No
[55]	2020	No	No	No	Yes	No
[56]	2020	No	No	No	No	No
[57]	2021	No	No	No	Yes	No
[58]	2020	No	No	No	Yes	No
[59]	2020	No	No	No	No	No
[60]	2020	No	No	No	Yes	No
[61]	2021	No	No	No	Yes	No
[62]	2021	No	No	No	Yes	No
[63]	2020	No	No	No	Yes	No
[64]	2020	No	No	No	Yes	No
[65]	2020	No	No	No	Yes	No
[66]	2020	No	No	Yes	No	No
[67]	2020	No	No	No	No	No
[68]	2020	No	No	No	Yes	No
[69]	2021	No	No	No	No	No
[70]	2020	No	No	No	Yes	No
[71]	2021	No	No	NO	Yes	No
[72]	2021	No	No	No	Yes	No
[73]	2021	Yes	No	No	Yes	No
[74]	2020	No	No	No	Yes	No
[75]	2022	No	No	No	No	No
[76]	2020	No	No	No	Yes	No
[77]	2021	No	No	No	No	No
[78]	2021	No	No	No	No	No
[79]	2020	No	No	No	Yes	No
[80]	2021	No	Yes	No	Yes	No
[81]	2021	No	Yes	No	No	No
[82]	2020	No	No	No	Yes	No
[83]	2022	No	No	No	Yes	No

2.6.6 Motivations

As seen in Table 2.1, although the literature comes with some surveys somewhat relevant to this study, there is no survey with all of the following properties.

- Presenting a taxonomy on all existing kinds of IoT extensions.
- Studying all security challenges and mechanisms for all kinds of IoT extensions.
- Presenting a future roadmap for secure IoT extensions in consideration of AI's role.

This study is an attempt to address the above gap. The most relevant survey is the one reported in [73], where the authors have covered a group of IoT extensions and tried to anticipate what the future may hold for these technologies. However, this work is different from our work in the following ways.

- It does not provide any taxonomy on existing IoT extensions.
- It does not focus on security-related challenges and mechanisms.
- It does not discuss the role of AI in future developments of IoT extensions.

2.7 Security Challenges and Mechanisms in IoT

2.7.1 IoT Under the Ground

Internet of Underground Things

Internet of underground things has been used in a variety of applications including, but not limited to precision agriculture, pipeline monitoring, border control, oil and gas reservoir exploration, and monitoring of oil wells or soil fertility [51][52][84]. In our reviews, we have not found any research work focusing on the security of Internet of Underground Things.

Internet of Mine Things Things

Internet of Mine Things is used in applications such as mine water control. There is a close relationship between Internet of Underground Things and Internet of Mine Things, in a way that they have been studied alongside each other in some recent works [85]. To the best of our knowledge, there is no research report focusing on the security of this IoT extension.

2.7.2 IoT on the Ground

Extensions with Applications in Medicine

Internet of Medical Things

The recent advancements in mini-hardware manufacturing, microcomputing, and Machine-to-Machine (M2M) communications have made it possible for IoT platforms to reshape many existing networking applications. Healthcare systems are among these applications. Their evolution under the impact of IoT has led to an IoT extension referred to as the Internet of Medical Things.

The application areas of the internet of medical things (IoMT) vary from heart [86][87][88][89] and skin [90] disease detection, as well as C-reactive protein and serum Amyloid detection to healthcare monitoring [91], emotion recognition [92][93], tumor prediction [94], Colonoscopy [95], remote patient diagnosis [96] and surgery [97].

As suggested in recent research, the most important security challenges and mechanisms of this extension can be listed below.

- Security Challenges
  - Privacy

    The authors of [98] suggest the use of a blockchain-based record to have decentralized electronic health records. They propose that the blockchain model be used in part with smart-contract based service automation. Some of the major drawbacks of such a system include high latency, large storage costs, and single-point failure. The proposed solution is the use of a Distributed Data Storage System. Device authentication is handled by a decentralized selective ring based access control. The anonymity of the patient information is protected through the use of different patient anonymity algorithms.

    Similarly, the authors of [99] uses the blockchain based model. The proposed system uses a triple subject purpose based access control model. The model would work in part with a transactional blockchain network to also allow for a more decentralized approach. The access to the system will be limited to users with certain privileges following a Local Differential Privacy based policy. This will prevent malicious users from having access to the entire system. The proposed blockchain-enabled method has been tested in a live setting with more than 100,000 patient records and has shown great improvements over current systems.

    To compare the decentralized blockchain methods proposed above, [100] uses two non-colluding severs and a privacy-preserving cloud-aided diagnosis scheme to create a secure way to outsource diagnoses. This diagnosis scheme uses a combination of AES and homomorphic encryption to make user requests more efficient. The analysis of this work illustrates that the proposed scheme is better than prior works when looking at the system in terms of security and usability. The authors of [101] goes further and talks about how most new solutions focus on data encryption, increasing the cost of sending and computing information to patients

and users. The scheme these authors propose focuses on three main points, a guarantee of privacy, efficient integrity verification to prevent incorrect query and computation, and lastly lightweight operations of the patient and the user. This aims to take full advantage of cloud-aided systems while limiting resource costs.

Another area that has gained a lot of attention is the future of 5G networks. [102] suggests a method of device-to-device communication for medical services that uses future 5G networks. The method is the use of an intelligent trust cloud management system. The authors propose an update to the current system to make it more adaptive and intelligent in a wireless medium. Tests done by the authors demonstrate that the updates will address trust uncertainty and improve detection accuracy of malicious devices.

The following research [103] was inspired by the current pandemic and proposes a new privacy-enhanced data fusion strategy. The design of the system is proven to successfully demonstrate an improvement in the protection of data fusion during the outbreak of Covid-19. The authors take into account task-completion, classification accuracy, reliability and a low rate of errors based on its use in IoMT. They are able to do this through the use of a validation method based on deterministic policy gradient which keeps the accuracy of the data intact. The authors believe that most current systems lack the ability to accurately and efficiently validate the large amounts of data caused by the pandemic.

– Trust

Trust is an important factor towards successful communication, especially in the realm of IoMT. The authors of [104] discuss the reasons that trust struggles in current systems. The main attack focused on in this work is the Sybil attack. The attack creates a fake node in an attempt to infiltrate the system. The proposed solution to the detection of malicious activity is the use of trust management. It allows a system to authenticate their neighboring nodes while neglecting the malicious nodes. The proposed version of trust management focuses on the use of fuzzy logic processing and the fuzzy filter.

Most of the sensors in medical devices have a limited amount of resources to implement many proposed protocols to safely authenticate each other. The authors of [105] propose a group key agreement (GKA) protocol to allow for a reduction in computational cost and an increase in the possibility of more dynamic connections between groups of sensors. The GKA would be performed using a physical unclonable function (PUF) to create unique fingerprints. The method focuses on higher security and efficiency.

– Attack Resilience

As more information and systems are developed in the IoT there is a growing number of ways for systems to be attacked. A common goal of these attacks is intrusion into a system or attempts to breach data. Authors of [106] proposes a method of intrusion detection through the use of a deep learning-based method

called the Deep Belief Network algorithm. When tested, the system received a 95% success rating in most classes of attacks.

Another common attack on these systems are man-in-the-middle-attacks (MITM). These attacks are especially dangerous because they often do not raise alarms. The authors of [107] propose a framework that is capable of sending a smaller digital signature by creating a key based on the strength of the received signal. When tested, the false alarm rate was low, while its ability to detect MITM attacks was high.

- Security Mechanisms

  - Authentication

    As the automation of remote health care continues to grow, the need for authentication continues to grow with it. The focus on a trustworthy, efficient, and resourceful system is important to the growth of the industry. The authors of [108] suggest an improvement to use of a mutual authentication protocol for a Telecare Medical Information System (TMIS) proposed by Chiou et al. [109] in 2016. The authors discuss the short comings of the current system and suggest the use of smart service authentication. The method better protects patient anonymity and stolen smart device attacks through the use of three stages: initialization by a security-authority center, registration by a medical censor, and authentication by a smart device. Smart device authentication makes use of a common key to allow for mutual authentication. When the researchers of [108] tested the method it showed significant improvements to the Chiou et al. [109] method.

    As discussed previously mutual key authentication can be a strong tool. One such method of doing so is mutual authentication and key agreement (MAAKA). This is a method of authentication that has been proposed frequently but tends to fall short in the case of being provably secure and lightweight (PSL) solutions. This tends to be a problem as most of the systems are complex and have a wide variety of requirements. The authors of [110] propose a new solution to create a PSL-MAAKA protocol. The protocol is kept lightweight by using hashing algorithms and XOR operations for authentication. Security is ensured by using a random oracle model. Through security analysis testing, a long list of properties proposed by the authors of [110], the research proves that the PSL-MAAKA protocol out performs other schemes including, Ali et al.'s [111], Fotouhi et al.'s [112], Chang et al.'s [113] and Kumari et al.'s [114].

    The authors of [115] propose another method of mutual authentication that ensures that both the source and destination are checked for integrity to prevent packet loss. The main focus of the authors is to defend against the black hole attack, a commonly forgotten attack. It is an attack in which a router deletes all messages it was supposed to forward. The proposed scheme is the combined use of medium access control and enhanced on demand vector enabled routing.

Mobile devices must start a session with a registered device in order to begin communication. The encryption method used, is the well known elliptical-curve Diffie-Hellman method. Through simulation testing they were able to prove the effectiveness of the scheme against multiple attacks with a high rate of success.

Mutual key authentication allows users to ensure that the data they collect are the same information that is sent. There are other methods that allow for the same authentication through a form of digital signature. The authors of [116] propose a method composed of four main parts: check sum computation, novel left data mapping (LDM), pixel repetition method (PRM), and RC4 encryption. PRM is used to upscale an input image. RC4 is then used to encrypt the binary secret data that is then grouped together in 3-bit groups that are then converted to decimal. Using LDM, the decimal digits are encoded and inserted into a cover image. To protect against taper, a check sum digit is created and inserted into a main diagonal pixel. If the image is tampered with the check sum digit will not match when calculated again. This is a form of digital signature to check authenticity of the data received. The experimental results collected by the authors of [116] show that the proposed system outperforms some of the best systems when focusing on computational complexity, the ability to detect tapering, payload, and imperceptibility.

– Encryption

Encryption is very important in a secure transport of information from IoMT to another location. One such method proposed by the authors of [117] suggests the use of the Rivest Cipher to generate a key value followed by the use of the Elliptic Curve Digital Signature Algorithm (ECDSA) to encrypt the value. Lastly, the value is hashed using SHA256. The proposed scheme is tested by the authors and proven to be sufficient against attacks.

With IoMT a lot of authors have looked for easy ways to transmit data from IoMT to servers. This leads us to the use of smartphones in today's society. They allow for easy transportation of data between users and healthcare professionals. The issue comes with communicating that sensitive data in a way that does not allow attackers to take advantage of the system of communication. The authors of [118] have proposed a method using blockchain and key authentication agreements. The protocol would provide a secure place for keys to be managed on the blockchain. This would allow for the secure transfer of keys between implanted devices, personal servers, and cloud servers. The data would then be accessible to appropriate users via the blockchain. The Automated Validation of Internet Security Protocols and Applications (AVISPA) tool was used to perform tests on the proposed system and proved to be resilient against attacks.

Since the beginning of Covid-19, many physicians have moved to remote care for their patients, also known as telemonitoring. When doing so, doctors must transmit an extensive amount of patients' personal data. To keep the information safe, the authors of [119] have proposed a lightweight method of mutual authentication

and secret key establishment protocol. The secret key agreement uses PUFs to allow devices to check the authenticity of a sensor node as well as a doctor's legitimacy before relaying information. The scheme has been robustly tested with the use of AVISPA tools and has performed well, preventing attacks such as MITM and using less of a systems than similar schemes.

Also influenced by the pandemic, the authors of [120] propose a time-bound group key authentication using extended chaotic maps. These time-bound group keys allow for groups of devices to authenticate each other for a short period of time. This function is low-cost as the device does not need to retrieve a key every time it connects to the application layer, rather than encrypting and decrypting every time like other methods. The chaotic maps' unpredictable nature makes them useful in the authentication and key-agreement process of the scheme.

For IoMT, it is important to protect the integrity and confidentiality of the data. The authors of [121], inspired by the pandemic, propose an Attribute-Based Encryption (ABE) method for providing user privacy and confidentiality. This method is a partially-policy-hidden and large universe ABE model that is publicly traceable. An area of focus for the authors is that the amount of data is independent of the publicly available information; this allows for any amount of electronic health records (EHR) to be stored. In addition, any person who is in possession of the encryption key is able to easily track the data linked to it. The final area of focus of the system is that it will have fewer bilinear pairings, allowing for smaller costs during decryption.

A big concern with most encryption is the cost of encryption and decryption. Using traditional encryption, there is a large cost of computation making it an unfeasible way for patients' data to be transferred in real time. The authors of [122] propose a light weight and efficient encryption algorithm that could be used efficiently in the transferring of image data. The method uses two permutation methods to secure the image. This new encryption method takes into account 256 bits to be encrypted and then breaks them into 16 different blocks of 16 bits. They have tested the algorithm on multiple test images and, when compared to the current standard, have proved to be much more efficient when considering execution time when compared to other similar forms of encryption.

– Signcryption

Encryption and electronic signatures are significant parts of the transfer of data securely. Signcryption is a system design that achieves privacy and authenticity without increasing the cost of computation by combining the digital signature and encryption algorithm. Other higher-cost models separate encryption from signing, creating a less cost-effective option. The authors of [123] propose the use of signcryption in conjunction with a publicly verifiable cloud-centric health care system. This system collects data from IoMT and outsources the data to the cloud server through the patient's smart phone. When tested by the authors, the scheme had less energy consumption compared to other related schemes.

- Intrusion Detection

  As stated above, IoMT is rapidly expanding. IoMT is opening more avenues for attacks. Without an effective intrusion detection system an attacker could steal sensitive data or severely affect patients health. The authors of [124] propose a novel mobile agent based intrusion detection system. The agents will employ machine learning algorithms in order to look for the signs of a breach. The agents are composed of a sensor agent, a cluster head agent, and a detective agent. Through the use of data collection and principle component analysis, the agents work together to find abnormalities in a network. By emulating different use case scenarios the authors were able to obtain promising results when considering accuracy.

- Security Evaluation

  Along with intrusion detection there is a strong need for security evaluations in IoMT. An insecure medical device could cause massive amounts of health complications to large groups of people in a very short period of time. The authors of [125] propose a hierarchical model consisting of three steps. The first step is to use a fault tree (FT) on the infrastructure of the IoMT that consist cloud/fog/edge member systems. The second step is to go through the subbranches of the same member systems. The last step is to use FT on the continuous-time Markov chain of devices in the subsystems. The proposed model takes into account a variety of different failure points, including attacks on the system. The proposed evaluation method has the opportunity to greatly improve the security of current and future IoMT in the realm of cloud/fog/edge member systems.

In addition to security, some recent research works focusing on internet of medical things have worked on improving other design objectives such as performance [126].

Internet of Health Things

In the following, we discuss the security challenges and mechanisms of internet of health things (IoHT).

- Security Mechanisms

  - Encryption

    The authors of [127], propose a symmetric key encryption to be used in IoHT. The method has a lower computational and communication cost than its asymmetric counterpart. The authors solve this issue through the use of a low memory symmetric key generation model that mimics group secret key agreements. The authors of [128] break down flaws in a current encryption technique based on chaotic maps, a conditional shift algorithm, and a modified Mandelbrot set[129]. When simulating an attack the authors only needed one plaintext-ciphertext pair. Using this information the authors performed a chosen-plaintext attack (CPA)

and were able to crack the scheme with little computational time. To improve the system, the authors of [128] suggest using confusion and diffusion based on Shannon's Theory [130]. Using the chaotic system, a substitution box can be created to satisfy the properties of confusion. To implement diffusion, a key from the Mandelbrot set can have XOR applied to the chaotic sequences and the image layer. The conditional shift algorithm should not use XOR on the key and original image. Using these improvements the authors agree that the initially proposed scheme can be implemented and used securely.

Radio-frequency identification (RFID) is a resource constrained device that has had improvements in protection recently. Many access control systems use this type of device for high level security purposes. Such a device requires a lightweight cryptographic algorithm. The authors of [131] propose an algorithm called SLIM, which is a 32-bit block cipher based on the structure of the Feistel network. Since it is a block cipher, it uses the same key for encryption and decryption allowing for it to be more lightweight. SLIM has demonstrated a strong ability to prevent attacks on RFIDs.

Another scheme to achieve security in IoHT is ciphertext-policy weighted attribute-based encryption (CP-WABE). But this system has several issues including being non-scalable, high computational cost and time, and high memory. The authors of [132] propose some changes that, through theoretical and experimental analysis, have proven to be more efficient than CP-WABE. To resolve these issues the authors use 0-1 encoding [133]. To make sure the scheme can run on a more inefficient system, offline/online encryption and outsourced decryption are used. Through experimental testing, the authors prove the scheme is more efficient than existing schemes.

– Signcryption

One of the greatest concerns for security in IoHT is the authenticity of a patients' health records sent over the internet. Along with this is the anonymity of the sender and receiver of the data needing to be preserved. The current methods of signcryption that use certificateless cryptography do not allow for security anonymity and the anonymity of the receiver at the same time. To solve this, the authors of [134] propose a form of signcryption based Hyperelliptic Curve Cryptosystem (HCC). The use of HCC in the proposed model creates lower computational costs to the system than in current systems that use cryptographic techniques such as RSA, elliptic curve cryptography (ECC), and bilinear pairing. Using the Random Oracle Model of testing the authors were able to guarantee a high level of security when considering receiver anonymity, confidentiality, and unforgeability.

– Data Provenance

Provisions in Data Provenance are important if it is to be accepted by stakeholders. The proposed system by authors of [135], suggests the use of a lightweight federated learning and differential privacy to protect the privacy and security of

the data. The method would work in conjunction with blockchain smart contracts to manage authentication of federated nodes, trust management, and edge training. To fully support encryption of the data set, federated nodes use additive encryption while the blockchain performs multiplicative encryption. The system was tested with deep learning applications and Covid-19 patient data sets. The authors claim that these tests provide strong potential for use in IoHT.

Although security is a critical design objective in internet of health things, it is not the only one. Researchers have studied other objectives such as performance [136], timeliness [137] and reliability [138] as well.

Internet of Bodies

In an Internet of Bodies, different kinds of worn, implanted, embedded or swallowed devices located in, on or around the human body are interconnected over a network. Internet of bodies have received a research focus in recent years. In one article [11] the authors deploy a programming framework for combining information from several source devices. This allows doctors to monitor and use multiple forms of data to better schedule computer to human interactions. In [139] the authors propose an orthogonal and non-orthogonal capacitive body channel access schemes. A handful of optimization protocols are put in place to optimize the throughput of information while maintaining lower power costs. The methods used are max-min rate, QoS sufficient operational regimes, and max-sum rate. The proposed scheme is tested sufficiently and proven to not degrade performance with larger networks. In our research, we have not come across any research report related to the security of this extension.

Internet of Bio-Nano Things

Internet of bio-nano things is a recent extension of IoT [140]. It is used in molecular biology [141], disease diagnosis [142] and related areas.To the best of our knowledge, security of this extension has not been studied in any existing research report.

Extensions with Applications in Transportation

Internet of Vehicles (IoV)

IoV is a distributed network of connected cars, RSUs, and central Cloud platforms. IoV makes it possible to integrate smart vehicles with the Internet and consequently to their environments, such other vehicles, pedestrians, public infrastructures, computing nodes and sensors. IoV should definitely be considered as a significant trend in recent research on IoT. Especially, software-defined internet of vehicles has received a research focus in recent years [143], [144], [145], [146], [147], [148].

Although a wide range of objectives such as performance [149][150], mobility [151], reliability [152] and QoS [153][154] have been considered in the design of internet of vehicles, security is probably the most important one [155], [156], [8], [157].

Security challenges faced by internet of health things as well as security mechanisms used in this area are listed below.

- Security Challenges
  - Privacy

    IoV is the collection of sensors and devices located in cars that connect to each other or to a central location. The data collected by these sensors are usually consisting of location information and identity of the vehicle. The privacy of this information is paramount to the safety of the vehicle's owner. One method proposed by the authors of [158] is a Concerted Silence-based Location Privacy Preserving Scheme. The method would create an unlinkable connection between the location services of a vehicle and the safety functionality of the vehicle. The identity of the vehicle on the network must enter a silence period in which the location of the vehicle is not shared before it is able to link to the location of the car. This will allow for a bit of unpredictability in location, but not making it impossible for there to be a link between the two. In the testing, it was proven to be successful in prevention when simulated against a global passive attacker. The authors of [159] propose a different method based on double k anonymity (reduces correlation between requests and users while maintaining service quality) to help secure the link between the identity of a vehicle and its location. The method makes use of a cloud-server as a intermediate stop for data between a vehicle and a service provider. In the cloud-server requests from the vehicle are reduced through the use of a permutation and combination methods that involve the use of randomly generated matrixes. The authors tested the algorithm extensively to prove its safety and time efficiency.

    Many current systems set up for privacy in location services do not have the ability to offer real-time updates to location information, such as the methods listed above. The scheme proposed by the authors of [160], gives a solution that will allow real-time updates to these location-based services (LBS) while allowing privacy of a user's location. This is done with shadow vehicles. When a vehicle requests location services it will find two other vehicles and request their locations as well. The other cars will make similar calls. When the data are received back to the car, it discards invalid locations and uses its actual location. If an attacker is monitoring the LBS server, they will be unable to know which vehicle is the correct one. After simulation testing, the results showed that there was a high level of privacy for the proposed scheme and it allowed for real-time LBS.

    In location services of IoV, Geo-indistinguishability (Geo-Ind) is a important privacy concern. This provides location privacy, but does not work if exposed to poorly reported locations. Testing done by the authors of [161] have shown a probability of over 50% that true location is reported incorrectly. To correct Geo-Ind the authors recommend to add an additional mechanism called Perturbation-Hidden. This would allow for the pseudo-locations of the user to be guaranteed. The mechanism used to perform this task will be a differential private exponential approach. To attain 100% plausible pseudo-locations, the authors implement dynamic programming.

Privacy protection is achieved by a variety of methods. One such method is through the use of fog computing environments. The authors of [162] propose a data transmission system that takes advantage of a crowd-sensing model based on fog nodes. The location prediction is based on social infection theory. Lastly, selfishness nodes are implemented using the Robin Steiner bargaining game to carry out transmission. Through experimental testing, when paired against malicious nodes, selfish nodes have strong competitiveness in combating attacks. Another method based on the use of fog computing environments is a scheme proposed by the authors of [163]. The scheme uses crowd-based sensing architecture in conjunction with encryption and authentication methods such as hashing, partially blind signature authentication, homomorphic encryption (creates a ciphertext that can be worked with as if it were in plain text), and zero-knowledge verification. When compared to similar architecture, the method achieves a 60% increase in user feedback delay and a 44% increase in efficiency. To protect privacy, the authors of [164] use a decentralized traceable privacy preserving scheme. The proposed scheme requires the use of multiple fog servers. The servers would be responsible for tracking the ID of the vehicle as well as the projected route it is taking. The true ID of the vehicle is hidden by certificate authority and the secret sharing scheme. To find the true identity of the vehicle, a voting machine is implemented to find the most reliable fog server to use. Using real-or-random model the authors are able to prove that the scheme is able to securely transmit data.

Blockchain's involvement in IoT has been important in recent years, as more schemes are developed using its decentralized nature, fully secure, and information management abilities. The authors of [165] propose a scheme that uses blockchain in conjunction with federated learning to securely transmit learning model parameters instead of the actual data. Federated learning and blockchain when integrated together can prevent issues each of them have on their own. Federated learning on its own is susceptible to poisoning attacks and blockchain is overly robust. The combination of the two allows for the system to work effectively and securely.

As talked about earlier routing vehicles through the use of location based data has many privacy concerns. To combat these many challenges, the authors of [166] propose a Privacy-Preserving based Secured Framework for Internet of Vehicles (P2SF-IoV). The proposed method first uses blockchain technology to securely transmit the data. The blockchain then implements a deep learning algorithm known as the SLSTM technique. This is used to catch other types of attack, such as malicious nodes or intrusion. Performance of the deep learning algorithm is then evaluated using IoT-Botnet and ToN-IoT datasets to help improve accuracy. The authors compare this method to blockchain and non-blockchain methods and outperformed them overall in terms of detection rates, accuracy, and false alarm rates.

Vehicle to everything communication is the ability of a vehicle to communicate with an entire network, composed of infrastructure, other vehicles, and pedestrians. An area that is important to maintain the security of such a network is authentication. In [167] the authors propose a scheme that takes advantage of blockchain to maintain privacy while lowering communication and storage costs. The authors use a form of blockchain known as CyberChain. This is coupled with a Privacy-Preserving Parallel Pedersen Commitment (P4C) to allow for stronger privacy. To further accelerate the authentication process, the authors use Diffused Practical Byzantine Fault Tolerance. These two algorithms allow for the low latency that is required in time-sensitive IoVs. Through simulation and qualitative analysis, the authors show that the proposed scheme has lower latency, communication and storage cost, and greater privacy than other similar methods.

In recent years, edge computing has become the center of attention in IoV. It eases congestion in vehicle networks using end-to-end communication. This is done by transmitting information to end nodes instead of the server, thereby reducing latency. The authors of [168] propose a secure service offloading method (SOME), that uses edge computing but is able to tackle some of the traditional edge computing issues. The scheme uses a software defined network (SDN) to handle issues with quality of service such as resource conflicts and communication interruptions. These issues can cause degradation of other similar schemes. Issues with privacy related to SDN cause a need for modification of current SDN systems. These are handled through the use of an offloading time for drivers, creating a gap in location of the vehicle and what can be observed by a server. SOME is evaluated through experiments conducted by the authors.

Routing shipments is a challenging task that has been simplified by the emergence of IoV. Since there is so much location data available, the collection and management of it creates an easy way to route traffic. To protect this data the authors of [169] propose a Differentially Private Trajectory Database algorithm. To create this system, a data set of time points is made into a 3 dimensional trajectory set. The data set is then analyzed using a trajectory release model that uses prefix trees to determine the flow of traffic and predict the route of least resistance. The method also takes advantage of the Markov model to reduce the cost of adding noise. To reduce the cost further noise is only added to every other layer. The proposed algorithm has been shown to have better data availability with an acceptable level of privacy through experimental and theoretical analysis.

In most instances privacy of IoV focuses mainly on location information. In some taxis, facial imaging data is collected. To protect this data, a new scheme that generates and restores facial images is proposed by the authors of [170]. The method first runs numerous perturbations based on the semantics of the image. Then it is run through an adversarial network to generate a scrambled version of the original image. The key is then concealed steganographically in the image. A restorative network is able to read the key and understands how to decode the

received image. Through experimental testing the proposed scheme shows high detection resistance, better quality and more secure filtering defense.

To address the issues of MITM, impersonation, unlinkability, and traceability attacks, the authors of [171] suggest the use of a batch verification-based authentication mechanism that takes advantage of ECC techniques. This allows a vehicle to authenticate neighboring vehicles. The authors have compared this scheme to relevant schemes and have concluded that the proposed scheme offers better security and functionality than other similar methods.

– Trust

There are many issues with current systems of large network IoV communication. In [172] the authors discuss some of the challenges faced by current models and other foreseeable challenges that these networks face. The challenges are broken into four categories including privacy of information, privacy of multi-party, trust, and consent of information sharing. Privacy of information must take into account the large volume of personal information being shared in the network. To create privacy the system implemented must use minimal amounts of information as an attack could leave this information vulnerable. The concern of multi-party privacy is taken into account as third party services can be breached and expose large amounts of personal data. Trust must be managed to allow nodes to safely share data between each other. The trust management system needs to be real-time as to prevent bottle necking in many systems. Lastly, consent to share information should be given by users when using these systems. Each of these categories are vital to the creation of a more secure system but may also have some trade-offs in terms of speed and efficiency in the network. The networks proposed below each take a different stance on what is important in these systems and how it should be approached.

Trust management is a tool used in networks that prevents malicious nodes from gaining access to sensitive information. In a study done in [173], the authors propose a novel hybrid trust management scheme. The scheme uses two steps to evaluate the trust-worthiness of a node. The first step analyzes the trust of the node in the transport layer. The second step evaluates the trust of the node in the application layer. Through testing, the authors have concluded that the proposed scheme has a trust level of 75%, which is higher than the 60% baseline found in ART [174], Chen [175], and TMEC [176].

As more infrastructure and vehicles are being connected, the networks of communications are becoming more complex which makes it more difficult for messages to be reliable. The authors of [177] propose a trust management system that uses blockchain along with a reputation value scheme to gauge the probability that a message is accurate. Credibility and the ability of a vehicle to be able to influence the system is based on the reputation value. A value is decreased when the system receives false messages. The performance of the system is tested through simulations and proven to be accurate at detecting and limiting malicious vehi-

cles. Through the use of the blockchain-based method, the authors have created a secure way of storing data.

Video surveillance has been an increasing technology in IoV. The issue is that transmitting such large amounts of video data is strenuous on the resource limited systems in IoV. As a vehicle does not need to communicate directly to a server but can send video data to a much closer edge node, the use of edge computing can be used to resolve the issue. Many of these systems have trust related issues during communication that can reveal sensitive data. In [178] the authors propose a trust-aware task offloading method designed to improve edge computing methods. This method is used to balance the load on edge nodes through the use of the Strength Pareto Evolutionary Algorithm 2 (SPEA2) which minimizes response time and increase layers of privacy. In experimental testing the scheme was proven to be time efficient and has a high level of trust.

Trust management is important to the safety of people who use IoVs. One malicious user is capable of putting many lives in danger. There are many issues with current trust management systems which may cause failure in current schemes including the lack of scalability, single points of failure, reduced quality in the system, and lack of availability. These systems can also inhibit real-time accuracy. The authors of [179] propose a method of blockchain-based adaptive trust management through the use of smart contracts that is able to combat the current issues in traditional trust management systems. The blockchain is used to securely mange the trust network and an incentive algorithm is employed to convince users to perform well. The use of blockchain sharding can reduce stress on the main blockchain and increase throughput of data. The current work has been tested and proven feasible in real world applications. Another Blockchain based trust management system using smart contracts is proposed by the authors of [180]. The proposed scheme also uses physically unclonable functions (PUFs), certificates, and dynamic Proof of Work (PoW) algorithms. The blockchain is used to manage trusted vehicles. Once a vehicle has established trust PUFs assign the vehicle a unique ID. RSU establish certificates to preserve privacy of vehicles. dynamic PoW allows for the system to scale to the level of traffic which in turn takes up less resources when it is not needed. Through security and performance analysis the system is proven to be feasible in IoV and is superior when compared to similar methods of trust management.

Many location based emergency services used in location of vehicles are very large IP-Based networks. The issue with these systems is that they have high amounts of latency, problems with evenly disseminating information, and are vulnerable to attacks on the systems trust. The authors of [181] propose an emergent semantic based information-centric fog system. To help increase trust the authors implement a semantic-based trustworthy routing scheme. This scheme would allow for the system to detect fake nodes in the system. To do this the authors implement fog nodes to maintain three different data structures, a forwarding information

base, a pending interest table, and a content store. Using this information the scheme is able to analyze the traffic effectively and find fake nodes from the network. Through testing the system had a decrease in failure rate by 50% when compared to the traditional systems without fog networks or clouds.

As mentioned earlier, intelligent routing is an important system in IoV that could allow for a reduction in wasted time. That being said, with an increase in IoV there is a large influx of data that needs to be processed in real time. To help combat this the authors of [182] address issues in security, trust, and privacy as well as propose a deep learning model to process the data. To do this it is proposed to use a lightweight 1D convolutional neural network (CNN) model. Through testing it was shown to cause very little delay in real-time trust management.

Large scale networks in IoV are becoming an increasingly tough challenge for having good network performance while still managing trust in the network. In the article [183], the authors discuss a hardware trusted model to build a trust chain. This would allow for a high level of protection, a tested running environment, and trusted state attestation (ability to prove its identity). To prevent more latency created by the trust management system, it is proposed to use a remote novel batch approach. Simulation testing has proved that the trust worthiness of the network is intact while not creating an overly latent network. As discussed above larger networks create issues as each node in the network must be verified using a trust management scheme. The authors of [184] propose a scheme that takes advantage of the blockchain to limit the bottle necking that can occur in other schemes. Blockchain allows for a system to be traceable, untamperable, unforgeable, and transparent in a network of vehicles. Through the use of Dirichlet distribution, reputation regression, and revocation punishment the scheme can manage and classify the trust of vehicles in the network. This model shows a strong ability to find malicious nodes in a network when tested via simulations.

– Attack Resilience

In IoV, the ability of a vehicle to defend against an attack is paramount to the safety of the passengers. One such attack known as the Sybil Distributed Denial of Service (DDoS) Attack has shown the vulnerabilities of edge node detection in current systems. The authors of [185] propose a Real-Time Edge Detection Scheme for Sybil DDoS. The authors designed an algorithm called Fast Quartile Deviation Check (FQDC) to catch and locate an attack. This algorithm is based on entropy theory and a modified version of other deviation algorithms such as Quartile Deviation [186], [187], Generalized Extreme Studentized Deviate (GESD) [188], Linear Regression and Confidence Interval. The authors modify the algorithm to have simple calculations, quick response, and low omission rates, to make it more applicable to IoV. When tested, the system detected all Sybil DDoS Attacks with an average alarm time of under 5 seconds.

Another important area for attack resilience in a system is when considering vehicle to vehicle (V2V) communication. The authors of [189] propose a blockchain

based scheme to authenticate vehicles in real time. Since V2V communication must be in real time, the proposed scheme is free from low latency and heavy computation complexities through the use of blockchain technology. This technology creates blocks of information that are each hashed and shared with the corresponding vehicles. The hash function used in this scheme is SHA-1. Using the Pearson Correlation Coefficient the correlation of communication rate is .9749 without an adversary and is calculated as .1282 when there is an adversary. This is done while considering the Received Signal Strength Indicator. This proves the scheme is an effective method of attack resilience.

- Confidentiality

  Improvements in sensor-enabled vehicles has led to the increased need for physical layer security (PLS). With the growing density of vehicular networks, PLS will become significantly more important. The authors of [190] propose a PLS framework for a network consisting of a legitimate receiver and an eavesdropper. To capture the mobility of the communication channel, a double-Rayleigh fading channel is implemented. To measure the performance of the scheme average secrecy capacity and secrecy outage probability are presented. The two performance measures are then provided in alternative forms to be able to use them with a moment generating function. The tests show that number of vehicles with signals that interfere will affect the system and shows that there is correlation between the performance and the uncertainty of a eavesdropper's vehicle location.

- Security Mechanisms

  - Anomaly Detection

    Anomaly detection is the monitoring of data collected by a system to detect either false data or malicious activity. The use of SDN can be used to create systems that can help catch attackers that are targeting a specific node in the network. The authors of [191] propose a hybrid method that uses probabilistic data structures. The scheme is composed of four phases: i) A monitoring scheme that takes advantage of Count-Min-Sketch as the probabilistic data structure that monitors and filters incoming traffic; ii) A Bloom filter-based control scheme that is used to authenticate the nodes deemed suspicious; iii) A quotient filter that is used to store malicious nodes; iv) A hypperlog counter that measures the flow passing through switches to find malicious nodes with a high level of connection. Through experimental testing, the scheme has proven to be a strong candidate for anomaly detection when considering speed, accuracy and efficiency in detection.

    Controller area network (CAN) bus anomaly detection is a form of detection specifically for attacks on the CAN bus protocol in certain vehicles. Many of the current CAN anomaly detection systems have poor performance rates. This tends to be from the lack of abnormal IoV data. The authors of [192] propose a method for message classification in IoV that establishes a weak model to classify

redundant data. The method also allows for classification of a broad range of data. The proposed method is able to decrease computational costs as well as time, without taking away from the accuracy. The authors then propose an improved support vector domain description scheme. They add the Markov model and the Gaussian kernel function to reduce redundancies and false-negatives. Testing of the method shows an increase in accuracy when compared to other models.

– Signcryption

  As discussed earlier, edge computing is an advancing technology that has many applications in IoV. The use of edge computing with 5G networks allows for a scheme free from latency. In [193] the authors propose a multi-message and multi-receiver signcryption scheme that uses multicast channels. The issue with typical multicast channels is that they are prone to many attacks due to the fact that they are more exposed. The proposed scheme uses a certificateless setting to help with these challenges. This is because a key's security is dependent on security of a channel. The method the authors use creates a pseudo partial key to be used on a public channel. The method also uses HCC because of the smaller key size allowing the scheme to be lighter weight. Through testing, the scheme shows that it has high security with low cost of computation.

– Authentication

  Security in IoV is something that has not been studied enough in recent years. In [194], the authors propose a method of authentication through the use of a fog based identity scheme. They do this through the use of two layers. The first layer of the scheme is a security authentication scheme outside the fog. The second layer is a security monitoring layer for all of the other vehicles in the network. The authentication method used is a two-way form between the identity of the vehicle and a deep learning algorithm that conducts real-time security. Through testing, the scheme was proven to be accurate and able to adapt to the increasing number of high-speed networks in IoV.

  Ad hoc networks allow for vehicles to connect in real-time. This allows high-levels of communication but most of these communications happen on open channels. There are plenty of attacks, such as eavesdropping, that can take advantage of these channels leaving users vulnerable. To help protect the location and identity of the vehicle the authors of [195] propose a new key agreement and mutual authentication scheme using elliptic curve cryptography. Vehicles are grouped into clusters based on the location of its closest road side unit. In each cluster there is a designated cluster head. One area of authentication and session key creation is between a vehicle and its cluster head. The second area of authentication is between the vehicle and other vehicles around it. After analysis the authors found that the scheme was able to defend against many of the attacks that happen on open channels for IoV. The authors of [196] propose a similar form of mutual authentication called three-byte-based Media Access Control. The architecture of the network is split into two chains, local and public. Similar to the previous

scheme, the local chain is controlled by the cluster head in terms of authentication and communication. The public chain is controlled by the base station. To communicate the vehicles use their Media Access Control address and can alter the authentication by using the last 3 bytes of it. The constant use of those bytes allow for the network to constantly authenticate and keep a high level of integrity. The system is able to remain lightweight as most of the heavy computation is done through base stations and cluster heads. The scheme proved to be a usable method of authentication as it had very high detection rates, low computational costs, and had low latency.

There are many different authentication methods but many are not lightweight which is very important in IoV (and many other resource-constrained devices). The authors of [197] introduce a lightweight key authentication protocol that enables a server and device to share a secret key. This can be used to create a secure session between the server and the device in a way that is more lightweight. Testing shows that the proposed scheme is more efficient in computation and communication costs than current systems while still maintaining security. This is done through the use of XOR operations and SHA-3.

Quantum computing is a growing technology that raises concerns in most facets of cybersecurity. This could allow for solving some major cryptography problems in polynomial time. The authors of [198] propose a quantum defended scheme that uses a novel certificateless data authentication protocol. The scheme is protected from quantum attacks using lattice-based cryptography. The use of this in conjunction with a blockchain allows the scheme to be secure while being more energy efficient and storage efficient than other methods for lightweight use in IoV.

To maintain safety of IoV, communication is happening constantly between vehicles and the infrastructure. This makes authentication important to the integrity of the system. To create a system that is able to keep the identity and location for a vehicle separate while allowing the authentication of the vehicle, the authors of [199] propose a conditional anonymous authentication method. The system uses a third party called tracer, to allow for the scheme to reveal malicious vehicles falsely authenticating. The scheme uses group signatures and pseudonyms to allow for a tracer to strongly identify malicious actors. For the authentication portion of the scheme the authors propose a privacy preserving authentication method that works in tandem with the third party tracer scheme to block abusive behavior on the network. The scheme uses multiple tracers when revealing a vehicles identity in-order to prevent the wrongful reveal of a trusted user on the network. The scheme uses a tracing key in a distributed manner that makes it impossible for the single tracer to reveal a vehicle. Through testing, the scheme was proven to be abuse resistant and secure against malicious attackers.

– Fraud Detection

Fraud detection has ample uses in IoV. In [200], the authors propose a spatio-

temporal cost combination based framework. This can be used in the detection of fraud in taxi driving. When the taxi first connects to the network, a predicted trajectory is created to determine the route the taxi would typically take. This is then used with a statistical model that is based off of three elements, time of travel, distribution trajectory, and the cost of travel. The real-time data is then collected and used to create graphs that can be monitored for abnormalities against the predicted statistical model. This is an example of an outlier detection algorithm being used to find a fraudulent actor in a network.

– Encryption

SDNs are widely used in network management systems. The authors of [201] have previously presented a routing protocol that is able to use road side units (RSU) in ad hoc networks for vehicles to route communications [202]. The authors upgrade the previous work with a scheme they call SURFER. The scheme takes advantage of the SDN architecture as well as a blockchain of RSUs to more efficiently route packages. The authors implement the the scheme in two different ways. The first method is to utilize SURFER entirely inside the RSU network. This similar to the previous work in all instances of communication except for infrastructure to infrastructure communication. The second method is to utilize the SURFER within the entire IoV network. This is a different communication method than the previous work. Each of the SURFER methods was proven to be effective through testing in the security and management of packet communication. SURFER-1 has a lower overall control overhead, traffic flow, and packet loss than SURFER-2 but the overall performance remains similar.

With everything becoming connected into the infrastructure of IoV, security is becoming a big concern to the safety of these large scale networks. For this to be possible, much of the communication must happen over open channels. The authors of [203] propose a method using a blockchain-assisted certificateless key agreement protocol. As discussed in previously mentioned schemes, the authentication agreement happens with the cluster head and then with a RSU to establish secret keys. The cloud server collects information from the RSU to create a transaction. These transactions form blocks which is then voted on using practical Byzantine fault tolerance (PBFT) consensus algorithm [204] to apply the block into the blockchain. The scheme was tested through formal analysis and informal analysis each of which proved that this scheme provides better security, lower communication costs, and offers more functionality than other similar models.

The introduction of 5G has allowed for many advancements in real-time communication offered in IoV infrastructure. It is important to authenticate all of the information coming in to the system to allow for this kind of infrastructure to be usable. Many of the industry standard schemes have large amounts of delays, lack of privacy, and reduced efficiency in communication. To handle this the authors of [205] propose the use of ECC along with Ant Colony Optimization On-demand Distance Vector protocol for the purpose of routing. The scheme takes advantage

of three different components. The first one is the use of Certificate Authorities (CA) for key generation. The vehicles unique number plate is used to create private-public key pairs when ECC is applied. The second component is the ability of the system to detect malicious vehicles. To do this the system sends periodic messages and checks for an appropriate response. If the system receives multiple inappropriate responses the vehicle is marked as malicious. The last component is the Ant Colony Optimization On-demand Distance Vector routing. The On-demand Distance Vector routing portion of the method is reactive and uses route discovery and route maintenance to find the best route. This is improved with Ant Colony Optimization which allows for a source vehicle to find the best route to a destination vehicle through multiple different vehicles. Through simulation testing, the scheme has shown higher throughput, lower delays, and lower routing overhead than other similar state of the art methods.

In many cities there is a missing component of privacy of user-data in toll transponders. In [206] the authors propose a privacy risk reduction model to improve the current toll transponder infrastructure in the city. The scheme uses a fully homomorphic encryption protocol. The scheme would be a post-quantum encryption method that works with a blockchain model. The privacy of this scheme is evaluated and passes when compared to European General Data Protection Regulation and the California Consumer Privacy Act requirements.

– Misbehavior Detection

Misbehaviour detection is similar to fraud detection in the fact that it is used in finding harmful or potentially harmful actors in a network. Misbehavior detection monitors behavior in a network and flags traffic that is abnormal. Deep learning has also gained a lot of attention for misbehavior detection because of its non-linear mapping ability. The issue with this is that deep learning takes time to train and is very hard to scale. The authors of [207] propose a form of misbehavior detection that uses a broad learning system (BLS). This method performs a similar task to deep learning but consumes less resources and is real time. Key features are found in raw data and used to establish the BLS. The system is the updated with newly generated data using incremental learning. Through experiments, this scheme performs better than other deep learning algorithms in terms of time and computation costs while remaining accurate. Unlike deep learning, the proposed scheme is also scalable for the use in IoV.

Many IoVs are vulnerable to cyber-attacks. This makes data integrity an important part of any IoV system. Many of the conventional ways of checking data integrity will not work in IoVs in terms of overhead and computation cost. Since many methods do not work in IoV there is a lack of protection and an RSU can be hijacked. In [208] the authors propose a lightweight method to check data integrity and find malicious RSUs. The scheme uses a probabilistic model for checking messages between intelligent vehicles and RSUs to find malicious RSUs. The scheme uses information over a period of time to create the model. The

scheme then uses a generalized likelihood ratio test to find the RSUs that are malicious as well as check integrity of messages. Through simulation testing the scheme shows a slight drop in latency and the number of bits communicated. The scheme also offers a 99% probability of detection.

– Intrusion Detection

It is not always possible to make a system that is completely impervious to intrusion. That is why it is important to create a detection system that can find when a malicious actor has infiltrated a system. The authors of [209] propose a multitiered hybrid intrusion detection system. The system uses a signature to check the identity of actors in a system. The system also uses anomaly detection algorithm to identify both known and unknown attacks in a system. Using testing the scheme has proven to be a strong detection method against many different attacks and is capable of being implemented in real-time systems.

Data vulnerability is something that is heavily focused on in the realm of IoV. Controller area networks (CAN) are the most popular system implemented in vehicles today to allow for sensors in a single vehicle to work in conjunction. Many of these CAN implementations are not secure enough and are vulnerable to attacks including DoS and Fuzzy attacks. In [210] the authors propose the use of deep learning techniques in intrusion detection to protect CAN. To detect malicious attacks the scheme is based on a VGG-16 architecture developed by a group of researchers at the University of Oxford in 2014. The scheme is trained on the CAN-intrusion-dataset to train the deep learning algorithm on types of intrusion on CAN systems. Experimental testing has shown that 96% of intrusions are caught and false positive rates are lowered in modern CAN intrusion detection systems.

– Falsification Detection

In IoV the ability for smart traffic routing is made possible by the ability of each vehicle to share its route. These can be useful in routing shipments but issues arise in most systems because a lack of storage. This issue can be made worse by the falsification of data being pushed to such a system and overloading the storage. The method proposed by the authors of [211] is a heuristic distributed scheme. The routes submitted by a user either penalize or reward them based on the contacts' confirmation. Through the use of a time-homogeneous semi-Markov process the system can check the accuracy of mobility patterns and then submit them to the cloud server via RSUs. The cloud then has the capability of calculating whether a vehicle is malicious. Theoretical models and simulations show that the model can effectively identify falsified data.

– Threat Hunting

With IoV infrastructure becoming larger and more vast in devices the security threats are becoming extensively hard to predict. This leaves IoV open to a lot of different cyber-attacks. The authors of [212] investigate intelligent attacks on

IoV and models the process of attack and defense through the stackleberg game. The stackleberg game allows the authors to minimize attacks while increasing defense. Through the model the authors were able to effectively create a defense model that was not influenced by what type of attack was performed, allowing for uniform defense. The solution proposed allows for balanced work and does not degrade the performance of the system.

Internet of Autonomous Vehicles

Improvements in video analytics in recent years has allowed for a tremendous amount of growth in the safety of autonomous vehicles. These improvements come with the added challenge of securely and reliably relaying video data. The authors of [213] propose a framework that implements both blockchain and multi-edge computing in autonomous vehicles. The use of these methods allows for a reduction in latency in the scheme. The use of deep reinforcement learning is optimized through the use of two different processes. The Markov decision process is used in reducing latency and allowing for a greater amount of throughput. Then an asynchronous advantage actor-critic algorithm improves the resource allocation of the model. Through testing, the authors were able to show that the scheme was effective at moving data quickly.

Internet of Connected Vehicles

Internet of connected vehicles (IoCV) has been used in urban services [214] and related areas.

Among security challenges and mechanisms related to internet of connected things, one may refer to the following.

- Security Challenges
  - Privacy

    Edge computing is a growing technology in IoCV that takes much of the burden of communication off of the vehicles that tend to have a low amount of resources. Many of these edge computing systems have issues in privacy including untrusted edge nodes which can leave location data vulnerable to attackers. Most proposed systems offer security with trusted nodes but do not discuss the unavoidable untrusted nodes that are important to the system. The authors of [215] argued that the need for security and privacy provisions in internet of connected vehicles increases with the mobility. They focused on the privacy considerations of communications between IoT layer vehicles and potentially-untrusted edge controllers as these communications contain private information such as location and speed. They reviewed related privacy preservation approaches and observed that existing approaches assume both parties (vehicles and edge controllers) to be trusted, which is not the case in some real-world scenarios. To bridge this gap, they developed a differentially-private data streaming system that injects a noise in the IoT layer instead of the transportation infrastructure. Their method scales

the noise on the basis of the data correlation. They evaluated their method and demonstrated that it outperforms state-of-the-art approaches.

One of the biggest risks that faces IoV is the lack of security in intelligent terminals that are in all smart vehicles. These terminals can be taken attacked by malicious groups and threaten the safety of the vehicle. In [32] the authors propose two authentication protocols to protect the intelligent terminal. The first authentication protocol used is to examine the behavior of the user when using and entering the network. The second layer of authentication is a password. For this authentication method to be effective the behavior must be kept private. No part of the authentication protocol reveals this information. In analyzing the protocol it is shown to be effective in terms of computation and communication costs.

– Attack Resilience

Trust management is an important system in IoCV but tends to be quite inefficient as they tend to assume that the number of road side units are limited. The authors of [216] create a scheme and assume that RSUs are able to provide efficient communication to any vehicle. They propose a system in which all vehicles contact RSUs directly to get all traffic communications. This allows for a more reliable and controlled spread of traffic information that can be checked easier for malicious activity. The method uses market trading in order to reduce the spread of malicious activity and reward sharing of information by weighing communications based on trustworthiness. Simulations prove the scheme to be effective at blocking malicious information from spreading.

Internet of Electric Vehicles

Internet of Electric Vehicles (IoEV) has been studied in many recent research reports [217]. A lot of articles focus on the safe transfer of energy from one vehicle to another or from vehicle to infrastructure. The authors of [218] propose a system of energy transfer that takes advantage of blockchain. All transactions are performed using smart contracts and are recorded through the blockchain. The smart contracts allow for optimal pricing and optimal energy allocation. A bidirectional auction approach based on the Bayesian approach is used to create a smart way of setting price. Simulations can prove that this system improves the current energy sharing system drastically. Energy management is also an important design challenge in IoEV; see [219][220][221] for the details. There are no research works focusing on the security challenges or mechanisms in Internet of Electric Vehicles.

Extensions with Applications in Physical Security

Internet of Surveillance Things

There are only a few research works focusing on the security of this extension.

- Security Challenges

– Trust

Image processing over multiple devices in surveillance of smart cities is an important task in increasing safety. The ability of a system to be able to find similarities and differences in an image found from vastly different interconnected surveillance devices is called saliency detection and is currently lacking in IoST. In [222] the authors propose a scheme that uses co-saliency which allows the use of more accurate saliency in IoST than other saliency enabled devices. The first contribution is a neural network that is able to find semantic with different repetitive fields on a single device. The authors then offer a two-path communication system between IoST to allow for comparing of surveillance information of different devices. The last contribution is a network refinement method that helps improve neural networks and better label semantic features. Using three public data sets the authors showed that their proposed method was superior when compared to four other state of the art schemes, CBCS [223], CBCS_S[223], CSHS [224], and CSDW [225].

Extensions with Applications in Industrial Control

Internet of Controllable Things

In recent years, Internet of Controllable Things (IoCT) has been studied in some research work. In [226] the authors propose an ensemble learning method and resource allocation scheme for the purpose of effectively scheduling remote automated observing systems (RAOS). RAOS are used to monitor environmental and meteorological elements for the purpose of efficiently collecting information. Bagging, AdaBoost, and Snapshot are all ensemble methods to capture features of clouds. These features are then applied to a CNN for classification. A cloud-edge framework is used in order to reduce communication stress on RAOSs as large amounts of data are transposed to the server. The scheme is tested experimentally and shows a high level of accuracy in cloud classification and is able to improve task allocation.

The authors are not aware of any research report related to the security of Internet of controllable Things.

Extensions with Military Applications

Internet of Battlefield Things

Recent literature comes with some research work focusing on Internet of Battlefield Things (IoBT). Knowledge of enemy locations on a battlefield can heavily favor troops in battle. The authors of [227] propose a localization method of enemies using soldier's locations and the direction in which they are shooting. This is done through the use of particle swarm optimization and k-nearest neighbor (KNN)-based clustering algorithms. Together they are able to predict the general area in which an enemy may be located. Testing of the algorithms shows promising results in terms of real-time results and accuracy for the prototype. A lot of these large scale systems are deployed using mobile edge connections. In IoBT there are

many electronic counter measures that can prevent a normal edge network from working. The authors of [228] propose a scheme that allows for connections in the edge network to move when a node is destroyed to allow for a more continuous connection. The problem is broken down into a lot of smaller sub-optimization problems using a heuristic algorithm to allow for the optimal connection. The proposed scheme is shown to have a lower time and energy consumption over the typical edge computing network when electronic counter-measures are in place. Among design challenges of this extension, one may refer to energy efficiency, latency and robustness [229]. So each scheme needs to take these into account.

In our reviews, we have not found any research work related to the security of this extension.

Extensions with Applications in Agriculture

Internet of Trees

Internet of Trees is a recent extension of IoT that can be used to monitor the health of trees. Trees and plants can be outfitted with sensors allowing for farmers to decrease over watering and improve quality of the plants that are being produced. The authors of [230] propose a system that works with electromagnetic sensors that uses spectral dispersion to measure moisture content. The sensors are linked together to better understand how a group of trees may need to be watered most effectively. The network of trees is combined through a representative network system based on long range (LoRa) protocol. The system is proven to be low-cost as energy is collected through solar and can reduce the amount of water used in the agriculture of trees.

Security challenges and mechanisms of this extension have not been adequately studied in the literature.

Internet of Agro Things

Internet of Agro Things (IoAT) has been studied in some recent research works. Crop production and yield is increasingly important in areas that have limited land for production. The ability to monitor crops and understand what can be done to increase output can be enhanced with networks of sensors in IoAT. In [231] the authors propose a CNN that is able to perform analysis on crop images. The sensor nodes collect images of plants to send to the CNN and are solar powered, reducing energy consumption. When tested in a 3-moth trial it was shown to be 99% accurate and was able to sustain harsh weather.

The authors are not aware of any reported research focusing on the security of this extension.

Extensions with Applications in Entertainment

Internet of Media Things

Internet of media things has been studied in some recent research works [232].

Some variants of internet of media things are studied below.

- Internet of Video Things

  Internet of video things connects things with visual sensors [233].

  Objectives such as scalability [6] have been considered in the design of internet of video things.

- Internet of Audio Things

  Internet of Audio Things refers to a network connecting physical objects called Audio Things with computing devices embedded inside them aiming at the production, transmission and analysis of audio in distributed environments. There is a survey in this regard studied in [54].

Internet of media Things has not been adequately studied from a security perspective.

Internet of Multimedia Things

Internet of multimedia things is a recent extension of IoT [234][235].

Researchers have considered the following security challenges and mechanisms in the design of this extension.

- Security Challenges

  - Confidentiality

    Low-cost compression while maintaining confidentiality of internet of multimedia things would allow for major advancements in entertainment. The authors of [236] propose a low-cost and confidentiality-preserving multi-image compressed acquisition model. The scheme evenly groups images together using the sigmoid sequence and each group is randomly assigned compressive sensing. The groups are then combined into a larger image and then encrypted to increase confidentiality. The image is sent to the cloud and run through a decryption algorithm. The cloud is able to use the designated reconstruction algorithm to recreate the image. Through simulations, the scheme has proven to be effective in confidentiality and cost in transmission of the images.

- Security Mechanisms

  - Authentication

    Internet of multimedia things has many applications in other fields including health care, surveillance, and the automotive industry. Each of these industries transmit large amounts of multimedia data. The authentication of edge devices on a network while protecting privacy of user information is a large focus of the industry. In [31] the authors propose a multi-layer framework based on edge computing to solve the problem. The scheme provides security through a four way handshake that happens between pre-made clusters. To keep privacy the

framework uses aggregation based on frame matching and an Label Distribution protocol based technique that adds noise to the aggregation. When compared to existing privacy-preserving schemes the proposed framework outperforms them based on a lower rate of error and data load.

Extensions with Social Applications

Internet of People

Internet of People is a recent trend in research on IoT that has led to a variety of different discoveries. The authors of [237] propose a method to improve the current recommendation systems that are becoming used more in areas such as social media searches. The algorithm they propose takes a users relationship in a network and the item's relationship in a network. To adjust weights of items in the system a tuning parameter is added. Objects that are not yet seen are extracted and ranked based on resource scores. Testing shows a high accuracy on top recommended items for given datasets.

Similar to the above, the authors of [238] create a interest detection framework based on social networks. Using similarities between different likes and dislikes of a user a proximity function is able to create links between items. The scheme uses a greedy community detection algorithm to further find users with common likes and dislikes. Lastly a link detection algorithm is used to create links between items that are commonly linked together using community information. When tested experimentally, the proposed method outperforms other deep learning schemes built for similar purposes.

To the best of the authors' knowledge, security challenges and mechanisms of this extension have not been adequately studied in existing research works.

Internet of Scholars

Internet of Scholars (IoS) has appeared in a few recent research reports. Scholars are having a more difficult time finding needed publications and scholarly connections as more publications are released. A recommendation tool specifically for scholars can be very useful. The authors of [239] introduce the idea of a scholarly friend recommendation system. Using academic social networks, the authors hope to help scholars find people who do research in areas that could benefit each other. The authors first construct a attributed social network using digital libraries. Attributed random walk is used to model scholar attributes and network structure. To create recommendations a graph recurrent neural framework is used. The effectiveness of the model is shown when tested on information collected from ResearchGate and LinkedIn.

In our review, we have not found any research work focusing on the security of Internet of Scholars.

Internet of Mobile Things

Internet of Mobile Things has been also recently studied in literature. There are many applications that involve networks of mobile devices. Issues arise due to the computational limitations these devices have which makes it difficult to send large amounts of data. In [240]

the authors propose a scheme for fog computing based on Fountain codes, reducing latency and processing time of receiving positions of mobile devices. The fog computing scheme is able to offload tasks using its high computation power. The scheme takes advantage of maximum distance separable code allowing for the scheme to be highly flexible with low complexity. Testing shows that through the use of the Fountain code-based scheme the loads of transmission and communication are reduced.

This extension has not been studied from a security perspective in existing research works.

Extensions with Applications in Smart Homes

Internet of Kitchen Things

Internet of Kitchen Things (IoKT) has been of interest to some researchers in recent years. Many kitchen devices are being added into the world of IoT such as refrigerators and ovens. When connected to a network it offers a great amount of convenience to the users. It can allow users to preheat their ovens from work or see what items they need in the refrigerator while at the store. One area they struggle with is understanding the people they work for. The authors of [241] introduce the idea of TupperwareEarth which aims to reduce cooking tasks for users based on the network of IoKT. The system is designed to allow for real-time management of inventory. The scheme uses an ontology-based database to allow for the device to suggest recipes based on users inventory, appliances, and preference. User studies have proven it to be a useful tool in the kitchen.

Our work has not led to the identification of any published research on the security of this extension.

Extensions with Applications in Critical Infrastructures

Internet of Energy

Some research work have discussed Internet of Energy (IoE) as an extension of IoT. As more data is transmitted there are more areas for error such as receiving low quality data. Further adding to issues, most devices must use edge networks to offload higher computational tasks. Lack of privacy among edge nodes, low-quality data being transmitted, and low-quality results from low quality data all arise due to edge computing. The framework proposed by the authors of [242] consists of three main parts. A data quality evaluation is used to provide high quality data to the blockchain. The next part is data repairing to fix any incomplete or low quality data before being added to the blockchain. Lastly is distributed reinforcement learning for task arrangement to offload tasks in an effective way that reduces burden on nodes in the network. Numeric results show that the scheme is effective at offloading tasks.

Another scheme proposed by the authors of [243] is used in the preserving of energy due to shortages caused by Covid-19. The proposed scheme is able to better allow for the distribution of energy across a grid based on needs of each area. Using edge based architecture the scheme creates an energy efficiency framework. Using an interface users

can monitor consumption and environmental data. Energy saving strategies based on the user's habits are also given to reduce potential waste. These calculations are created from a rule-based algorithm. This is one of the first instances, as far as the authors know, at implementing an energy saving recommender. The scheme proves effective as a prototype in giving effective strategies to lower energy usage.

To the best of the authors' knowledge, there is no published research related to the security of this extension.

2.7.3 IoT in the Sea

Internet of Ships (IoS)

IoS refers to the interconnection of a large number of smart, physical devices or infrastructures associated with ships, ports, or maritime transportation systems, aiming at improved shipping industry in terms of efficiency, safety, and environmental sustainability. IoS has found its applications a broad spectrum of scenarios, including collaborative decision making, route planning and optimization, cargo tracking, safety enhancements, automatic fault detection, preemptive maintenance, energy-efficient operations, automatic berthing and environmental monitoring [70].

There has been many recent developments in IoS. Fault diagnosis in IoS is something that has been studied and handled through the use of deep learning to improve performance in shipping. In [244] the authors propose a fault tolerance scheme that uses a privacy-preserving federated learning approach. The scheme is able to, without data leakage, manage shipping agents to develop a model by sharing parameters. Federated learning is used to help with a lack of insufficient data to help in training a deep learning model. To protect fault data the authors encrypt the parameters using a Paillier-based communication scheme. The fault diagnosis is handled by a control algorithm. This algorithm is adaptive and changes the model for training. Analysis of the method proves this to be an effective fault diagnosis scheme when tested on a fault dataset.

Internet of Ships has not been studied from a security perspective in the current literature.

Internet of Underwater Things

Internet of Underwater Things (IoUT) have been used in data aquisition [245], smart oceans [246] and similar areas.

Researchers have considered the following security challenges and mechanisms regarding IoUT.

- Security Challenges
  - Privacy

    IoUT is the network of devices used in sensing, communication, and controlling the environment. Recently, proposed schemes focus on information collection and position estimation in IoUT. The localization systems proposed in these are

based around an anchor node. In these schemes location privacy is not correctly protected making the anchor node vulnerable to attack. The authors of [247] propose a privacy-preserving localization system. The scheme uses a privacy-preserving asynchronous transmission protocol to detect malicious anchor nodes and hide location information of anchor nodes while not being synchronized to a clock. To localize the target location a privacy-preserving estimator with ray compensation is used to avoid localization bias. Through testing simulations and experiments, the authors prove the scheme to be an effective system of localization.

In addition to security, energy efficiency [248] has been considered as a design objective in recent research on internet of underwater things.

2.7.4 IoT In the Sky

Internet of ViSAR Vehicles

Industrial Video Synthetic Aperture Radar (ViSAR) is a new technology that is used in Unmanned Aerial Vehicles (UAV) for real-time surveillance. This has useful applications in monitoring natural disasters at night without the need for a source light. Most ViSAR vehicles take a large amount of bandwidth and have a low data rate of communication making an effective system hard to design. The authors of [249] propose a loss-less data collection technique that eliminates redundant information from being communicated back, lowering costs of data exchange. The scheme takes advantage of the method of reversible watermarking and combines it with dual-phase interpolation-based embedding. This method will use a greedy network of weights. Through the use of simulations, the proposed method is proven to be better than previous methods in terms of reliability, efficiency, and speed.

Our reviews have not led to the identification of any research report related to the security of this extension.

Internet of Aerial Vehicles

Air traffic management is becoming an ever-increasing area of focus for aerial vehicles. With this comes the security issues that are beginning to arise as more of these systems are designed. Current systems are unable to handle the amount of communication that will occur as more aerial vehicles need to be managed. The authors of [250] propose a method of advanced automatic-dependent surveillance-broadcasting (ADS-B) that allows for easy tracking and monitoring of aerial vehicles. To do this, the authors take advantage of a grouping-based conflict detection algorithm. The flight paths of aerial vehicles are then predicted using a combination of machine learning algorithms, long short term memory (LSTM), and deep sentence embedding-based trajectory prediction. Through testing the proposed scheme was proven to be able to detect conflicts within seconds.

Internet of Drones

A drone is an autonomous aerial vehicle. Internet of Drones are used in a variety of application areas, including civilian and military aerial photography, Cloud and Fog computing, Unmanned Aerial Vehicles (UAVs), Wireless Sensor Networks(WSNs), and mobile computing. Some recent research works have been focusing on internet of drones [251]. The following security challenges and mechanisms have been studied in research works focusing on internet of drones (IoD).

- Security Challenges
  - Privacy

    In recent years there has been an increase in the use of drones in many different aspects, such as structural evaluations, public safety, and in industrial settings. In many cases, the information being relayed back from these drones is sensitive, so it is important to make sure the privacy is well kept. The authors of [252] propose a privacy-aware authenticated key agreement scheme. This scheme does not require drones to store secret keys, which in turn creates a method that requires less storage on the limited space of the drones. To the best knowledge of the authors, this is the first time that the physical security of the drone has been studied. Third party communication and mobile edge computing are both supported in the authentication of the UAV. This is done without losing privacy.

    In IoD, privacy during communication between a moving point and a ground unit is vital to the safety of the user and the drone. In [253] the authors propose a blockchain based framework for securely managing data. The scheme is used as an access control between a drone and its ground unit by establishing a session key. All communication is published to the blockchain for management and review. A consensus-based algorithm verifies the information published to the blockchain. The Automated Validation of Internet Security Protocols and Applications (AVISPA) tool is used in testing and proves the security of the proposed scheme. Analysis of the scheme further demonstrates its high level of performance and security.

- Security Mechanisms
  - Authentication

    Many of the recently proposed schemes in IoD either degrade the efficiency of these devices or are proven completely insecure. The authors of [254] propose the use of ECC and symmetric key primitives to create a new authentication method between a specific user and the drone. The user is able to access the server through the network and a password. The server then tracks the flying area of the drone and is able to link it to the user once authenticated. To test the security of the method, the authors use the random oracle method.

    When it comes to authentication in IoD many proposed systems use centralized authentication. The issue with this is that these systems typically have single

point of failure and struggle with cross-domain authentication. In [255] the authors propose a blockchain-based cross-domain authentication scheme to be used in tandem with 5G. The issues of storage limitation and authentication latency are areas blockchain struggles with. To mitigate these issues there is a local private blockchain to support local actions. Only authorized individuals are able to view and mange devices on this. The authentication method used is a multi-signature smart contract. This allows for authentication of terminals by using consortium blockchain. To securely transmit data the parties negotiate a session key for communication. The method was analysed to prove its effectiveness and efficiency.

– Encryption

The need for real-time data is useful in some types of drones. Instead of storing information at the server it is sent directly to the user. For this to happen there needs to be a high level of privacy. In [256] the authors propose a robust authenticated key management protocol. The scheme uses a high level Authenticated Encryption with Associated Data (AEAD) along with ECC and SHA-1. The scheme validates a user and allows for the creation of a session key for secure communication with the drone. Random oracle model is used to validate the session key is secure. Compared to related authentication key management schemes, the proposed scheme has lower storage costs, overhead, and computational costs.

Encryption in drones can be used in the creation of session keys to create secure channels for communication. In the process of creating this secure channel, it is important to maintain the anonymity of the drone and the user. The authors of [257] propose that in any session there should be a focus on pseudonymity and unlinkability. If a protocol only used pseudonymity then when communication is analyzed the user's privacy could be breached. If a protocol only takes into account unlinkability then a stolen drone could have its session key stolen. On the basis of these principles, the authors propose a system of first key agreement. The protocol works by first sending the drone a pseudonym, being used for the session, to the user. The user then decrypts the pseudonym using the password that the user obtains when registering the drone. The user then sends their pseudonym to the server. The server then creates two session keys sent to the drone with the users pseudonym. Once decrypted, the drone sends the session key to the user to decrypt and verify with the server allowing for an authenticated connection. Through testing of efficiency, the authors found that their protocol was more inefficient than other schemes, but when looking at other methods with key exchange protocols providing full forward secrecy, it was one of the most efficient, in terms of computational costs.

Internet of Unmanned Aerial Vehicles (UAVs)

A UAV is a remotely-controlled aerial vehicle. Internet of UAVs has been studied in some recent research works [258].

It has found its applications in object tracking and similar areas [259].

Recent literature highlight the following security challenges and mechanisms with respect to internet of UAVs.

- Security Mechanisms
  - Malware Detection

    Advanced persistent threat (APT) has become one of the biggest threats to security in recent years. IoT tends to have less secure structures than most systems, so APT is an especially egregious threat, especially for UAVs. If malware is inserted on a UAV, it is able to then communicate with a command and control center (C&C) which is responsible for communication with the drone. The current ideology behind malware detection is through the monitoring of behaviors when communicating with the C&C. This would typically work but APT uses a low traffic mode that allows it to mix in normal communication to confuse the malware detection system. The authors of [260] propose a way of detecting this attack. APT attacks use domain name systems (DNS) to locate C&C centers and each time will log information on the DNS logs. The logs can be observed for signs of malware. With this information, the authors proposed a malware detection scheme using string matching and Fourier transformation. To preprocess the data, the authors convert DNS time stamps of DNS requests into strings. Then to monitor the requests, the authors use a trained random forest model to identify suspicious activity in the logs and to alert to compromised UAVs. Through testing on data sets, analyzed by ATP security experts, the authors have found the proposed method to be 94% accurate.

2.7.5 IoT in Space

Internet of Remote Things

Internet of Remote Things (IoRT) has been of interest to researchers in recent years. Gateways are a way for terrestrial networks and IoRT to communicate and allow for IoRT services. Each gateway can possibly have different channel conditions, locations, and other varying parameters which can affect performance of communication. This makes gateway placement vital to how IoRT is able to communicate. The authors of [261] propose a way to effectively place gateways to minimize access distance and amount of gateways needing to be created. Distributed resource allocation (DRA) algorithms are designed using principles of alternating direction method of multipliers (ADMM). This allows the algorithm to find the total revenue and cost of gateway placement and cost of deployment and optimize them. A genetic-based gateway placement algorithm is then used based on the data given by the previous algorithms to offer a solution. The proposed scheme shows through testing its ability to effectively place gateways in a way that improves communication and lowers costs.

The authors are not aware of any research work related to security challenges or mechanisms of this extension.

Internet of Space Things

Recently, researchers have paid attention to Internet of Space Things (IoST). Cube satellites are new types of satellites that offer global communication at low costs. They offer advantages over normal satellites including short development to deployment and lower cost of development and deployment due to the off-the-shelf components. These make them great tools for creating large scale networks. An automatic network slicing framework for space-ground integrated networks is proposed by the authors of [262] to use these cube satellites to their full capabilities. The design tackles challenges such as dual objectives of route computation and is able to allocate resources to avoid service level agreement violations. The system being automatic means it does not require prior information in terms of resource availability to slice. To allow for low signaling overhead the scheme uses an online segment routing-based approach to route communications. The authors have done benchmark testing that has shown the usefulness and effectiveness of the proposed scheme for large network communication in IoST.

According to our reviews, this extension has not been studied from a security perspective.

Internet of Satellites

Some research work have studied Internet of Satellites in the area of anti-jamming technology as smart jamming has become more of a threat in recent years. The authors of [263] use Stackelberg game and reinforcement learning to minimize the cost of creating an efficient anti-jamming protocol. To do this the authors create the problem as a Stackelberg game for anti-jamming. The scheme for anti-jamming is broken into two parts. To find the best routing that is available the authors use a deep reinforcement learning routing algorithm. To make fast decisions a fast response anti-jamming algorithm is implemented. The scheme uses these methods together to make the best decision for anti-jamming. The scheme shows low routing cost and solid anti-jamming protection when tested.

In our review, we have not identified any published research focusing on the security of this extension.

2.8 Related Work

While social authentication is discussed often in recent years, there still exists issues with current methods rendering them unusable for applications into IoT. The goal of this thesis is to present the best methods of combining social authentication and bot detection in order to create a secure and usable fallback authentication method. This method should provide adequate social cybersecurity but also cover the objectives of performance, QoS, QoE, timeliness, reliability, scalability, fault tolerance, energy efficiency, and security that are also important to IoT devices.

Chapter 3

TBSA Mitigations

There are many different versions of TBSA. The following sections will go through some of the most prevalent schemes of TBSA, some of which have been used in the industry [36], [37], [38], [39], [40], [41], [42], [43], [44]. Each subsection provides a brief explanation of the design choices and methods used in applying them. Furthermore, each scheme is then analyzed for security challenges. The challenges of TBSA range from attacks to design flaws that need to be considered before implementation can begin. The sections will break down each of these concerns, some of which overlap from scheme to scheme. This Chapter is currently under review for publication.

3.1 Fourth-Factor Authentication

An earlier form of TBSA was introduced by Brainard et al. [36] called fourth factor authentication. The scheme was designed as a fallback authentication method using someone you know. The concept is based on the idea that there are currently three types of authentication: something you have, something you know, and something you are [36]. In other words something you have is a token, something you know is a password, and something you are is biometrics. The authors create a novel form of authentication around the concept of the fourth factor they coined as someone you know. This is one of the original designs of TBSA.

The application is designed with a helper and asker webpage and an underlying administrative program using C++ and Microsoft framework. A user is first prompted for a password and can click an option for a forgotten password. The user is then asked to contact a helper through out-of-band services and to enter that helper's username. Once a helper is contacted for assistance in authentication, they must enter their username and password to retrieve a vouching code for the asker requesting it. The helper then must convey the vouching code to the user. The user must enter their four digit PIN and the vouching code in order to regain access using a temporary password. Once inside their account they can reset their password. This allows a user who can remember their PIN but not their password to regain access to their account.

Security Challenges

This method is one of the earlier designs of TBSA. The design of [36] is created using only a single trustee. This in itself makes it an easier target for attackers. In the case of a *spidering attack* an attacker only needs to crack a single helper account to authenticate into many accounts. This can be very dangerous and over time lead to an entire network of users to have compromised accounts. The authors attempt to stop this dangerous progression of spidering by making the authenticator enter a four-digit PIN. This seems like a good idea but a four-digit PIN can be cracked instantly using *jack-the-ripper*[264]. Using the birthday paradox, a four-digit pin consisting of ten-thousand combinations has about a fifty percent chance of being guessed after only one hundred and twenty attempts.

Further concerns include a helper impersonating a user. Since the method proposed in [36] only requires a single trustee, it leaves room for a malicious helper to create a vouching code for themselves to enter another users account. Once again the only prevention of this is the use of a four-digit PIN, which can quickly be cracked. This creates a system in which personal data can be attained by any helper who is able to verify a user.

Similar to other TBSA systems, social engineering is another concern that needs to be considered. This is due to the fact that communication is a key part of authentication and messages for retrieving vouching codes can be spoofed. As with any system where spoofing is a threat, good security practices will prevent this method from being effective. Good security practices is not something that can be guaranteed. This is shown with the fact that a large percent of attacks occur with social engineering and typically have a high success rate [265]. An attacker can use social engineering and message spoofing to convince a user to send them a vouching code for the account they are attempting to infiltrate. If the helper does not do a good job verifying the user (i.e., asking questions or verifying their voice) then an attacker can easily attain the vouch codes.

3.2 Trustee-based Social Authentication for Windows Live

Schechter et al. [37] propose a form of TBSA to be used for Windows Live. The authors designed a TBSA system that is built for the purpose of being a fallback authentication method for Windows Live. The user is required to give the emails of people they wish to use as their trusted list. When a user forgets their password they can begin the fallback authentication process on the Windows Live application. The system will send a vouching code to the trusted users previously denoted. The user must then obtain the vouching codes from the trustees in order to be re-authenticated. It is encouraged by the system to do this via call or in person as to avoid the possibility of spoofing that occurs through texts and email. The authors tested this using a prototype and found that users were able to reliably regain access to their accounts while also remaining relatively secure.

Unlike Fourth Factor Authentication [36], Windows Live requires a user to obtain more than a single vouching code to complete the fallback authentication process. Schechter et

al. [37] explain the situation that if there are four trustees in a user's list, they must obtain two trustee codes for the fallback authentication method to be complete. This prevents the vulnerability of a single malicious trustee from gaining access to a user's account. The authors accept that this is more inconvenient than a single trustee but believe this can be justified given that it is a fallback authentication method and should not be used often.

Security Challenges

One of the main vulnerabilities current TBSA systems have is an attack designed by authors of [266] called the *forest fire attack*. The attack is used in two phases. The first phase is the ignition phase in which the attacker compromises a group of trustee accounts. This can and has already been done in a variety of ways such as brute force password cracking and phising [266]. Once a number of accounts are compromised the attacker can begin the propagation phase. The propagation phase is a mass attack typically completed by a botnet (a large set of compromised systems). Using the resources of the botnet an attacker is able to propagate through large amounts of usernames in order to attempt to ping the compromised trustee accounts. If the attacker is able to find a user that pings enough compromised trustee accounts the attacker gains access to that user's account. If the attacker does not have enough trustees to gain access the attacker can spoof messages to convince other trustees of a specific user to send verification codes.

The forest fire attack is used to take over multiple accounts by compromising a few. Since a user can be a trustee for multiple other users it can also be used to compromise a larger number of users by systematically compromising accounts [266].

In [266] the authors tested this method against a theoretical model of a TBSA system. This showed that with a relatively small seed group they could compromise two to three orders of magnitude of users. To reduce the numbers of this attack the authors introduce the solutions of hiding the trustee lists which increases the number of accounts an attacker must search and compromise. This seems like a good idea but ultimately is proven not to work as users have a hard time remembering who their trustees are [266] [267]. Without this reminder users are unable to obtain their vouching codes. The authors also suggest that users are warned of such spoofing attacks to increase awareness. This can provide some protection as warnings make the idea of attack more prevalent in a trustee's mind. Ultimately this will not stop all spoofing as even with all of the training currently in the industry there are still successful attacks happening. Lastly the authors suggest a method of trustee selection that mathematically reduces the centrality of trustees in the network. This can further reduce the chances for attackers to gain access to a large number of accounts through a small number of trustee accounts. These fixes reduce the effectiveness of the attack but does not stop the attack from working.

Specifically with this scheme the trusted members of a persons network are contacted via out-of-band services (i.e., email). This allows for a variety of people to be used for verification and makes it easier for a user to select a trusted person. Unlike other schemes, they can select anyone who has a valid email address. The issue with using out of band services such as email to send vouching codes is the increase in ability for spoofing to occur.

Attackers have been able to spoof emails, texts, and phone calls in many different attacks and have proven the vulnerabilities with using out-of-band services [266]. Along with this, users have no idea if a trusted member has stopped using an email or if it has been recycled by the email provider. The scheme can be implemented long before a user has a need to use it. This means that occasionally a user's trusted member may not have the same email they had before. This not only can make it impossible to verify a user but becomes a security threat as attackers can attain recycled emails.

Each of these vulnerabilities listed above are able to be used by attackers to further propagate a forest fire attack [266]. The authors of [37] discuss the vulnerabilities of the system when it comes to spoofing and perform small scale spoofing tests. The authors believe the tests performed have promising results in terms of security but lack the sample size to be significant [37].

3.3 Facebook's Trusted Contacts

Facebook's version of TBSA called Trusted Contacts was created in 2013 [38]. It was designed to allow users to select three to five friends on their friends list to act as verifiers if they are locked out. Trusted contacts must also have an account with Facebook as well to be used as a trusted contact. If a user is locked out of an account they must enter their full name, username, and phone or email. After the user is verified the user must identify one user in their trusted contacts by entering their full name. Trusted contacts will receive a code for verification. Similar to the previous methods a user must collect a code from their trusted users to regain access to their account. Once a user collects three of these codes they are able to reset their password to regain access to their account.

Security Challenges

Once again as discussed in the previous trustee-based scheme, the forest fire attack and other spoofing attacks are very prevalent for TBSA methods such as Trusted Contacts in Facebook [38]. For the forest fire attack to be successful, the attacker needs to target trustees of specific users. This allows them to spoof messages to these trustees in order convince them to send vouching codes. In any TBSA scheme it is important that the user is reminded of who their trustees are [267]. This means the information must be made available for the user but can also be leaked to an attacker. Facebook tries to prevent the information from being too readily available by making a user type the full name of one person in their list. The issue is that for more targeted spoofing attacks an attacker should be able to find out enough information through researching the target to guess one of their trusted members. While the idea of making a user enter the name of a trustee prevents direct access to trustees it does not stop a well informed attacker. Once an attacker has access to the trustees they can easily spoof messages to try to obtain vouching codes from trustees.

Similarly, forest fire attacks which sometimes use spoofing to further attack can work very efficiently at guessing trustees [266]. Facebook users can allow friends and friends of

friends to see their friends lists. Since forest fire attacks start with a seed of users they are able to view friends lists to brute force guess trusted users. Once this is completed then the forest fire attack can propagate as discussed in previous sections. Facebook has currently discontinued the service of Trusted Contacts due to some of the issues discussed above [38].

3.4 Video Notarization

The authors of [268] propose a form of TBSA that uses video chat as a way of authentication. The design can prevent device theft that can occur in typical TBSA by having to physically verify a user. The authors believe this reduces the likelihood of an attacker being able to impersonate the user in the fallback authentication process. Once a user activates the process the system will contact users from a set of notaries in order to begin a video chat. These notaries would be pre-verified people that are able to be used to verify a persons identity. Once a notary accepts the notification of authentication a video chat will begin between the user and the notary. The notary will also receive a photo of the user in order to help them identify the user. Once a notary has confirmed that a user is in control of their phone a link will be sent to that user to reset their password.

The authors conducted some user studies to test the usability and security if a scheme of this nature was implemented [268]. The first thing considered was that through the study the identification rate was not as high as the authors would have liked. This creates an issue to whether or not such a system is effective in authentication. The second thing tested was ability to tell whether or not the trustee was interacting with a video, photo, or a true user. It was concluded that while some trustees were able to effectively verify if they were speaking with a true user or not, not all trustees were able to. It should also be noted that the study was conducted on a very small group of university students. The authors express this is not a good representation of the population, the main concern with the survey group is it does not have a good representation of the population's comfort with or knowledge of technology [268].

Security Challenges

Some of the main security concerns with the application mentioned above are the ability for a trustee or stranger to adequately and accurately identify a user based on photos provided. Without this concept being able to be done in a way that provides the most reliability, the idea of video notarization as shown in [268] and [39] will not be able to be used. This does not complete rule out the possibility of such a tool, as studies have shown that in many cases friends are able to more accurately identify each other as opposed to strangers [269].

Other concerns are with the ability of an attacker to use software to make themselves look or sound like a user. The software for this has already been created by the authors of [270]. The software can take real-time video of one person and make it look as though they are another person talking. The software only requires a photo of the user they are attempting to mimic and a RGB real-time video input. This can be used to mislead users in a video

notarization setting. Similarly AI is already being used to mimic voices of other people in cyber-attacks [271]. The use of voice mimicry software and real-time video augmentation raises some concern with using video notarization for the purposes of authentication.

The final security challenge that should be discussed is the possibility of a malicious notary. The system randomly selects a notary as to avoid a notary from using themselves in a fallback authentication attempt. While more unlikely than some of the previous security challenges a malicious attacker could gain control of multiple accounts making their chances of being the notary for authentication more likely. The more accounts they gain the higher the likelihood of their notary account being selected for re-authentication. This allows them to maliciously notarize user accounts to gain access.

3.5 Video-based Social Authentication

Guo et. al. [39] propose a form of TBSA similar to [37] and [268], in which a user is verified through the use of a preset group of trustees and video notarization. For example, a user forgot their password and must reset it. To do this they would contact the system for which they have forgotten the password for. The system will then contact the group of trustees requesting a verification of the user. The user must be available for a video call. The trustee then must decide after the video chat whether or not to verify the user. Once verified, a user is able to access their account and reset their password.

This is believed to be more secure as another person is able to assess if the correct person is attempting to connect. This is more difficult to break than the previously mentioned fallback authentication methods. While viewed as more secure there are some security challenges that need to be addressed before implementation can occur which will be discussed in the next subsection. The proposed idea is not implemented in this thesis but is tested in a user study using a mock version to test usability and user comfort. Ultimately the authors believe that their data shows that users would be comfortable using this scheme.

Security Challenges

As discussed in previous sections, one of the most prominent threats is the forest fire attack. Video-based social authentication still has this issue even with the protection of video identification. Through the use of deepfake technology attackers are able to fake videos and voices in real-time to trick trustees into producing vouching codes. This is similar to spoofing in other methods. With enough trustee accounts captured or spoofed an attacker could gain access to a large number of accounts very quickly. The verification of a user in this scheme still only requires a single authorization. This leads to the risk of a malicious trustee and reduces the amount of work an attacker must put in to gain access to another users account. A malicious trustee can easily verify themselves into a persons account they are a trustee for. If an attacker can gain access to a single account in your trusted network they can easily verify themselves.

Another concern of many of these systems include design challenges. Number of trustees and how trustees are selected are two very debated topics in the use of TBSA [272]. Many current schemes of TBSA allow users to select trustees from their friends lists with no true restrictions. Something that has not been researched in-depth is how the number of trustees needed for verification and total number of trustees affects the usability and the security of such a system. It is assumed that a system would need at least two users for verification to reduce the chances of a single malicious trustee to access an account[272]. If a system allows a user to have an infinitely large trustee list and it only needs two verifiers it is very easy for an attacker to compromise an account. Increasing the the number of trustees on a list while decreasing the number of verifications improves usability but reduces security. On the other hand if a list of trustees is rather small while needing a large amount of verifications it can be nearly impossible for a user to use the TBSA system. Research is needed to determine what the best parameters are for number of trustees in a list as well as the number of trustees required for verification.

Trustees being shown in the verification process is something that has been discussed for improvement in security. This would remove the possibility for an attacker to find out the trustees and spoof messages to them. The issue is in many cases a user is unable to remember who their trustees are and need a reminder to know where to collect vouch codes [267][37]. This is why researchers assume that in all cases that the trustee list is available upon activation of TBSA [267].

Chapter 4

Proposed Solutions

As seen in Chapter 3 there are still vulnerabilities in current TBSA systems. The forest fire attack, while its effectiveness has been reduced, still is a potential threat to current systems. We propose the use of some auxiliary authentication schemes in order to verify that the trustee and user are the correct people accessing their account. Additionally, we offer solutions that improve security that does not affect usability. The following sections will discuss ways that current TBSA systems can be improved. This Chapter is currently under review for publication.

4.1 Knowledge verified TBSA

We propose the use of a knowledge-based social authentication (KBSA) process for users before they begin TBSA to regain access to their account. KBSA uses information that is specific to a person or group to create questions to be answered for authentication purposes [273]. This can be especially useful against forest fire attacks and targeted attacks where an attacker is not aware of the user's relationships.

As previously mentioned forest fire attacks are by design made to attack a large number of accounts at once [266]. The attacker will have to propagate through a large number of accounts in order to find accounts to compromise and spoof messages for. If a system requires a user to have n trustees to verify an account then an attacker must compromise that many trustee accounts to successfully compromise a user account. Since forest fire attacks are on such a large scale it is very unlikely for the attacker to have social knowledge of the person they are trying to attack and the relationship the trustee has to the user. This makes it much more difficult for the forest fire attack to propagate effectively enough to take over a large number of accounts. There are two promising KBSA methods that can be used for TBSA.

4.1.1 Methods for Implementation

The first KBSA method uses photo identification for authentication. Yardi et al. [41] designed a system called Lineup that uses Facebook's social network graph. This scheme uses photos (linked to the authenticating user's Facebook account) along with their tags. Using these photos as prompts, the authenticating user must identify the people in the photo. This works on the ability of the user to be able to recall the people that are shown in the photos. It is not used as a primary form of authentication but as an extra barrier to login when suspicious activity is detected. Due to the amount of facial recognition algorithms available today their are some flaws that need to be addressed before implementation. Polakis et al. [46] create an attack using publicly available knowledge to prove that the Lineup is not a viable option in its current state due to AI. To improve the scheme the authors offer the use of bot detection, removing suggested answers, and adding noise to photos as ways to stop AI from being efficient.

Another promising form of KBSA uses a similar model of collecting information from Facebook's network. Instead of using photos, the authors of [40] use data collected on users by Facebook. The data used is called *node attributes* and consists of information such as employment, location, schools attended, etc. The data of authenticating users' friends is also collected. Using these sets of data the authors were able to propose a scheme that automatically creates a set of questions based off of node data, pseudo-edge data, and edge data. Node data is information that relates directly to a person in the authenticating users network. Pseudo-edge data is information that relates to a group of friends. Finally, edge data refers to interactions between users. Through user testing the authors found that the information collected and used to form questions showed promising directions for a fully functional form of KBSA.

Both of the mentioned methods have the possibility to create a more secure form of authentication when used in conjunction with TBSA. In the next section the interaction between TBSA and KBSA will be analyzed to find the most secure way to implement them together. Additionally, vulnerabilities and ways to prevent them are discussed.

4.1.2 How KBSA Interacts

The purpose of implementing these two social authentication methods together is to reduce an attacker's ability to use message spoofing as a way to break TBSA. The idea is to use KBSA as another barrier that can not be broken through human error (i.e. falling for a spoofed message). To be able to do this we need to determine the best way for these methods to interact. KBSA and TBSA can interact in a couple of different ways. To determine the most effective way to implement, the design will be analyzed with knowledge-based before and after TBSA. The design will also be analyzed for use with the trustee and for the user. One thing that should be considered is that during trustee selection, a user should select candidates they have the most knowledge about. This allows for an easier authentication when using a KBSA scheme.

Before or After TBSA

The first scenario that needs to be analyzed is whether the KBSA should occur before or after the implementation of the TBSA. By using KBSA as a barrier to TBSA we are able to remove a large portion of attacks currently used on TBSA. The forest fire attack, as stated previously, works by taking advantage of the fallback authentication process TBSA to further gain control of more accounts [266]. KBSA can be used as a barrier to prevent such mass attacks from beginning. This also reduces the exposure to the trustees used in the scheme.

By implementing KBSA after TBSA the scheme prevent attacks to KBSA. KBSA can be vulnerable to attacks from attackers with extensive knowledge about the user and their relationships. Since KBSA does not only use personal information to create questions it is unlikely for an attacker to have all of the information required to answer the questions. But with the increase in social networking and publicly available knowledge it may not be impossible for an attacker to acquire enough information to by-pass KBSA. By implementing TBSA first you prevent knowledgeable attackers from beginning authentication.

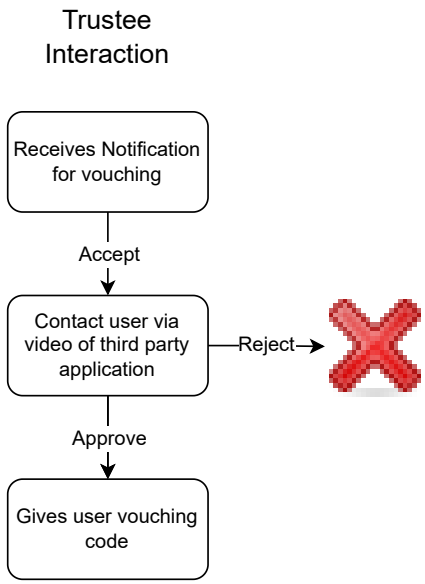

Figure 4.1: Knowledge Verified scheme design for trustee interaction.

To determine which method should be first we must analyze which poses a greater threat to security and privacy. To initiate these systems a user must enter their username, which should not release the identity of the user. When TBSA is initiated by the user the user must be reminded of who their trustees are [267]. This in itself poses a threat to the entirety of the system. It immediately tells an attacker who to target in order to gain access of the users account. This can also lead the attacker to who the user is by providing information of the relationships the user has. If a user initiates the fallback authentication process they are given the trustees names giving an attacker more information than they previously had. This then gives the attacker more information on how to break the KBSA side of the scheme. By implementing KBSA first, the attacker is not provided any information as to who the user is or who they may have relationships with. This provides a more secure and private social authentication scheme that relies on who you know.

That being said there are still some vulnerabilities that need to be considered with the order. The biggest concern is that an attacker may be able to crack both KBSA and TBSA. To be able to do this an attacker must first crack KBSA. This can be done if an attacker has extensive knowledge on a user and their relationships. This can be done but only allows an attacker to crack accounts they have extensive knowledge about, reducing the number of accounts that are vulnerable to a single attacker. Assuming an attacker is able to do this they

then must use spoofing and social engineering to attain the vouching codes from the trustees. While it may not be possible to prevent a knowledgeable attacker from beating KBSA it may be possible to prevent the attacker from infiltrating TBSA. To prevent elements such as spoofing from working, video notarization may be implemented during the vouching process along with methods of deep-fake detection. This reduces the likelihood for lazy vouching and spoofing to be effective. This even further reduces the likelihood of a knowledgeable attacker from breaking the scheme.

Another vulnerability that should be discussed is if a knowledgeable attacker is able to crack accounts of trustees and verify themselves. Since KBSA hides the trustee list, this attack focuses only on knowledgeable attackers as other attackers are unable to begin the TBSA authentication process. If a knowledgeable attacker is able to compromise enough trustee accounts it negates the use of TBSA. To do this an attacker would need to crack enough trustee accounts to gain access to a single user account. This could be prevented in ways as simply making sure each user and trustee has complex passwords on account creation and is fully aware of phishing or other social engineering methods.

Trustee or User Side

The next discussion is whether or not this should be used on the user end, trustee end, or both ends of TBSA. To do this we should look at the knowledge the person has and the security aspects of using it. Looking at this from the user end of the TBSA process, a user is responsible for initially setting their trusted users. This means a user should have knowledge to answer questions related to these trustees based on their relationship. Since multiple people are in the currently hidden trustee list, the KBSA method has a larger pool of information to create questions. This can reduce the likelihood for an attacker to have knowledge of all of the trustees and the relationships to successfully complete the authentication attempt.

Analyzing this from the trustee-side of the authentication, a trustee does not necessarily have a direct say in who they are authenticating for. This means that they may have a relationship with the user but may not have the most knowledge of the user that selected them. The trustee may also have less confidence in their ability to recall information about the user. For uses with KBSA this can be a barrier to authentication. Additionally, the trustee has less information to create questions from, due to the lack of relationships to be analyzed. To make the trustee side more plausible for implementation, a trustee can select additional users to base questions on. This increases the information pool to create questions, allowing reliability and security similar to user side implementation. This shows it is plausible to use in both the trustee and user side of authentication. Since KBSA was determined to be more advantageous to be implemented before trustee-based, it is not necessary to implement this on both user and trustee side of authentication. If implemented on the user side we reduce extra work for the trustee as well as it makes sure that the trustee will not be able to give a vouching code if an attacker can not first complete the knowledge-based portion for the user.

After analyzing the way that TBSA and KBSA interact, the best way for these two to

interact is through using KBSA before TBSA as can be seen in Figure 4.2. This prevents the release of trustee names and other information that is needed before TBSA. This reduces the information provided to attackers before attempting KBSA. KBSA can also be implemented on both the user and trustee side before they are able to interact with TBSA. While possible, it is unnecessary due to the trustee not even being notified until the user first completes their side of KBSA. This increases the security without requiring extra steps for the trustees. Reducing steps and robustness for trustees increases usability of the scheme. To prevent spoofing by knowledgeable attackers, video notarization should be used during the TBSA portion of the scheme backed by deep-fake detection methods.

4.1.3 The Design of Knowledge Verified TBSA

The final design is shown in Figure 4.2 and Figure 4.1, user and trustee interactions respectfully. The scheme begins with a typical login as seen in Figure 4.2. If a user is able to successfully login then they do not need to use the proposed fallback authentication scheme. If a user is unable to login they will be prompted to input their username to begin the fallback authentication process. After fallback authentication is initiated KBSA provides the user a series of questions based off of their social network. Figure 4.2 then shows if a user passes the KBSA method by being able to answer the majority of the questions they can begin TBSA. If unable to answer the majority of questions the authentication attempt will fail. Once TBSA has begun, a user is provided the names of their trustees and the trustees are alerted of the fallback authentication attempt. From here the design forces the user to wait until they have received three vouching codes from their trustees as shown in Figure 4.1. We can now move to Figure 4.1 to see the interaction for the trustee. We can see once a trustee receives a notification they can interact. The trustee can then contact the user via video of a third party application. This allows for a video to be monitored and to force a more secure interaction before a code can be given. As seen in Figure 4.1 the trustee can then either reject or approve the user that they are interacting with via video chat. If approved a user receives one of three codes. If rejected authentication fails. Figure 4.2 then shows that once three interactions are completed a user can be authenticated back into their account. If they can not retrieve three they will fail the authentication attempt. Using KBSA and TBSA together in the ways mentioned, allows for the creation of a novel social authentication scheme that is able to remain fully based on social connections and social knowledge.

4.2 CAPTCHA-aided TBSA

Additionally we propose the use of bot detection in conjunction with TBSA. The most effective way for a forest fire attack to be completed is through the use of a botnet [266]. A botnet takes advantage of a large scale network of bots and is able to attack a system much more efficiently, due to the amount of resources a botnet has available. To control the botnet, an attacker programs an algorithm to run on each of the separate compromised

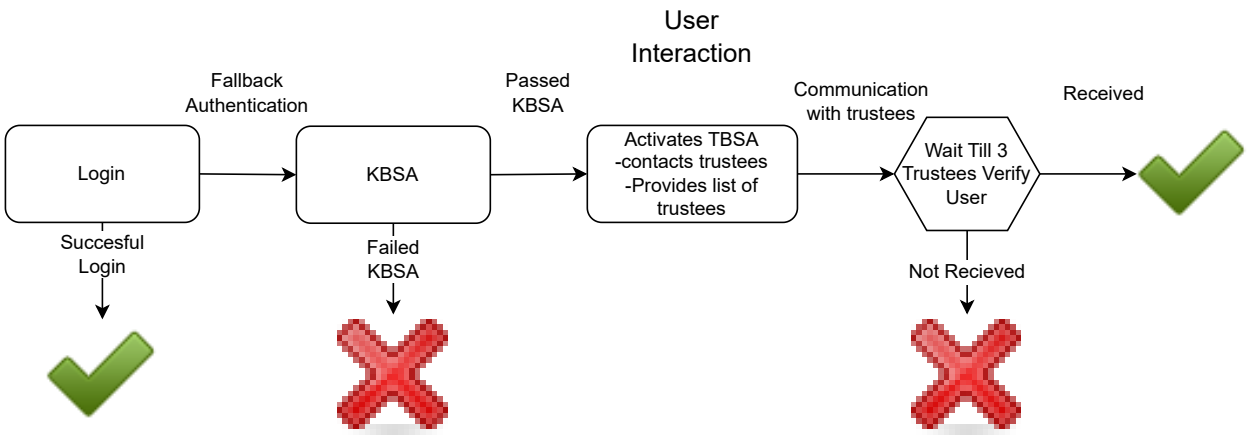

Figure 4.2: Knowledge Verified scheme design for user interaction.

systems in the network of bots. This allows for an attacker to do the work of thousands of people and machines. This makes the ability to detect bots an important tool for improving the security and privacy in TBSA.

By requiring a person to perform a modified Turing test to determine an individual is not a bot. A user must perform a task of some kind that is not able to be performed by a bot. One example of this used in our daily lives is CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart). This is different than a typical Turing test due to the fact that the judge is a computer and not a person. It was designed by von Ahn [47] in 2004 and since then has been implemented and improved by a variety of companies such as Google. There are many ways that these tests have been created. The original design has since been proven to not be secure [48]. The development of computer vision algorithms have advanced greatly since 2004. Many computer vision schemes can now accurately differentiate numbers and letters efficiently enough to solve the challenges. Many different forms of bot detection have been created to make it more difficult for AI to break them. CAPTCHAs have been designed in a variety of ways relying on different senses. The original was designed as a visual text-based task to be answered with text but there are other examples such audio, pattern recognition, and image-based. For the purposes of improving TBSA, there are two state-of-the-art methods that could be promising: Visual Turing Test (VTT) CAPTCHAs and audio adversarial CAPTCHA (aaeCAPTCHA).

4.2.1 Methods for Implementation

VTT CAPTCHAs are a form of bot detection that use the visual reasoning of an image. One of the most robust forms of this CAPTCHA has been proposed by Wang et al. [274]. VTT CAPTCHAs usually show a large group of objects at different distances, sizes, colors, and orientations. A person is then given a prompt (e.g., click the object under the letter f) that they need to complete. If completed correctly the user is allowed to continue through. Gao et al. [48] perform tests on current VTT CAPTCHAs using a novel attack that is

able to break typical questions a majority of the time. To improve the effectiveness of this CAPTCHA the authors found that their attack struggles when there are a large number of objects, an increased number of occlusions, an increased number of similar objects, and the attack has the most issues if the prompt uses common sense knowledge. Common sense prompts are things that are abstract concepts that are easily understood by humans (e.g. a mother is older than her son) but are not logically antiquated into computing. A question of such a nature is an unwritten rule understood by all humans. These types of questions accounted for 45% of the errors in the attack proposed. This shows that VTT CAPTCHAs can be promising with some improvements.

Another form that should be considered was proposed by Hossen et al. [50]. They propose a unique form of CAPTCHA called aaeCAPTCHA. To prevent the use of automatic speech recognition the scheme uses audio adversarial examples to perform as a CAPTCHA. A user must identify what is said to gain access. Through rigorous testing using state-of-the-art speech recognition technology the authors show that this improved version of audio CAPTCHAs can provide adequate bot detection. The authors conducted a user study in order to prove the usability. This is one of the most advanced audio CAPTCHA techniques currently available.

CAPTCHAs are a way for systems to prevent bots from being able to access resources or use services provided by a network. If a CAPTCHA can be used in a trustee-based system it can effectively reduce the ability of a forest fire attack to self propagate by reducing its ability to send requests to trustees, or vice versa. CAPTCHAs tend be very light tasks for true users to complete while being nearly impossible for an algorithm to solve. This makes it a viable option for reducing the effectiveness of the forest fire attack or any bot related attacks and not decrease usability.

4.2.2 How CAPTCHA Interacts

Similar to the previous section, we need to determine where and how CAPTCHA will be used. When implementing CAPTCHA into the system we need to determine the best place to introduce this in order to reduce the possibility of attacks compromising the scheme. The two places this should be considered for is on the user and on the trustee side of implementation. Additionally we will break down the flaws and benefits of using this on its own.

Trustee or User Side

CAPTCHA can be implemented very easily on either side of TBSA. That being said it should be determined if it is useful to include on both sides. Implementation on the user side of the scheme would have the goal of reducing the bot interaction with the user side of TBSA. The user side of TBSA, as discussed before, is where a user is provided a list of their trustees and the trustees are sent the vouching codes that are needed for recovery of the account. The reduction of bot interaction with the user side of authentication would prevent attacks such as the forest fire attack from being able to propagate without intervention from a human.

For mass attacks, this is an important feature of using bots. Without being able to work on a mass scale it can reduce the ability of attackers to perform effective forest fire attacks.

Implementation on the side of the trustee is another effective tool in preventing bot interaction. The trustee side of TBSA is where a trustee logs into their account and then can retrieve the vouching code to provide to the user. This once again can be a useful tool as it reduces the ability of bots to be able to interact and propagate further with the system. Given that it can be very useful in both circumstances of user and trustee side of TBSA, it could be very easily implemented in both. This makes it an effective and easily implementable tool for protection from forest fire attacks. The issue is that this does not stop a more targeted or manual attack that does not require bots. An attacker would simply need to propagate the attack by hand. This would require them to ping trustees from the users account and spoof messages to receive vouching codes from those trustees. While CAPTCHA reduces the effectiveness of the forest fire attack it does not remove the forest fire attack as a threat. We propose that CAPTCHA and TBSA should be combined with another method to further increase security.

Using this analysis we propose that this should be implemented in conjunction with other methods to prevent people from being able to target an individual as well as their trustees. One such example would be the previously proposed KBSA method. KBSA prevents all attacks on such a system where an attacker does not have knowledge of a specific user. The implementation of KBSA on the user side and use of CAPTCHA on the trustee side prevents large scale automated attacks on both fronts, user and trustee. The reason we propose to implement CAPTCHA purely on the trustee side is that it provides protection to the trustee from automated attacks without reducing the usability by such a large degree. KBSA implemented onto the trustee side would greatly increase the amount of time and size of the task required to be completed by the trustee. This increases the time a trustee must commit thereby reducing their likelihood to take time out of their day to complete.

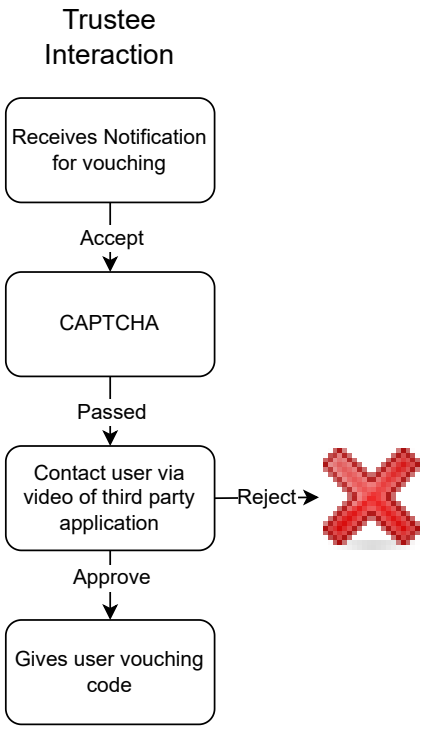

Figure 4.3: CAPTCHA-aided scheme design for trustee interaction.

4.2.3 The Design of CAPTCHA-aided TBSA

The final design for the proposed method is provided in Figure 4.4 and Figure 4.3 is one that only includes TBSA and CAPTCHA. The login process begins and is shown in Figure 4.4. A user must either login for authentication or provide username to begin fallback authentica-

tion. Figure 4.4 shows that once the username is entered
a CAPTCHA begins. This prevents a bot from interacting with the TBSA reducing the ability of mass attacks to propagate quickly. If CAPTCHA is completed successfully the user is provided the list of trustees and the trustees are alerted of the authentication attempt. If CAPTCHA is failed the authentication attempt fails as seen in Figure 4.4. We can then see in Figure 4.4 that we must wait for the user to receive three vouching codes from trustees to be authenticated. The trustee interaction begins with Figure 4.3 when the trustee receives notification of the authentication attempt. The trustee must complete a CAPTCHA, this once again stops automated attacks from happening. Once CAPTCHA is complete another video chat will be prompted by the trustee. Once again a trustee has the option to approve or reject the user. If failed the users authentication fails. If passed a user must receive two more vouching codes. Back on Figure 4.4 it is shown that if a user can attain three codes they will gain full access to their account as if they were able to login.

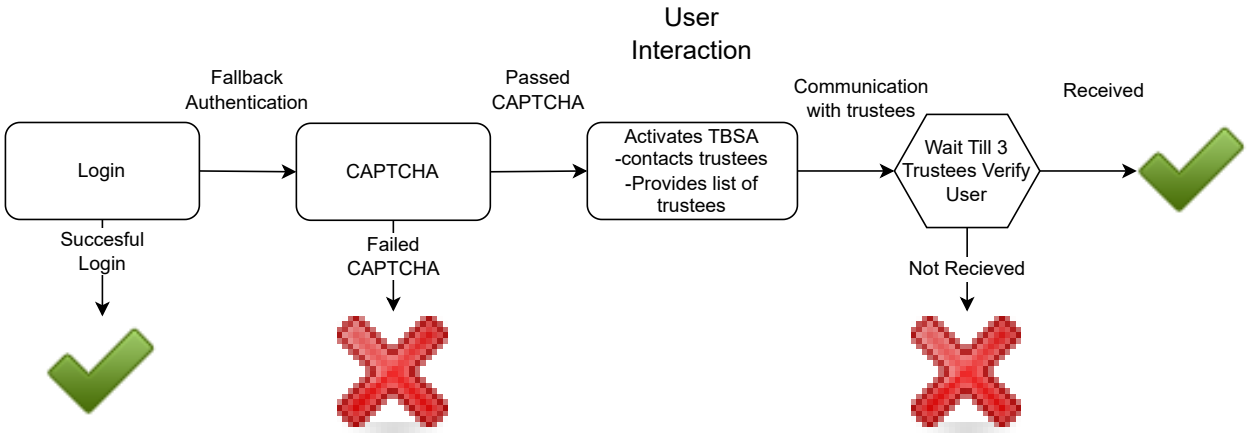

Figure 4.4: CAPTCHA-aided scheme design for user interaction.

Chapter 5

Knowledge verified CAPTCHA-aided TBSA Scheme

The schemes discussed in Chapter 3 all have design flaws that lead to them being vulnerable to attack. Using the social authentication mitigations in Chapter 3 and the proposed solutions in Chapter 4 we create a novel TBSA scheme called Knowledge verified CAPTCHA-aided TBSA. This scheme is proposed as a third party application that can be implemented into systems that require fallback authentication. This not only allows it to be secure but also scalable. The following subsections will discuss the proposed setup and design of the knowledge verified CAPTCHA-aided TBSA scheme. This Chapter is currently under review for publication.

5.1 Selecting Trustees

After an account is created or the fallback method is implemented a user must select trustees. Moderated trustee selection is essential to creating a network safe from attacks that propagate such as the forest fire attack. The first thing that needs to be discussed is the number of trustees that are needed in a network of trustees for verification. The second part of the trustee selection process will be what people can be selected as trustees. Each of these are important to creating a network of informed and reliable trustees for the verification process.

As seen in the previously mentioned schemes, there usually consists of three different trustees required for authentication. Of course, one user is not enough as it allows a malicious trustee to verify themselves into a user's account. Too many trustees needed for verification makes authentication too large of a burden. For the purposes of this scheme we plan to allow a user to select five trustees but only require three for verification. This allows for a user to have more options for verification possibly reducing the time it takes to complete. This becomes especially useful if one member of the trustee group is unavailable.

Trustee selection will be limited to those who have a low centrality. This can be calculated using the T-degree strategy proposed by the authors of [266]. The strategy can be used to alert the user to those in their network who have the lowest centrality and therefore allows

for increased security of their account. Along with this, each user will be assigned a security rating based on their password strength and security habits. Password strength should be enforced on account creation to increase security. The system can also run proactive password cracking tests on accounts to see if they are easily cracked. Security habits can be monitored through random system tests. One such example would be a fake phishing email or a fake request from the system. The more often they pass these tests the higher their rating. Lastly, over time as the system is used reliability can be tested for each trustee. If they are more likely to respond to a help request they get a higher rating. Each of these scores will be provided to the user for people already in their network to allow them to make an educated decision on trustee selection.

5.2 Design

Since this is a fallback authentication method it is only used if the user is unable to remember their password or complete any other form of primary authentication. In Figure 5.1 it is shown that a user starts the fallback authentication process and is prompted with KBSA. The scheme prompts the user with a set of five questions based on their relationship with their selected trustees, which have not yet been revealed. The questions range from last online interaction to photos of possible trustees to identify. If the user is able to get the majority correct they are given their list of trustees. During this process the trustees and user are notified of the authentication attempt through a third party application located on user's and trustees' phones as can be seen in the next steps of Figure 5.1 on the user side. The user is also given their trustee list to remind them who to contact about the authentication attempt. The use of KBSA reduces the the ability of the system to be targeted by anyone who does not have detailed knowledge of the user's interactions. This prevents targeted and non-targeted attacks alike. As stated in Chapter 2, KBSA that uses relationships to create questions is hard to crack unless an attacker has extensive knowledge of interactions. This effectively protects the the trustees from being revealed by anyone who activates the fallback authentication method. If KBSA fails, Figure 5.1 shows the authentication attempt fails.

Once the user has been notified through the third party application, they must verify that they are the ones that have made the request. If this is not done in an acceptable period of time (i.e., fifteen minutes) the authentication attempt will fail and will lock the account for a small amount of time (i.e., twelve hours). The task of verifying the request is as simple as opening their phone and selecting yes on the application. This can alert and prevent attacks early on in the authentication process. It will also notify a user that an attempt has been made on their account allowing them to take early action against attacks. Once the request is approved a user will then have to wait for trustees to contact them via video chat through the third party application on the user's phone.

On the trustee interaction side of Figure 5.1 it can be seen that a trustee receives a notification from the third party application. Figure 5.1 shows that a trustee must complete an aaeCAPTCHA in order to see who has requested verification. The aeeCAPTCHA provides a sound or a sentence that can be played multiple times. This sound that is played is cre-

ated in a way that is able to easily be recognized by people but not by a speech recognition algorithm. A user must identify what is being said in order to gain access to the verification request. This prevents a bot from being able to see requests or move through the process autonomously. Figure 5.1 then shows that once the CAPTCHA is completed a user will have the option to video chat with the user requesting the verification. The verification video chat will be an enforced one minute call. This reduces the possibility for lazy authentication. During the call both the user and trustee have the ability to stop and cancel the authentication attempt. After a minute, if the verifier is satisfied with the video chat they are able to verify the user. Deep fake detection will be used to monitor video chats in order to prevent attackers attempts to trick trustees. One such method proposed by Zi et al. [275] called 2D Attention-based Deepfake Detection Networks is a state-of-the-art method that could be used for implementation. Back on the user interaction side of Figure 5.1 a user must wait to be verified by three of their trustees. The user is then able to regain access to their account. If one verification fails the entire process fails as can be seen in Figure 5.1.

The implementation of these methods would provide a more advanced and robust approach to fallback authentication. Furthermore, the design is an improvement to TBSA that allows it to be a viable option. Our schemes employ the proposed solutions mentioned in Chapter 4 and each allows for the reduction of vulnerabilities that exist in most social authentication schemes. While our schemes are robust tasks to complete, they are necessary as to improve security. Since this is only used as fallback authentication, the benefits of having a more secure system out-weights the cons of having a more time consuming process as it should not be used that often by a single user.

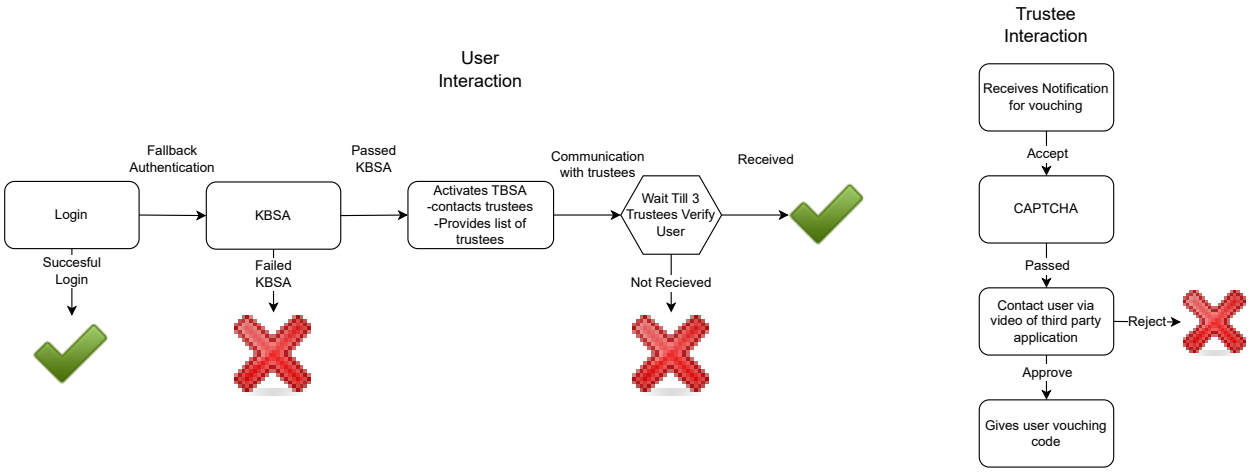

Figure 5.1: Knowledge Verified CAPTCHA-aided scheme design.

5.3 Discussion

While our scheme has applications in many different fields we feel as though the implementation of this into a social cybersecurity scheme will have even greater benefits. Furthermore,

there is a need for discussion with regards to trustee selection as it is an important part of any TBSA scheme.

5.3.1 Social Cybersecurity

A fully functional social authentication scheme has many applications in today's interconnected world. Most current security schemes focus on the individual user. An individual accesses their own account using some form of authentication. Many times in home, work, and other social environments, many people are accessing the same information and or need access to the same devices and accounts. The issue is that most of these systems are designed with an individual user in mind instead of a group. This interaction with multiple users and security protocols is called social cybersecurity.

With current security mechanisms in place people use poor practices in order to share the information they need. Users will share passwords or other forms of authentication which can negatively impact security. For example, in a home environment, multiple people all share the same password and username for a Netflix account. If someone in that trusted group decides to also share that password with a significant other the network gets larger for the rest of the group, further reducing security. The issue is that there are no checks in place with most current systems to be used securely in a social aspect. This currently applies to many devices and networks. Current standards in security need to be modified in order to take into account these social interactions.

The authors of [3] take an in-depth look at social cybersecurity, analyzing the social interactions of sharing information digitally, managing members of a social authenticated group, controlling online reputation, and helping others with security and privacy (S&P) problems. The authors further break down the categories of interaction such as relationships, family, social groups, and the public. We can use this to understand the different ways people interact to create methods that can protect accounts in a way that takes social interactions into account.

Research needs to head in a direction that allows for users to safely share the same resources. This is why we have proposed a method of fallback authentication that not only provides a more secure solution to traditional fallback but a more socially vested solution than current methods. The proposed schemes would work well within systems that rely on social cybersecurity. Questions and vouching that occurs in the proposed system can be based on the relationships and connections of the people in the shared network. This creates an entirely secure and enclosed network of users that are able to control and monitor their shared resources.

Based on [3], it does not seem any systems exist that effectively allow for social cybersecurity to be protected while not inhibiting a user's normal behavior. To do this, a scheme must be able to easily and securely authenticate a group of people for the same account, allow for effective management of members, and encourage positive S&P practices. We believe that our scheme would be ideal to be used in an environment that relies on a user's connection with the other members of their group account. This creates a purely social form of fallback authentication that has a group of people to base the information off of.

We believe the proposed schemes and solutions can be used as building blocks to creating a secure and usable system that takes into account social cybersecurity.

5.3.2 Limiting Trustee Selection

While discussing the security of TBSA it would not be possible to have a complete analysis without mentioning trustee selection. How a trustee is selected can improve the security of the system by reducing large interconnected networks of trustees that can allow attackers to vouch for many accounts. This can improve security by preventing trustees from having too many accounts to verify. If one trustee can verify many accounts it then becomes a very valuable account for attackers to compromise [266]. It has the ability to propagate a forest fire attack at much faster speeds. The authors of [266] purpose a strategy called T-Degree for the trustee selection process. T-Degree limits the centrality of nodes in the network of trusted users by reducing the number of users a trustee can vouch for. This in turn can reduce the ability of a forest fire attack to propagate. The authors believe that the ability of the forest fire attack to propagate is reduced by about two magnitudes when implementing this method. The main issue with this is it reduces the ability of a user to pick their most trusted contacts. Another aspect to be considered in trustee selection is limiting choices to users with high security rating. A security rating can be broken down into a couple of categories: password security and security habits.

Password security is something that can be inspected fairly easily and for the most part already is by most systems. One way this can be monitored is through proactive password checking run by the system administrator. This would actively attack account passwords to determine if they are weak and alert the account holder. Many schemes also have restrictions for how an account holder can set a password making it more difficult for them to choose weak passwords.

Security habits are something that is harder for a system to monitor. This can be done through occasional security tests that see how susceptible a user is to attacks such as a fake phishing or message spoofing. The more often a user passes these security test the higher their security rating is. This can then be used in determining if they would be a secure trustee.

Chapter 6

Implications of Using Knowledge verified CAPTCHA-aided TBSA in IoT

IoT devices, like any application that is able to collect and store data, is a valuable tool that can be applied to many portions of our daily lives. One such realm where this is becoming more prevalent are extensions that have applications in smart home technology. These IoT devices collect sensitive data that can be used to improve the lives of people who use them but if not properly protected can provide unauthorized access. Internet of Home devices range from security cameras, listening devices (e.g., baby monitors), Smart fridges, security systems, etc. Each of these devices could be connected to a single home owner's account. If an attacker can gain access to an account it can provide them with a plethora of information that could be used to further a malicious agenda. This is just one example as to why authentication is very important in IoT.

One of the main issues with IoT is that many of these devices are interconnected networks. A user must only pass through the first "access door" in order to gain access to all of their information which represents a controller [276]. This is convenient for users but as discussed in the previous paragraph carries dire consequences if the "access door" is breached. To prevent unauthorized access you must create an authorization scheme that can accurately determine the identity of the person authenticating. In many systems this is met with primary authentication usually in the realm of what you know (e.g., passwords, security questions, PINs), what you have (e.g., security card), or what you are (e.g. biometrics). In the case of all of these, but a security card, there needs to be a method of fallback authentication due to false rejection in biometrics and in the case of a forgotten password. This is where our proposed method of Knowledge verified CAPTCHA-aided TBSA can become an important tool. Our scheme takes on a new aspect called who you know that relies on a users social connections to provide authentication.

An "access door" is only as strong as its weakest point. If the authentication method is secure but the fallback method is not then the access door is weak. As mentioned in Chapter 1, there are currently two methods used in industry that have been proven to be insecure.

Those methods are security questions and out-of-band services. With our proposed scheme you rely purely on social connections and interactions for the purposes of authentication. Through the study of many schemes and security flaws related to these schemes we have been able to propose a design of a more secure and implementable fallback authentication.

One of the many issues and concerns of implementing anything in relation to IoT is the specific requirements of many of these devices, as well as the variations in requirements. The requirements of these devices include performance [16], Quality of Service (QoS) [17], Quality of Experience (QoE) [18], timeliness [19], reliability [20], scalability [21], fault tolerance [22], energy efficiency [23], and security. Aside from security, which is already shown in previous chapters, we must break down how our scheme design would perform in terms of each of these objectives. Since this is only a design we must make some assumptions during this process. Before this is done we shall determine the importance of each objective.

In the following we discuss the importance of each objective and how our scheme meets them.

Performance

It is important that the design works as intended. Without this the scheme is useless in any situation it is implemented into. It is hard to determine without the implementation of the scheme, how well it would perform. The referenced KBSA, CAPTCHA, and TBSA schemes each had a high level of performance when used separately. Based off of these separate components used to design our scheme we assume it would have a high level of performance.

QoS and QoE

QoS is another important objective to be implemented into this scheme. The service being provided is a fallback authentication method and the implementation of the scheme should be efficient. Along with QoS, QoE is an objective that focuses on the customer or the user interaction. It is important that the scheme is considered usable. For our proposed scheme we used many different scheme designs. One of the main portions of the design is video TBSA. In recent studies it has shown that many users would be comfortable and willing to use it in their daily lives [39]. The portions of the design including CAPTCHA and KBSA would depend on their implementation to determine their QoS and QoE.

Timeliness

Timeliness while important in many IoT devices (e.g., medical devices, security systems) is not as important in terms of a fallback authentication scheme. Since this is not the primary entry into a users account it is not used as often, making the longer time commitment of the scheme not as large of a concern. This does not mean that the fallback authentication scheme should take an excessive amount of time either. Timeliness is one area that our scheme lacks in as it is more of a time commitment than out-of-band services and security questions. In terms of time commitment users are at the mercy of the trustees responding

to their authentication requests. This delay was slightly mitigated in the design by adding additional trustees in a user's trustee list. This makes it so a user does not have to wait excessive amounts of time if one of the trustees is unavailable. They have multiple options of trustees for verification. While timeliness is not the most effective, security is much better than the alternatives.

Reliability

Reliability may be one of the most important aspects of a fallback authentication method as it is used to allow users to regain access to their account. Without reliability a user could permanently be locked out of their account. Each part of the design must be assessed for reliability. TBSA is reliable as long as a user is able to contact and retrieve vouching codes from trustees. CAPTCHA can be completed by most people. KBSA requires a user to answer questions about their interactions with people in their social network. This has been studied by the authors of [40] and shown that certain types of questions are easier for users to remember than others. In the implementation it is important to focus on these types of questions to allow for easier account recovery. With proper implementation and testing this could be a reliable method of fallback authentication.

Fault Tolerance and Energy Efficiency

Fault tolerance is not something that is as important in this system as others. Fault tolerance in IoT devices such as a pacemaker is more important as it can be life or death for a patient. Fault tolerance in connection with fallback authentication is more tied to reliability of the system as opposed to a true fault tolerance. Lastly is energy efficiency, in IoT this is important as many systems do not have access to a power source all the time. Fallback authentication on a controller does not typically have a limited access to power. This allows a scheme to be less energy efficient than other IoT devices.

Overall

After analyzing our scheme against each of these objectives it is clear that our design could be effective in the area of IoT. It meets most of the objectives presented above in an effective manner. While it may not be the most timely form of fallback authentication it is more secure than current industry standards. In the case of fallback authentication, security should be a more prominent concern as this is used as a back up in the authentication process. It should also be noted that this scheme has many uses outside of IoT as most account authentications require a form of fallback. The implementation of knowledge verified CAPTCHA-aided TBSA provides a robust and secure method of authentication that rivals any method of fallback authentication currently implemented in industry. We believe that our proposed schemes improve TBSA and allow for it to be a more viable option for future use.

Chapter 7

Conclusion

As the number of passwords people use in their daily lives increase, the need for a reliable and secure method of password recovery becomes vital. TBSA is a unique form of fallback authentication that relies on who you know instead of what you have, what you know, or who you are. In recent years there have been many designs each of which have been proven insecure through attacks such as the forest fire attack. Through the proposal of knowledge verified TBSA that incorporates CAPTCHAs, we have provided a secure method of TBSA that remains a fully social form of authentication. In this thesis, we have proposed a new scheme that could be implemented in many different environments. One such environment is IoT, as any network of IoT devices with a centralized login (i.e., Controller) can implement fallback authentication as to prevent a permanent lockout. While our proposed method may be less timely compared to other methods it provides more adequate security for the network of these sensitive devices.

One important future research direction would be to understand and analyze the parameters surrounding TBSA such as number of trustees. To study this a model of a network could be created using different parameters and have a forest fire attack performed on it. The validity of the parameters could be measured by the number of accounts compromised. Additional researcher should look into implementing this scheme into a group authentication scheme for shared accounts (i.e., social cybersecurity). Users have separate usernames and passwords but if fallback authentication is needed users in the group can re-authenticate using the fully social authentication scheme proposed above.

Bibliography

[1] Rackspace Technology Staff. World password day: Password security tips from a cybersecurity expert, May 2022.

[2] Inc Gigya. Survey guide: businesses should begin preparing for the death of the password, 2016.

[3] Yuxi Wu, W Keith Edwards, and Sauvik Das. Sok: Social cybersecurity. In *IEEE Symposium on Security and Privacy (Oakland)(2022). https://sauvikdas. com/uploads/paper/pdf/36/file. pdf*, 2022.

[4] Xiaolong Xu, Bowen Shen, Sheng Ding, Gautam Srivastava, Muhammad Bilal, Mohammad R. Khosravi, Varun G Menon, Mian Ahmad Jan, and Maoli Wang. Service offloading with deep q-network for digital twinning-empowered internet of vehicles in edge computing. *IEEE Transactions on Industrial Informatics*, 18(2):1414–1423, 2022.

[5] Prosanta Gope, Owen Millwood, and Biplab Sikdar. A scalable protocol level approach to prevent machine learning attacks on physically unclonable function based authentication mechanisms for internet of medical things. *IEEE Transactions on Industrial Informatics*, 18(3):1971–1980, 2022.

[6] Xuguang Zhang, Xin Wei, Liang Zhou, and Yi Qian. Social-content-aware scalable video streaming in internet of video things. *IEEE Internet of Things Journal*, 9(1):830–843, 2022.

[7] Muhammad Ibrar, Aamir Akbar, Syed Rooh Ullah Jan, Mian Ahmad Jan, Lei Wang, Houbing Song, and Nadir Shah. Artnet: Ai-based resource allocation and task offloading in a reconfigurable internet of vehicular networks. *IEEE Transactions on Network Science and Engineering*, 9(1):67–77, 2022.

[8] Sushil Kumar Singh, Pradip Kumar Sharma, Yi Pan, and Jong Hyuk Park. Biiovt: Blockchain-based secure storage architecture for intelligent internet of vehicular things. *IEEE Consumer Electronics Magazine (Early Access Article)*, pages 1–1, 2021.

[9] Yuanyuan Pan, Minghuan Fu, Biao Cheng, Xuefei Tao, and Jing Guo. Enhanced deep learning assisted convolutional neural network for heart disease prediction on the internet of medical things platform. *IEEE Access*, 8:189503–189512, 2020.

[10] Zhenyu Zhou, Zhao Wang, Haijun Yu, Haijun Liao, Shahid Mumtaz, Luís Oliveira, and Valerio Frascolla. Learning-based urllc-aware task offloading for internet of health things. *IEEE Journal on Selected Areas in Communications*, 39(2):396–410, 2021.

[11] Niko Mäkitalo, Daniel Flores-Martin, Javier Berrocal, José García-Alonso, Petri Ihantola, Aleksandr Ometov, Juan Manuel Murillo, and Tommi Mikkonen. The internet of bodies needs a human data model. *IEEE Internet Computing*, 24(5):28–37, 2020.

[12] Chaofeng Zhang, Mianxiong Dong, and Kaoru Ota. Deploying sdn control in internet of uavs: Q-learning-based edge scheduling. *IEEE Transactions on Network and Service Management*, 18(1):526–537, 2021.

[13] Dawei Fang, Xin Guan, Benran Hu, Yu Peng, Min Chen, and Kai Hwang. Deep reinforcement learning for scenario-based robust economic dispatch strategy in internet of energy. *IEEE Internet of Things Journal*, 8(12):9654–9663, 2021.

[14] Yue Zhang, Hequn Zhang, John Cosmas, Nawar Jawad, Kareem Ali, Ben Meunier, Adam Kapovits, Li-Ke Huang, Wei Li, Lina Shi, Xun Zhang, Jintao Wang, Israel Koffman, Muller Robert, and Charilaos C. Zarakovitis. Internet of radio and light: 5g building network radio and edge architecture. *Intelligent and Converged Networks*, 1(1):37–57, 2020.

[15] Raed Kontar, Naichen Shi, Xubo Yue, Seokhyun Chung, Eunshin Byon, Mosharaf Chowdhury, Jionghua Jin, Wissam Kontar, Neda Masoud, Maher Nouiehed, Chinedum E. Okwudire, Garvesh Raskutti, Romesh Saigal, Karandeep Singh, and Zhi-Sheng Ye. The internet of federated things (ioft). *IEEE Access*, 9:156071–156113, 2021.

[16] Guanjun Xu and Zhaohui Song. Performance analysis of a uav-assisted rf/fso relaying systems for internet of vehicles. *IEEE Internet of Things Journal (Early Access Article)*, pages 1–1, 2021.

[17] Wanying Huang, Tian Song, and Jianping An. Qa2: Qos-guaranteed access assistance for space-air-ground internet of vehicle networks. *IEEE Internet of Things Journal (Early Access Article)*, pages 1–1, 2021.

[18] Xiaoming He, Haodong Lu, Miao Du, Yingchi Mao, and Kun Wang. Qoe-based task offloading with deep reinforcement learning in edge-enabled internet of vehicles. *IEEE Transactions on Intelligent Transportation Systems (Early Access Article)*, pages 1–1, 2021.

[19] Luca Cesarano, Andrea Croce, Leandro Do Carmo Martins, Daniele Tarchi, and Angel A. Juan. A real-time energy-saving mechanism in internet of vehicles systems. *IEEE Access*, 9:157842–157858, 2021.

[20] Yuanzhi Ni, Lin Cai, Jianping He, Alexey Vinel, Yue Li, Hamed Mosavat-Jahromi, and Jianping Pan. Toward reliable and scalable internet of vehicles: Performance analysis and resource management. *Proceedings of the IEEE*, 108(2):324–340, 2020.

[21] Uzair Javaid and Biplab Sikdar. A secure and scalable framework for blockchain based edge computation offloading in social internet of vehicles. *IEEE Transactions on Vehicular Technology*, 70(5):4022–4036, 2021.

[22] Chien-Fu Cheng, Gautam Srivastava, Jerry Chun-Wei Lin, and Ying-Chen Lin. Fault-tolerance mechanisms for software-defined internet of vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 22(6):3859–3868, 2021.

[23] Umar Draz, Amjad Ali, Muhammad Bilal, Tariq Ali, Muhammad Aksam Iftikhar, Alireza Jolfaei, and Doug Young Suh. Energy efficient proactive routing scheme for enabling reliable communication in underwater internet of things. *IEEE Transactions on Network Science and Engineering*, 8(4):2934–2945, 2021.

[24] Amuleen Gulati, Gagangeet Singh Aujla, Rajat Chaudhary, Neeraj Kumar, Mohammad S. Obaidat, and Abderrahim Benslimane. Dilse: Lattice-based secure and dependable data dissemination scheme for social internet of vehicles. *IEEE Transactions on Dependable and Secure Computing*, 18(6):1–17, 2021.

[25] Rahul Saha, Gulshan Kumar, G. Geetha, Tai-Hoon-Kim, Mamoun Alazab, Reji Thomas, Mritunjay Kumar Rai, and Joel J. P. C. Rodrigues. The blockchain solution for the security of internet of energy and electric vehicle interface. *IEEE Transactions on Vehicular Technology*, 70(8):7495–7508, 2021.

[26] Bowen Wang, Yanjing Sun, Trung Q. Duong, Long D. Nguyen, and Nan Zhao. Popular matching for security-enhanced resource allocation in social internet of flying things. *IEEE Transactions on Communications*, 68(8):5087–5101, 2020.

[27] Trupil Limbasiya, Debasis Das, and Sajal K. Das. Mcomiov: Secure and energy-efficient message communication protocols for internet of vehicles. *IEEE/ACM Transactions on Networking*, 29(3):1349–1361, 2021.

[28] Lanjing Wang, Yasir Ali, Shah Nazir, and Mahmood Niazi. Isa evaluation framework for security of internet of health things system using ahp-topsis methods. *IEEE Access*, 8:152316–152332, 2020.

[29] Meiwei Kong, Jiaming Lin, Yujian Guo, Xiaobin Sun, Mohammed Sait, Omar Alkhazragi, Chun Hong Kang, Jorge A. Holguin-Lerma, Malika Kheireddine, Mustapha Ouhssain, Burton H. Jones, Tien Khee Ng, and Boon S. Ooi. Aquae-lite hybrid-solar-cell receiver-modality for energy-autonomous terrestrial and underwater internet-of-things. *IEEE Photonics Journal*, 12(4):27–41, 2020.

[30] Ahan Kak and Ian F. Akyildiz. Designing large-scale constellations for the internet of space things with cubesats. *IEEE Internet of Things Journal*, 8(3):1749–1768, 2021.

[31] Muhammad Usman, Mian Ahmad Jan, and Deepak Puthal. Paal: A framework based on authentication, aggregation, and local differential privacy for internet of multimedia things. *IEEE Internet of Things Journal*, 7(4):2501–2508, 2020.

[32] Fushan Wei, Sherali Zeadally, Pandi Vijayakumar, Neeraj Kumar, and Debiao He. An intelligent terminal based privacy-preserving multi-modal implicit authentication protocol for internet of connected vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 22(7):3939–3951, 2021.

[33] Ariel Rabkin. Personal knowledge questions for fallback authentication: Security questions in the era of facebook. In *Proceedings of the 4th Symposium on Usable Privacy and Security*, pages 13–23, 2008.

[34] John Podd, Julie Bunnell, and Ron Henderson. Cost-effective computer security: Cognitive and associative passwords. In *Proceedings Sixth Australian Conference on Computer-Human Interaction*, pages 304–305. IEEE, 1996.

[35] Joseph Bonneau, Elie Bursztein, Ilan Caron, Rob Jackson, and Mike Williamson. Secrets, lies, and account recovery: Lessons from the use of personal knowledge questions at google. In Aldo Gangemi, Stefano Leonardi, and Alessandro Panconesi, editors, *Proceedings of the 24th International Conference on World Wide Web, WWW 2015, Florence, Italy, May 18-22, 2015*, pages 141–150. ACM, 2015.

[36] John G. Brainard, Ari Juels, Ronald L. Rivest, Michael Szydlo, and Moti Yung. Fourth-factor authentication: somebody you know. In Ari Juels, Rebecca N. Wright, and Sabrina De Capitani di Vimercati, editors, *Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS 2006, Alexandria, VA, USA, October 30 - November 3, 2006*, pages 168–178. ACM, 2006.

[37] Stuart E. Schechter, Serge Egelman, and Robert W. Reeder. It's not what you know, but who you know: a social approach to last-resort authentication. In Dan R. Olsen Jr., Richard B. Arthur, Ken Hinckley, Meredith Ringel Morris, Scott E. Hudson, and Saul Greenberg, editors, *Proceedings of the 27th International Conference on Human Factors in Computing Systems, CHI 2009, Boston, MA, USA, April 4-9, 2009*, pages 1983–1992. ACM, 2009.

[38] Facebook Security. Introducing trusted contacts, 2013.

[39] Cheng Guo, Brianne Campbell, Apu Kapadia, Michael K. Reiter, and Kelly Caine. Effect of mood, location, trust, and presence of others on video-based social authentication. In Michael Bailey and Rachel Greenstadt, editors, *30th USENIX Security Symposium, USENIX Security 2021, August 11-13, 2021*, pages 1–18. USENIX Association, 2021.

[40] Sakshi Jain, Juan Lang, Neil Zhenqiang Gong, Dawn Song, Sreya Basuroy, and Prateek Mittal. New directions in social authentication. In *Proceedings of the Workshop on Usable Security*. Citeseer, 2015.

[41] Sarita Yardi, Nick Feamster, and Amy S. Bruckman. Photo-based authentication using social networks. In Christos Faloutsos, Thomas Karagiannis, and Pablo Rodriguez,

editors, *Proceedings of the first Workshop on Online Social Networks, WOSN 2008, Seattle, WA, USA, August 17-22, 2008*, pages 55–60. ACM, 2008.

[42] Andrew Dathan Frankel and Muthucumaru Maheswaran. Feasibility of a socially aware authentication scheme. In *2009 6th IEEE Consumer Communications and Networking Conference*, pages 1–6. IEEE, 2009.

[43] Yunus Durmus and Koen Langendoen. WIFI authentication through social networks—a decentralized and context-aware approach. In *2014 IEEE International Conference on Pervasive Computing and Communication Workshops (PERCOM WORKSHOPS)*, pages 532–538. IEEE, 2014.

[44] Yinglian Xie, Fang Yu, Qifa Ke, Martín Abadi, Eliot Gillum, Krish Vitaldevaria, Jason Walter, Junxian Huang, and Zhuoqing Morley Mao. Innocent by association: early recognition of legitimate users. In *Proceedings of the 2012 ACM conference on Computer and communications security*, pages 353–364, 2012.

[45] Hyoungshick Kim, John Kit Tang, and Ross J. Anderson. Social authentication: Harder than it looks. In Angelos D. Keromytis, editor, *Financial Cryptography and Data Security - 16th International Conference, FC 2012, Kralendijk, Bonaire, Februray 27-March 2, 2012, Revised Selected Papers*, volume 7397 of *Lecture Notes in Computer Science*, pages 1–15. Springer, 2012.

[46] Iasonas Polakis, Marco Lancini, Georgios Kontaxis, Federico Maggi, Sotiris Ioannidis, Angelos D. Keromytis, and Stefano Zanero. All your face are belong to us: breaking facebook's social authentication. In Robert H'obbes' Zakon, editor, *28th Annual Computer Security Applications Conference, ACSAC 2012, Orlando, FL, USA, 3-7 December 2012*, pages 399–408. ACM, 2012.

[47] Luis von Ahn, Manuel Blum, and John Langford. Telling humans and computers apart automatically. *Communications of the ACM*, 47(2):56–60, 2004.

[48] Yipeng Gao, Haichang Gao, Sainan luo, Yang Zi, Shudong Zhang, Wenjie Mao, Ping Wang, Yulong Shen, and Jeff Yan. Research on the security of visual reasoning CAPTCHA. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 3291–3308. USENIX Association, August 2021.

[49] Google recaptcha website. `https://developers.google.com/recaptcha/docs/versions`. Accessed: 2022-07-19.

[50] Imran Hossen and Xiali Hei. aaecaptcha: The design and implementation of audio adversarial captcha. In *2022 IEEE 7th European Symposium on Security and Privacy (EuroS&P)*, pages 430–447, 2022.

[51] Abdul Salam and Usman Raza. Current advances in internet of underground things. In Abdul Salam and Usman Raza, editors, *Signals in the Soil*, pages 321–356. Springer, 2020.

[52] Debjani Ghosh;Akash Anand;Satya Sankalp Gautam;Ankit Vidyarthi. Soil fertility monitoring with internet of underground things: A survey. *IEEE Micro*, 42(1):8–16, 2022.

[53] Abdulkadir Celik, Khaled N. Salama, and Ahmed M. Eltawil. The internet of bodies: A systematic survey on propagation characterization and channel modeling. *IEEE Internet of Things Journal*, 9(1):321–345, 2022.

[54] Luca Turchet, György Fazekas, Mathieu Lagrange, Hossein S. Ghadikolaei, and Carlo Fischione. The internet of audio things: State of the art, vision, and challenges. *IEEE Internet of Things Journal*, 7(10):10233–10249, 2020.

[55] Guojie Yang, Mian Ahmad Jan, Ateeq Ur Rehman, Muhammad Babar, Mian Muhammad Aimal, and Sahil Verma. Interoperability and data storage in internet of multimedia things: Investigating current trends, research challenges and future directions. *IEEE Access*, 8:124382–124401, 2020.

[56] Tan Li, Congduan Li, Jingjing Luo, and Linqi Song. Wireless recommendations for internet of vehicles: Recent advances, challenges, and opportunities. *Intelligent and Converged Networks*, 1(1):1–17, 2020.

[57] Eugen Borcoci, Ana-Maria Drăgulinescu, Frank Y. Li, Marius-Constantin Vochin, and Kjetil Kjellstadli. An overview of 5g slicing operational business models for internet of vehicles, maritime iot applications and connectivity solutions. *IEEE Access*, 9:156624–156646, 2021.

[58] Carlos Renato Storck and Fátima Duarte-Figueiredo. A survey of 5g technology evolution, standards, and infrastructure associated with vehicle-to-everything communications by internet of vehicles. *IEEE Access*, 8:117593–117614, 2020.

[59] Haibo Zhou, Wenchao Xu, Jiacheng Chen, and Wei Wang. Evolutionary v2x technologies toward the internet of vehicles: Challenges and opportunities. *Proceedings of the IEEE*, 108(2):308–323, 2020.

[60] Kayhan Zrar Ghafoor, Linghe Kong, Sherali Zeadally, Ali Safaa Sadiq, Gregory Epiphaniou, Mohammad Hammoudeh, Ali Kashif Bashir, and Shahid Mumtaz. Millimeter-wave communication for internet of vehicles: Status, challenges, and perspectives. *IEEE Internet of Things Journal*, 7(9):8525–8546, 2020.

[61] Muhammad Baqer Mollah, Jun Zhao, Dusit Niyato, Yong Liang Guan, Chau Yuen, Sumei Sun, Kwok-Yan Lam, and Leong Hai Koh. Blockchain for the internet of vehicles towards intelligent transportation systems: A survey. *IEEE Internet of Things Journal*, 8(6):4157–4185, 2021.

[62] Kashif Naseer Qureshi, Sadia Din, Gwanggil Jeon, and Francesco Piccialli. Internet of vehicles: Key technologies, network model, solutions and challenges with future

aspects. *IEEE Transactions on Intelligent Transportation Systems*, 22(3):1777–1786, 2021.

[63] Sameer Qazi, Farah Sabir, Bilal A. Khawaja, Syed Muhammad Atif, and Muhammad Mustaqim. Why is internet of autonomous vehicles not as plug and play as we think ? lessons to be learnt from present internet and future directions. *IEEE Access*, 8:133015–133033, 2020.

[64] Kefeng Wei, Lincong Zhang, Yi Guo, and Xin Jiang. Health monitoring based on internet of medical things: Architecture, enabling technologies, and applications. *IEEE Access*, 8:27468–27478, 2020.

[65] Waleed Bin Qaim, Aleksandr Ometov, Antonella Molinaro, Ilaria Lener, Claudia Campolo, Elena Simona Lohan, and Jari Nurmi. Towards energy efficiency in the internet of wearable things: A systematic review. *IEEE Access*, 8:175412–175435, 2020.

[66] Pijush Kanti Dutta Pramanik, Arun Solanki, Abhinaba Debnath, Anand Nayyar, Shaker El-Sappagh, and Kyung-Sup Kwak. Advancing modern healthcare with nanotechnology, nanobiosensors, and internet of nano things: Taxonomies, applications, architecture, and challenges. *IEEE Access*, 8:65230–65266, 2020.

[67] Areej Omar Balghusoon and Saoucene Mahfoudh. Routing protocols for wireless nanosensor networks and internet of nano things: A comprehensive survey. *IEEE Access*, 8:200724–200748, 2020.

[68] Tie Qiu, Zhao Zhao, Tong Zhang, Chen Chen, and C. L. Philip Chen. Underwater internet of things in smart ocean: System architecture and open issues. *IEEE Transactions on Industrial Informatics*, 16(7):4297–4307, 2020.

[69] Mohammad Jahanbakht, Wei Xiang, Lajos Hanzo, and Mostafa Rahimi Azghadi. Internet of underwater things and big marine data analytics—a comprehensive survey. *IEEE Communications Surveys & Tutorials*, 23(2):904–956, 2021.

[70] Sheraz Aslam, Michalis P. Michaelides, and Herodotos Herodotou. Internet of ships: A survey on architectures, emerging applications, and challenges. *IEEE Internet of Things Journal*, 7(10):9714–9727, 2020.

[71] Seng W. Loke Jonathan Kua and, Chetan Arora, Niroshinie Fernando, and Chathurika Ranaweera. Internet of things in space: A review of opportunities and challenges from satellite-aided computing to digitally-enhanced space living. *Sensors*, 21(1):1–33, 2021.

[72] Laith Abualigah, Ali Diabat, Putra Sumari, and Amir H. Gandomi. Applications, deployments, and integration of internet of drones (iod): A review. *IEEE Sensors Journal*, 21(22):25532–25546, 2021.

[73] Huansheng Ning, Feifei Shi, Shan Cui, and Mahmoud Daneshmand. From iot to future cyber-enabled internet of x and its fundamental issues. *IEEE Internet of Things Journal*, 8(7):6077–6088, 2021.

[74] Xiaofan Jia, Ling Xing, Jianping Gao, and Honghai Wu. A survey of location privacy preservation in social internet of vehicles. *IEEE Access*, 8, 2020.

[75] Diana Pamela Moya Osorio, Ijaz Ahmad, José David Vega Sánchez, Andrei Gurtov, Johan Scholliers, Matti Kutila, and Pawani Porambage. Towards 6g-enabled internet of vehicles: Security and privacy. *IEEE Open Journal of the Communications Society*, 3(1):82–105, 2022.

[76] Palak Bagga, Ashok Kumar Das, Mohammad Wazid, Joel J. P. C. Rodrigues, and Youngho Park. Authentication protocols in internet of vehicles: Taxonomy, analysis, and challenges. *IEEE Access*, 8:54314–54344, 2020.

[77] Ali Ghubaish, Tara Salman, Maede Zolanvari, Devrim Unal, Abdulla Al-Ali, and Raj Jain. Recent advances in the internet-of-medical-things (iomt) systems security. *IEEE Internet of Things Journal*, 8(11):8707–8718, 2021.

[78] Vangelis Malamas, Fotis Chantzis, Thomas K. Dasaklis, George Stergiopoulos, Panayiotis Kotzanikolaou, and Christos Douligeris. Risk assessment methodologies for the internet of medical things: A survey and comparative appraisal. *IEEE Access*, 9:40049–40075, 2021.

[79] Mohammad Wazid, Ashok Kumar Das, Sachin Shetty, and Minho Jo. A tutorial and future research for building a blockchain-based secure communication scheme for internet of intelligent things. *IEEE Access*, 8:88700–88716, 2020.

[80] Muktar Yahuza, Mohd Yamani Idna Idris, Ismail Bin Ahmedy, Ainuddin Wahid Abdul Wahab, Tarak Nandy, Noorzaily Mohamed Noor, and Abubakar Bala. Internet of drones security and privacy issues: Taxonomy and open challenges. *IEEE Access*, 9:57243–57270, 2021.

[81] Sidra Zafar, Mohsin Nazir, Taimur Bakhshi, Hasan Ali Khattak, Sarmadullah Khan, Muhammad Bilal, Kim-Kwang Raymond Choo, Kyung-Sup Kwak, and Aneeqa Sabah. A systematic review of bio-cyber interface technologies and security issues for internet of bio-nano things. *IEEE Access*, 9:93529–93566, 2021.

[82] Lanfang Sun, Xin Jiang, Huixia Ren, and Yi Guo. Edge-cloud computing and artificial intelligence in internet of medical things: Architecture, technology and application. *IEEE Access*, 8:101079–101092, 2020.

[83] Xiaolong Xu, Haoyuan Li, Weijie Xu, Zhongjian Liu, Liang Yao, and Fei Dai. Artificial intelligence for edge service optimization in internet of vehicles: A survey. *Tsinghua Science and Technology*, 27(2):270–287, 2022.

[84] Nasir Saeed, Mohamed-Slim Alouini, and Tareq Y. Al-Naffouri. 3d localization for internet of underground things in oil and gas reservoirs. *IEEE Access*, 7:121769–121780, 2019.

[85] Sudip Misra, Minu Tiwari, Tamoghna Ojha, and Yash Raj. Panda: Preference-based bandwidth allocation in fog-enabled internet of underground-mine things. *IEEE Systems Journal*, 15(4):5144–5151, 2021.

[86] Chunyan Guo, Jiabing Zhang, Yang Liu, Yaying Xie, Zhiqiang Han, and Jianshe Yu. Recursion enhanced random forest with an improved linear model (rerf-ilm) for heart disease detection on the internet of medical things platform. *IEEE Access*, 8:59247–59256, 2020.

[87] Zhongyu Wang, Hongbin Sun, Dong Zhao, and Tiechao Jiang. Convolution denoising regularized auto encoder stacked method for coronary acute syndrome in internet of medical things platform. *IEEE Access*, 8:57389–57399, 2020.

[88] Junxin Chen, Shuang Sun, Li bo Zhang, Benqiang Yang, and Wei Wang. Compressed sensing framework for heart sound acquisition in internet of medical things. *IEEE Transactions on Industrial Informatics*, 18(3):2000–2009, 2022.

[89] Berken Utku Demirel, Islam Abdelsalam Bayoumy, and Mohammad Abdullah Al Faruque. Energy-efficient real-time heart monitoring on edge-fog-cloud internet-of-medical-things. *IEEE Internet of Things Journal (Early Access Article)*, pages 1–1, 2021.

[90] Md. Nazmul Hossen, Vijayakumari Panneerselvam, Deepika Koundal, Kawsar Ahmed, Francis M. Bui, and Sobhy M. Ibrahim. Federated machine learning for detection of skin diseases and enhancement of internet of medical things (iomt) security. *IEEE Journal of Biomedical and Health Informatics (Early Access Article)*, pages 1–1, 2022.

[91] Yu Qiu, Haijun Zhang, and Keping Long. Computation offloading and wireless resource management for healthcare monitoring in fog-computing-based internet of medical things. *IEEE Internet of Things Journal*, 8(21):15875–15883, 2021.

[92] Tao Zhang, Minjie Liu, Tian Yuan, and Najla Al-Nabhan. Emotion-aware and intelligent internet of medical things toward emotion recognition during covid-19 pandemic. *IEEE Internet of Things Journal*, 8(21):16002–16013, 2021.

[93] Weizhi Meng, Yong Cai, Laurence T. Yang, and Wei-Yang Chiu. Hybrid emotion-aware monitoring system based on brainwaves for internet of medical things. *IEEE Internet of Things Journal*, 8(21):16014–16022, 2021.

[94] Based Gautschi Model–A Numerical Approach. Internet of medical things (iomt) assisted vertebral tumor prediction using heuristic hock transformation. *IEEE Access*, 8:17299–17309, 2020.

[95] Jie Chen, Xiaoxiao Song, Zhichao Huang, Jianqiang Li, Zhaoxia Wang, Chengwen Luo, and Fei Yu. On-site colonoscopy auto-diagnosis using smart internet of medical things. *IEEE Internet of Things Journal (Early Access Article)*, pages 1–1, 2021.

[96] Zhiwei Guo, Yu Shen, Shaohua Wan, Wenlong Shang, and Keping Yu. Hybrid intelligence-driven medical image recognition for remote patient diagnosis in internet of medical things. *IEEE Journal of Biomedical and Health Informatics (Early Access Article)*, pages 1–1, 2021.

[97] Hao Wang, Shuai Ding, Shanlin Yang, Chenguang Liu, Shui Yu, and Xi Zheng. Guided activity prediction for minimally invasive surgery safety improvement in the internet of medical things. *IEEE Internet of Things Journal (Early Access Article)*, pages 1–1, 2021.

[98] Bhaskara S. Egala, Ashok K. Pradhan, Venkataramana Badarla, and Saraju P. Mohanty. Fortified-chain: A blockchain-based framework for security and privacy-assured internet of medical things with effective access control. *IEEE Internet of Things Journal*, 8(14):11717–11731, 2021.

[99] Shupeng Wang, Guangjun Wu, Zhaolong Ning, and Jun Li. Blockchain enabled privacy preserving access control for data publishing and sharing in the internet of medical things. *IEEE Internet of Things Journal (Early Access Article)*, pages 1–1, 2021.

[100] Bin Xie, Tao Xiang, Xiaofeng Liao, and Jiahui Wu. Achieving privacy-preserving online diagnosis with outsourced svm in internet of medical things environment. *IEEE Transactions on Dependable and Secure Computing (Early Access Article)*, pages 1–1, 2021.

[101] Xiuqing Lu and Xiangguo Cheng. A secure and lightweight data sharing scheme for internet of medical things. *IEEE Access*, 8:5022–5030, 2020.

[102] Liu Yang, Keping Yu, Simon Xianyi Yang, Chinmay Chakraborty, Yinzhi Lu, and Tan Guo. An intelligent trust cloud management method for secure clustering in 5g enabled internet of medical things. *IEEE Transactions on Industrial Informatics (Early Access Article)*, pages 1–1, 2021.

[103] Hui Lin, Sahil Garg, Jia Hu, Xiaoding Wang, Md. Jalil Piran, and M. Shamim Hossain. Privacy-enhanced data fusion for covid-19 applications in intelligent internet of medical things. *IEEE Internet of Things Journal*, 8(21):15683–15693, 2021.

[104] Ahmad Almogren, Irfan Mohiuddin, Ikram Ud Din, Hisham Almajed, and Nadra Guizani. Ftm-iomt: Fuzzy-based trust management for preventing sybil attacks in internet of medical things. *IEEE Internet of Things Journal*, 8(6):4485–4497, 2021.

[105] Tian-Fu Lee, Xiucai Ye, and Syuan-Han Lin. Anonymous dynamic group authenticated key agreements using physical unclonable functions for internet of medical things. *IEEE Internet of Things Journal (Early Access Article)*, pages 1–1, 2022.

[106] S. Manimurugan, Saad Al-Mutairi, Majed Mohammed Aborokbah, Naveen Chilamkurti, Subramaniam Ganesan, and Rizwan Patan. Effective attack detection in internet of medical things smart environment using a deep belief neural network. *IEEE Access*, 8:77396–77404, 2020.

[107] Osman Salem, Khalid Alsubhi, Aymen Shaafi, Mostafa Gheryani, Ahmed Mehaoua, and Raouf Boutaba. Man-in-the-middle attack mitigation in internet of medical things. *IEEE Transactions on Industrial Informatics*, 18(3):2053–2062, 2022.

[108] B. D. Deebak and Fadi Al-Turjman. Smart mutual authentication protocol for cloud based medical healthcare systems using internet of medical things. *IEEE Journal on Selected Areas in Communications*, 39(2):346–360, 2021.

[109] Shin-Yan Chiou, Zhaoqin Ying, and Junqiang Liu. Improvement of a privacy authentication scheme based on cloud for medical environment. *Journal of medical systems*, 40(4):1–15, 2016.

[110] Jiliang Li, Zhou Su, Deke Guo, Kim-Kwang Raymond Choo, and Yusheng Ji. Pslmaaka: Provably secure and lightweight mutual authentication and key agreement protocol for fully public channels in internet of medical things. *IEEE Internet of Things Journal*, 8(17):13183–13195, 2021.

[111] Rifaqat Ali, Arup Kumar Pal, Saru Kumari, Marimuthu Karuppiah, and Mauro Conti. A secure user authentication and key-agreement scheme using wireless sensor networks for agriculture monitoring. *Future Generation Computer Systems*, 84:200–215, 2018.

[112] Mahdi Fotouhi, Majid Bayat, Ashok Kumar Das, Hossein Abdi Nasib Far, S Morteza Pournaghi, and Mohammad-Ali Doostari. A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care iot. *Computer Networks*, 177:107333, 2020.

[113] Chin-Chen Chang and Hai-Duong Le. A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks. *IEEE Transactions on wireless communications*, 15(1):357–366, 2015.

[114] Saru Kumari, Xiong Li, Fan Wu, Ashok Kumar Das, Hamed Arshad, and Muhammad Khurram Khan. A user friendly mutual authentication and key agreement scheme for wireless sensor networks using chaotic maps. *Future Generation Computer Systems*, 63:56–75, 2016.

[115] Jiangfeng Sun, Fazlullah Khan, Junxia Li, Mohammad Dahman Alshehri, Ryan Alturki, and Mohammad Wedyan. Mutual authentication scheme for the device-to-server communication in the internet of medical things. *IEEE Internet of Things Journal*, 8(21):15663–15671, 2021.

[116] Shabir A. Parah, Javaid A. Kaw, Paolo Bellavista, Nazir A. Loan, G. M. Bhat, Khan Muhammad, and Victor Hugo C. de Albuquerque. Efficient security and authentication for edge-based internet of medical things. *IEEE Internet of Things Journal*, 8(21):15652–15662, 2021.

[117] Senthil Murugan Nagarajan, Ganesh Gopal Deverajan, Kumaran U, Thirunavukkarasan M, Mohammad Dahman Alshehri, and Salem Alkhalaf. Secure data transmission in internet of medical things using res-256 algorithm. *IEEE Transactions on Industrial Informatics (Early Access Article)*, pages 1–1, 2021.

[118] Neha Garg, Mohammad Wazid, Ashok Kumar Das, Devesh Pratap Singh, Joel J. P. C. Rodrigues, and Youngho Park. Bakmp-iomt: Design of blockchain enabled authenticated key management protocol for internet of medical things deployment. *IEEE Access*, 8:95956–95977, 2020.

[119] Mehedi Masud, Gurjot Singh Gaba, Salman Alqahtani, Ghulam Muhammad, B. B. Gupta, Pardeep Kumar, and Ahmed Ghoneim. A lightweight and robust secure key establishment protocol for internet of medical things in covid-19 patients care. *IEEE Internet of Things Journal*, 8(21):15694–15703, 2021.

[120] Meriske Chen and Tian-Fu Lee. Anonymous group-oriented time-bound key agreement for internet of medical things in telemonitoring using chaotic maps. *IEEE Internet of Things Journal*, 8(18):13939–13949, 2021.

[121] Peng Zeng, Zhiting Zhang, Rongxing Lu, and Kim-Kwang Raymond Choo. Efficient policy-hiding and large universe attribute-based encryption with public traceability for internet of medical things. *IEEE Internet of Things Journal*, 8(13):10963–10972, 2021.

[122] Mohammad Kamrul Hasan, Shayla Islam, Rossilawati Sulaiman, Sheroz Khan, Aisha-Hassan Abdalla Hashim, Shabana Habib, Mohammad Islam, Saleh Alyahya, Musse Mohamed Ahmed, Samar Kamil, and Md Arif Hassan. Lightweight encryption technique to enhance medical image security on internet of medical things applications. *IEEE Access*, 9:47731–7742, 2021.

[123] Mahender Kumar and Satish Chand. A secure and efficient cloud-centric internet-of-medical-things-enabled smart healthcare system with public verifiability. *IEEE Internet of Things Journal*, 7(10):10650–10659, 2020.

[124] Geethapriya Thamilarasu, Adedayo Odesile, and Andrew Hoang. An intrusion detection system for internet of medical things. *IEEE Access*, 8:181560–181576, 2020.

[125] Tuan Anh Nguyen, Dugki Min, Eunmi Choi, and Jae-Woo Lee. Dependability and security quantification of an internet of medical things infrastructure based on cloud-fog-edge continuum for healthcare monitoring using hierarchical models. *IEEE Internet of Things Journal*, 8(21):15704–15748, 2021.

[126] G. Enrico Santagati, Neil Dave, and Tommaso Melodia. Design and performance evaluation of an implantable ultrasonic networking platform for the internet of medical things. *IEEE/ACM Transactions on Networking*, 28(1):29–42, 2020.

[127] Kristtopher Kayo Coelho, Michele Nogueira, Mateus Coutinho Marim, Edelberto Franco Silva, Alex Borges Vieira, and José Augusto M. Nacif. Lorena: Low memory symmetric-key generation method for based on group cryptography protocol applied to the internet of healthcare things. *IEEE Access*, 10:12564–12579, 2022.

[128] Noor Munir, Majid Khan, Mohammad Mazyad Hazzazi, Amer Aljaedi, Abd Al Karim Haj Ismail, Adel R. Alharbi, and Iqtadar Hussain. Cryptanalysis of internet of health things encryption scheme based on chaotic maps. *IEEE Access*, 9:105678–105685, 2021.

[129] Nestor Tsafack, Syam Sankar, Bassem Abd-El-Atty, Jacques Kengne, Jithin K. C., Akram Belazi, Irfan Mehmood, Ali Kashif Bashir, Oh-Young Song, and Ahmed A. Abd El-Latif. A new chaotic map with dynamic analysis and encryption application in internet of health things. *IEEE Access*, 8:137731–137744, 2020.

[130] Claude E Shannon. Communication theory of secrecy systems. *The Bell system technical journal*, 28(4):656–715, 1949.

[131] Bassam Aboushosha, Rabie A. Ramadan, Ashutosh Dhar Dwivedi, Ayman El-Sayed, and Mohamed M. Dessouky. Slim: A lightweight block cipher for internet of health things. *IEEE Access*, 8:203747–203757, 2020.

[132] Hang Li, Keping Yu, Bin Liu, Chaosheng Feng, Zhiguang Qin, and Gautam Srivastava. An efficient ciphertext-policy weighted attribute-based encryption for the internet of health things. *IEEE Journal of Biomedical and Health Informatics (Early Access Article)*, pages 1–1, 2021.

[133] Hsiao-Ying Lin and Wen-Guey Tzeng. An efficient solution to the millionaires' problem based on homomorphic encryption. In *International Conference on Applied Cryptography and Network Security*, pages 456–466. Springer, 2005.

[134] Insaf Ullah, Ali Alkhalifah, Sajjad Ur Rehman, Neeraj Kumar, and Muhammad Asghar Khan. An anonymous certificateless signcryption scheme for internet of health things. *IEEE Access*, 9:101207–101216, 2021.

[135] Mohamed Abdur Rahman, M. Shamim Hossain, Mohammad Saiful Islam, Nabil A. Alrajeh, and Ghulam Muhammad. Secure and provenance enhanced internet of health things framework: A blockchain managed federated learning approach. *IEEE Access*, 8:205071–205087, 2020.

[136] Francisco Airton Silva, Tuan Anh Nguyen, Iure Fé, Carlos Brito, Dugki Min, and Jae-Woo Lee. Performance evaluation of an internet of healthcare things for medical monitoring using m/m/c/k queuing models. *IEEE Access*, 9:55271–55283, 2021.

[137] Long Qin and Yinming Xie. Real-time monitoring system of exercise status based on internet of health things using safety architecture model. *IEEE Access*, 9:27333–27345, 2021.

[138] Umer F. Abbasi, Noman Haider, Azlan Awang, and Komal S. Khan. Cross-layer mac/routing protocol for reliable communication in internet of health things. *IEEE Open Journal of the Communications Society*, 2(1):199–216, 2021.

[139] Abdulkadir Celik and Ahmed M. Eltawil. Enabling the internet of bodies through capacitive body channel access schemes. *IEEE Internet of Things Journal (Early Access Article)*, pages 1–1, 2021.

[140] Muhammad Ali, Yifan Chen, and Michael J. Cree. Autonomous in vivo computation in internet-of-nano-bio-things. *IEEE Internet of Things Journal (Early Access Article)*, pages 1–1, 2021.

[141] Maheshi B. Dissanayake and N. Ekanayake. On the exact performance analysis of molecular communication via diffusion for internet of bio-nano things. *IEEE Transactions on NanoBioscience*, 20(3):291–295, 2021.

[142] Ian F. Akyildiz, Maysam Ghovanloo, Ulkuhan Guler, Tevhide Ozkaya-Ahmadov, A. Fatih Sarioglu, and Bige D. Unluturk. Panacea: An internet of bio-nanothings application for early detection and mitigation of infectious diseases. *IEEE Access*, 8:140512–140523, 2020.

[143] Liangtian Wan, Lu Sun, Kaihui Liu, Xianpeng Wang, Qingqing Lin, and Tong Zhu. Autonomous vehicle source enumeration exploiting non-cooperative uav in software defined internet of vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 22(6):3603–3615, 2021.

[144] Liangtian Wan, Lu Sun, Kaihui Liu, Xianpeng Wang, Qingqing Lin, and Tong Zhu. Autonomous vehicle source enumeration exploiting non-cooperative uav in software defined internet of vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 22(6):3603–3615, 2021.

[145] Neetesh Kumar, Rashmi Chaudhry, Omprakash Kaiwartya, Neeraj Kumar, and Syed Hassan Ahmed. Green computing in software defined social internet of vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 22(6):3644–3653, 2021.

[146] Chuan Lin, Guangjie Han, Jiaxin Du, Tiantian Xu, and Yan Peng. Adaptive traffic engineering based on active network measurement towards software defined internet of vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 22(6):3697–3706, 2021.

[147] Jianbin Gao, Kwame Opuni-Boachie Obour Agyekum, Emmanuel Boateng Sifah, Kingsley Nketia Acheampong, Qi Xia, Xiaojiang Du, Mohsen Guizani, and Hu Xia.

A blockchain-sdn-enabled internet of vehicles environment for fog computing and 5g networks. *IEEE Internet of Things Journal*, 7(5):4278–4291, 2020.

[148] Shiva Raj Pokhrel. Software defined internet of vehicles for automation and orchestration. *IEEE Transactions on Intelligent Transportation Systems*, 22(6):3890–3899, 2021.

[149] Bingpeng Zhou, An Liu, Vincent Lau, Jinming Wen, Shahid Mumtaz, Ali Kashif Bashir, and Syed Hassan Ahmed. Performance limits of visible light-based positioning for internet-of-vehicles: Time-domain localization cooperation gain. *IEEE Transactions on Intelligent Transportation Systems*, 22(8):5374–5388, 2021.

[150] Le Doan Hoang, Phuc Viet Trinh, Thanh V. Pham, Dimitar Kolev, Carrasco-Casado Alberto, Kubo-OKA Toshihiro, Morio Toyoshima, and Anh T. Pham. Throughput analysis for tcp over the fso-based satellite-assisted internet of vehicles. *IEEE Transactions on Vehicular Technology (Early Access Article)*, pages 1–1, 2021.

[151] Shanchen Pang, Nuanlai Wang, Min Wang, Sibo Qiao, Xue Zhai, and Neal N. Xiong. A smart network resource management system for high mobility edge computing in 5g internet of vehicles. *IEEE Transactions on Network Science and Engineering*, 8(4):3179–3191, 2021.

[152] Trupil Limbasiya and Debasis Das. Iovcom: Reliable comprehensive communication system for internet of vehicles. *IEEE Transactions on Dependable and Secure Computing*, 18(6):2752–2766, 2021.

[153] Yaping Cui, Xinyun Huang, Peng He, Dapeng Wu, and Ruyan Wang. Qos guaranteed network slicing orchestration for internet of vehicles. *IEEE Internet of Things Journal (Early Access Article)*, pages 1–1, 2022.

[154] Lingwei Xu, Xinpeng Zhou, Mohammad Ayoub Khan, Xingwang Li, Varun G Menon, and Xu Yu. Communication quality prediction for internet of vehicle (iov) networks: An elman approach. *IEEE Transactions on Intelligent Transportation Systems (Early Access Article)*, pages 1–1, 2021.

[155] Rateb Jabbar, Noora Fetais, Mohamed Kharbeche, Moez Krichen, Kamel Barkaoui, and Mohammed Shinoy. Blockchain for the internet of vehicles: How to use blockchain to secure vehicle-to-everything (v2x) communication and payment*. *IEEE Sensors Journal*, 21(14):15807–15823, 2021.

[156] Ashutosh Sharma and Neeraj Kumar. Third eye: An intelligent and secure route planning scheme for critical services provisions in internet of vehicles environment. *IEEE Systems Journal (Early Access Article)*, pages 1–1, 2021.

[157] Rongbo Zhu, Hao Liu, Xiaozhu Liu, Shaohua Wan, and Wenjie Hu. Contract-theory-based secure spectrum sharing framework in internet of vehicles. *IEEE Consumer Electronics Magazine (Early Access Article)*, pages 1–1, 2021.

[158] Leila Benarous, Salim Bitam, and Abdelhamid Mellouk. Cslpps: Concerted silence-based location privacy preserving scheme for internet of vehicles. *IEEE Transactions on Vehicular Technology*, 70(7):7153–7160, 2021.

[159] Ling Xing, Xiaofan Jia, Jianping Gao, and Honghai Wu. A location privacy protection algorithm based on double k-anonymity in the social internet of vehicles. *IEEE Communications Letters*, 25(10):3199–3203, 2021.

[160] Jiaqi Huang, Yi Qian, and Rose Qingyang Hu. A privacy-preserving scheme for location-based services in the internet of vehicles. *Journal of Communications and Information Networks*, 6(4):385–395, 2021.

[161] Xinghua Li, Yanbing Ren, Laurence T. Yang, Ning Zhang, Bin Luo, Jian Weng, and Ximeng Liu. Perturbation-hidden: Enhancement of vehicular privacy for location-based services in internet of vehicles. *IEEE Transactions on Network Science and Engineering*, 8(3):2073–2086, 2021.

[162] Wenjuan Zhang and Gang Li. An efficient and secure data transmission mechanism for internet of vehicles considering privacy protection in fog computing environment. *IEEE Access*, 8:64461–64474, 2020.

[163] Gang Sun, Siyu Sun, Hongfang Yu, and Mohsen Guizani. Toward incentivizing fog-based privacy-preserving mobile crowdsensing in the internet of vehicles. *IEEE Internet of Things Journal*, 7(5):4128–4142, 2020.

[164] Ke Gu, Keming Wang, Xiong Li, and Weijia Jia. Multi-fogs-based traceable privacy-preserving scheme for vehicular identity in internet of vehicles. *IEEE Transactions on Intelligent Transportation Systems (Early Access Article)*, pages 1–1, 2021.

[165] Bimal Ghimire and Danda B. Rawat. Secure, privacy preserving and verifiable federating learning using blockchain for internet of vehicles. *IEEE Consumer Electronics Magazine (Early Access Article)*, pages 1–1, 2021.

[166] Randhir Kumar, Prabhat Kumar, Rakesh Tripathi, Govind P. Gupta, and Neeraj Kumar. P2sf-iov: A privacy-preservation-based secured framework for internet of vehicles. *IEEE Transactions on Intelligent Transportation Systems (Early Access Article)*, pages 1–1, 2021.

[167] Haoye Chai, Supeng Leng, Jianhua He, Ke Zhang, and Baoyi Cheng. Cyberchain: Cybertwin empowered blockchain for lightweight and privacy-preserving authentication in internet of vehicles. *IEEE Transactions on Vehicular Technology (Early Access Article)*, pages 1–1, 2021.

[168] Xiaolong Xu, Qihe Huang, Haibin Zhu, Suraj Sharma, Xuyun Zhang, Lianyong Qi, and Md Zakirul Alam Bhuiyan. Secure service offloading for internet of vehicles in sdn-enabled mobile edge computing. *IEEE Transactions on Intelligent Transportation Systems*, 22(6):3720–3729, 2021.

[169] Sujin Cai, Xin Lyu, Xin Li, Duohan Ban, and Tao Zeng. A trajectory released scheme for the internet of vehicles based on differential privacy. *IEEE Transactions on Intelligent Transportation Systems (Early Access Article)*, pages 1–1, 2021.

[170] Jingjing Yang, Jiaxing Liu, Runkai Han, and Jinzhao Wu. Generating and restoring private face images for internet of vehicles based on semantic features and adversarial examples. *IEEE Transactions on Intelligent Transportation Systems (Early Access Article)*, pages 1–1, 2021.

[171] Anil Kumar Sutrala, Palak Bagga, Ashok Kumar Das, Neeraj Kumar, Joel J. P. C. Rodrigues, and Pascal Lorenz. On the design of conditional privacy preserving batch verification-based authentication scheme for internet of vehicles deployment. *IEEE Transactions on Vehicular Technology*, 69(5):5535–5548, 2020.

[172] Efstathios Zavvos, Enrico H. Gerding, Vahid Yazdanpanah, Carsten Maple, Sebastian Stein, and m.c. schraefel. Privacy and trust in the internet of vehicles. *IEEE Transactions on Intelligent Transportation Systems (Early Access Article)*, pages 1–1, 2021.

[173] Farhan Ahmad, Fatih Kurugollu, Chaker Abdelaziz Kerrache, Sakir Sezer, and Lu Liu. Notrino: A novel hybrid trust management scheme for internet-of-vehicles. *IEEE Transactions on Vehicular Technology*, 70(9):9244–9257, 2021.

[174] Wenjia Li and Houbing Song. Art: An attack-resistant trust management scheme for securing vehicular ad hoc networks. *IEEE transactions on intelligent transportation systems*, 17(4):960–969, 2015.

[175] Ray Chen, Fenye Bao, MoonJeong Chang, and Jin-Hee Cho. Dynamic trust management for delay tolerant networks and its application to secure routing. *IEEE Transactions on Parallel and Distributed Systems*, 25(5):1200–1210, 2013.

[176] Ji-Ming Chen, Ting-Ting Li, and John Panneerselvam. Tmec: a trust management based on evidence combination on attack-resistant and collaborative internet of vehicles. *IEEE Access*, 7:148913–148922, 2018.

[177] Haibin Zhang, Jiajia Liu, Huanlei Zhao, Peng Wang, and Nei Kato. Blockchain-based trust management for internet of vehicles. *IEEE Transactions on Emerging Topics in Computing*, 9(3):1397–1409, 2021.

[178] Xiaolong Xu, Qi Wu, Lianyong Qi, Wanchun Dou, Sang-Bing Tsai, and Md Zakirul Alam Bhuiyan. Trust-aware service offloading for video surveillance in edge computing enabled internet of vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 22(3):1787–1796, 2021.

[179] Pranav Kumar Singh, Roshan Singh, Sunit Kumar Nandi, Kayhan Zrar Ghafoor, Danda B. Rawat, and Sukumar Nandi. Blockchain-based adaptive trust management

in internet of vehicles using smart contract. *IEEE Transactions on Intelligent Transportation Systems*, 22(6):3616–3630, 2021.

[180] Uzair Javaid, Muhammad Naveed Aman, and Biplab Sikdar. A scalable protocol for driving trust management in internet of vehicles with blockchain. *IEEE Internet of Things Journal*, 7(12):11815–11829, 2020.

[181] Qiaolun Zhang, Jun Wu, Michele Zanella, Wu Yang, Ali Kashif Bashir, and William Fornaciari. Sema-iiovt: Emergent semantic-based trustworthy information-centric fog system and testbed for intelligent internet of vehicles. *IEEE Consumer Electronics Magazine (Early Access Article)*, pages 1–1, 2021.

[182] Ghulam Muhammad and Musaed Alhussein. Security, trust, and privacy for the internet of vehicles: A deep learning approach. *IEEE Consumer Electronics Magazine (Early Access Article)*, pages 1–1, 2021.

[183] Qixu Wang, Xingshu Chen, Xin Jin, Xiang Li, Dajiang Chen, and Xue Qin. Enhancing trustworthiness of internet of vehicles in space-air-ground integrated networks: Attestation approach. *IEEE Internet of Things Journal (Early Access Article)*, pages 1–1, 2021.

[184] Zhigang Yang, Ruyan Wang, Dapeng Wu, Boran Yang, and Puning Zhang. Blockchain-enabled trust management model for the internet of vehicles. *IEEE Internet of Things Journal (Early Access Article)*, pages 1–1, 2021.

[185] Jiabin Li, Zhi Xue, Changlian Li, and Ming Liu. Rted-sd: A real-time edge detection scheme for sybil ddos in the internet of vehicles. *IEEE Access*, 9:11296–11305, 2021.

[186] ZHANG Xiaoqing HE Zhongtang. Two-phase placement algorithm with energy efficiency optimization for virtual machins bsed on data center. *Journal of Computer Applications*, 34(11):3222, 2014.

[187] Antony T Buller and John McManus. The quartile-deviation/median-diameter relationships of glacial deposits. *Sedimentary Geology*, 10(2):135–146, 1973.

[188] Sesham Srinu, Amit Kumar Mishra, and Shiba Farooq. Improved gesd test for cooperative sensing over impaired cognitive radio networks. In *2014 annual IEEE India conference (INDICON)*, pages 1–5. IEEE, 2014.

[189] Mohsin Kamal, Gautam Srivastava, and Muhammad Tariq. Blockchain-based lightweight and secured v2v communication in the internet of vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 22(7):3997–4004, 2021.

[190] Abubakar U. Makarfi, Khaled M. Rabie, Omprakash Kaiwartya, Kabita Adhikari, Galymzhan Nauryzbayev, Xingwang Li, and Rupak Kharel. Toward physical-layer security for internet of vehicles: Interference-aware modeling. *IEEE Internet of Things Journal*, 8(1):443–457, 2021.

[191] Sahil Garg, Amritpal Singh, Gagangeet Singh Aujla, Sukhdeep Kaur, Shalini Batra, and Neeraj Kumar. A probabilistic data structures-based anomaly detection scheme for software-defined internet of vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 22(6):3557–3566, 2021.

[192] Xinghua Li, Hengyou Zhang, Yinbin Miao, Siqi Ma, Jianfeng Ma, Ximeng Liu, and Kim-Kwang Raymond Choo. Can bus messages abnormal detection using improved svdd in internet of vehicle. *IEEE Internet of Things Journal (Early Access Article)*, pages 1–1, 2021.

[193] Insaf Ullah, Muhammad Asghar Khan, Fazlullah Khan, Mian Ahmad Jan, Ram Srinivasan, Spyridon Mastorakis, Saddam Hussain, and Hizbullah Khattak. An efficient and secure multimessage and multireceiver signcryption scheme for edge-enabled internet of vehicles. *IEEE Internet of Things Journal*, 9(4):2688–2697, 2022.

[194] Liangjun Song, Gang Sun, Hongfang Yu, Xiaojiang Du, and Mohsen Guizani. Fbia: A fog-based identity authentication scheme for privacy preservation in internet of vehicles. *IEEE Transactions on Vehicular Technology*, 69(5):5403–5415, 2020.

[195] Palak Bagga, Ashok Kumar Das, Mohammad Wazid, Joel J. P. C. Rodrigues, Kim-Kwang Raymond Choo, and YoungHo Park. On the design of mutual authentication and key agreement protocol in internet of vehicles-enabled intelligent transportation system. *IEEE Transactions on Vehicular Technology*, 70(2):1736–1751, 2021.

[196] Muhammad Adil, Jehad Ali, Muhammad Attique, Muhammad Mohsin Jadoon, Safia Abbas, Sattam Rabia Alotaibi, Varun G. Menon, and Ahmed Farouk. Three byte-based mutual authentication scheme for autonomous internet of vehicles. *IEEE Transactions on Intelligent Transportation Systems (Early Access Article)*, pages 1–1, 2021.

[197] Harsha Vasudev, Varad Deshpande, Debasis Das, and Sajal K. Das. A lightweight mutual authentication protocol for v2v communication in internet of vehicles. *IEEE Transactions on Vehicular Technology*, 69(6):6709–6717, 2020.

[198] Daya Sagar Gupta, Arijit Karati, Walid Saad, and Daniel Benevides Da Costa. Quantum-defended blockchain-assisted data authentication protocol for internet of vehicles. *IEEE Transactions on Vehicular Technology (Early Access Article)*, pages 1–1, 2022.

[199] Jiangtao Li, Yufeng Li, Chenhong Cao, and Kwok-Yan Lam. Conditional anonymous authentication with abuse-resistant tracing and distributed trust for internet of vehicles. *IEEE Internet of Things Journal (Early Access Article)*, pages 1–1, 2021.

[200] Xiangjie Kong, Bing Zhu, Guojiang Shen, Tewabe Chekole Workneh, Zhanhao Ji, Yang Chen, and Zhi Liu. Spatial-temporal-cost combination based taxi driving fraud detection for collaborative internet of vehicles. *IEEE Transactions on Industrial Informatics*, 18(5):3426–3436, 2022.

[201] Khaleel Mershad. Surfer: A secure sdn-based routing protocol for internet of vehicles. *IEEE Internet of Things Journal*, 8(9):7407–7422, 2021.

[202] Khaleel Mershad, Hassan Artail, and Mario Gerla. Roamer: Roadside units as message routers in vanets. *Ad Hoc Networks*, 10(3):479–496, 2012.

[203] Durbadal Chattaraj, Basudeb Bera, Ashok Kumar Das, Sourav Saha, Pascal Lorenz, and YoungHo Park. Block-clap: Blockchain-assisted certificateless key agreement protocol for internet of vehicles in smart transportation. *IEEE Transactions on Vehicular Technology*, 70(8):8092–8107, 2021.

[204] Miguel Castro and Barbara Liskov. Practical byzantine fault tolerance and proactive recovery. *ACM Transactions on Computer Systems (TOCS)*, 20(4):398–461, 2002.

[205] Sunitha Safavat and Danda B. Rawat. On the elliptic curve cryptography for privacy-aware secure aco-aodv routing in intent-based internet of vehicles for smart cities. *IEEE Transactions on Intelligent Transportation Systems*, 22(8):5050–5059, 2021.

[206] Hassan Karim and Danda B. Rawat. Tollsonly please—homomorphic encryption for toll transponder privacy in internet of vehicles. *IEEE Internet of Things Journal*, 9(4):2627–2636, 2022.

[207] Xiao Wang, Yushan Zhu, Shuangshuang Han, Linyao Yang, Haixia Gu, and Fei-Yue Wang. Fast and progressive misbehavior detection in internet of vehicles based on broad learning and incremental learning systems. *IEEE Internet of Things Journal (Early Access Article)*, pages 1–1, 2021.

[208] Nalam Venkata Abhishek, Muhammad Naveed Aman, Teng Joon Lim, and Biplab Sikdar. Drive: Detecting malicious roadside units in the internet of vehicles with low latency data integrity. *IEEE Internet of Things Journal (Early Access Article)*, pages 1–1, 2021.

[209] Li Yang, Abdallah Moubayed, and Abdallah Shami. Mth-ids: A multitiered hybrid intrusion detection system for internet of vehicles. *IEEE Internet of Things Journal*, 9(1):616–632, 2022.

[210] Imran Ahmed, Awais Ahmad, and Gwanggil Jeon. Deep learning-based intrusion detection system for internet of vehicles. *IEEE Consumer Electronics Magazine (Early Access Article)*, pages 1–1, 2021.

[211] Saeid Iranmanesh, Forough Shirin Abkenar, Abbas Jamalipour, and Raad Raad. A heuristic distributed scheme to detect falsification of mobility patterns in internet of vehicles. *IEEE Internet of Things Journal*, 9(1):719–727, 2022.

[212] Talal Halabi, Omar Abdel Wahab, Ranwa Al Mallah, and Mohammad Zulkernine. Protecting the internet of vehicles against advanced persistent threats: A bayesian stackelberg game. *IEEE Transactions on Reliability*, 70(3):970–985, 2021.

[213] Xiantao Jiang, F. Richard Yu, Tian Song, and Victor C.M. Leung. Intelligent resource allocation for video analytics in blockchain-enabled internet of autonomous vehicles with edge computing. *IEEE Internet of Things Journal (Early Access Article)*, pages 1–1, 2020.

[214] Bin Cao, Xinghan Chen, Zhihan Lv, Ruichang Li, and Shanshan Fan. Optimization of classified municipal waste collection based on the internet of connected vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 22(8):5364–5373, 2021.

[215] Soheila Ghane, Alireza Jolfaei, Lars Kulik, Kotagiri Ramamohanarao, and Deepak Puthal. Preserving privacy in the internet of connected vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 22(8):5018–5027, 2021.

[216] Zhihong Tian, Xiangsong Gao, Shen Su, and Jing Qiu. Vcash: A novel reputation framework for identifying denial of traffic service in internet of connected vehicles. *IEEE Internet of Things Journal*, 7(5):3901–3909, 2020.

[217] Qi Liu, Kondwani Michael Kamoto, Xiaodong Liu, Yonghong Zhang, Zaiqiang Yang, Mohammad R. Khosravi, Yanwei Xu, and Lianyong Qi. A sensory similarities approach to load disaggregation of charging stations in internet of electric vehicles. *IEEE Sensors Journal*, 21(114):15895–15903, 2021.

[218] Long Luo, Jingcui Feng, Hongfang Yu, and Gang Sun. Blockchain-enabled two-way auction mechanism for electricity trading in internet of electric vehicles. *IEEE Internet of Things Journal (Early Access Article)*, pages 1–1, 2021.

[219] Ayesha Sadiq, Muhammad Umar Javed, Rabiya Khalid, Ahmad Almogren, Muhammad Shafiq, and Nadeem Javaid. Blockchain based data and energy trading in internet of electric vehicles. *IEEE Access*, 0:7000–7020, 2021.

[220] Adugna Gebrie Jember, Wenhe Xu, Chao Pan, Xiongwen Zhao, and Xin-Cheng Ren. Game and contract theory-based energy transaction management for internet of electric vehicle. *IEEE Access*, 8:203478–203487, 2020.

[221] Hayla Nahom Abishu, Abegaz Mohammed Seid, Yasin Habtamu Yacob, Tewodros Ayall, Guolin Sun, and Guisong Liu. Consensus mechanism for blockchain-enabled vehicle-to-vehicle energy trading in the internet of electric vehicles. *IEEE Transactions on Vehicular Technology*, 71(1):946–960, 2022.

[222] Zhifan Gao, Chenchu Xu, Heye Zhang, Shuo Li, and Victor Hugo C. de Albuquerque. Trustful internet of surveillance things based on deeply represented visual co-saliency detection. *IEEE Internet of Things Journal*, 7(5):4092–4100, 2020.

[223] Huazhu Fu, Xiaochun Cao, and Zhuowen Tu. Cluster-based co-saliency detection. *IEEE Transactions on Image Processing*, 22(10):3766–3778, 2013.

[224] Zhi Liu, Wenbin Zou, Lina Li, Liquan Shen, and Olivier Le Meur. Co-saliency detection based on hierarchical segmentation. *IEEE Signal Processing Letters*, 21(1):88–92, 2013.

[225] Dingwen Zhang, Junwei Han, Chao Li, Jingdong Wang, and Xuelong Li. Detection of co-salient objects by looking deep and wide. *International Journal of Computer Vision*, 120(2):215–232, 2016.

[226] Jinglin Zhang, Pu Liu, Feng Zhang, Hironobu Iwabuchi, Antonio Artur de H. e Ayres de Moura, and Victor Hugo C. de Albuquerque. Ensemble meteorological cloud classification meets internet of dependable and controllable things. *IEEE Internet of Things Journal*, 18(5):3323–3330, 2021.

[227] Nikhil B. Gaikwad, Hrishikesh Ugale, Avinash Keskar, and N. C. Shivaprakash. The internet-of-battlefield-things (iobt)-based enemy localization using soldiers location and gunshot direction. *IEEE Internet of Things Journal*, 7(12):11725–11734, 2020.

[228] Di Lin and Weiwei Wu. Heuristic algorithm for resource allocation in an internet of battle things. *IEEE Systems Journal (Early Access Article)*, pages 1–1, 2022.

[229] Chong Yu, Shuaiqi Shen, Haojun Yang, Kuan Zhang, and Hai Zhao. Leveraging energy, latency and robustness for routing path selection in internet of battlefield things. *IEEE Internet of Things Journal (Early Access Article)*, pages 1–1, 2021.

[230] Rashad Ramzan, Muhammad Omar, Omar Farooq Siddiqui, Taoufik Saleh Ksiksi, and Nabil Bastaki. Internet of trees (iotr) implemented by highly dispersive electromagnetic sensors. *IEEE Sensors Journal*, 21(1):642–650, 2021.

[231] Venkanna Udutalapally, Saraju P. Mohanty, Vishal Pallagani, and Vedant Khandelwal. scrop: A novel device for sustainable automatic disease prediction, crop selection, and irrigation in internet-of-agro-things for smart agriculture. *IEEE Sensors Journal*, 21(16):17525–17538, 2021.

[232] Anselmo Luiz Éden Battisti, Débora Christina Muchaluat-Saade, and Flávia C. Delicato. Enabling internet of media things with edge-based virtual multimedia sensors. *IEEE Access*, 9:59255–59269, 2021.

[233] Chang Wen Chen. Internet of video things: Next-generation iot with visual sensors. *IEEE Internet of Things Journal*, 7(8):6676–6685, 2020.

[234] Edward Curry, Dhaval Salwala, Praneet Dhingra, Felipe Arruda Pontes, and Piyush Yadav. Multimodal event processing: A neural-symbolic paradigm for the internet of multimedia things. *IEEE Internet of Things Journal (Early Access Article)*, pages 1–1, 2022.

[235] Piyush Yadav, Dhaval Salwala, and Edward Curry. Vid-win: Fast video event matching with query-aware windowing at the edge for the internet of multimedia things. *IEEE Internet of Things Journal*, 8(13):10367–10389, 2021.

[236] Mengdi Wang, Di Xiao, and Yong Xiang. Low-cost and confidentiality-preserving multi-image compressed acquisition and separate reconstruction for internet of multimedia things. *IEEE Internet of Things Journal*, 8(3):1662–1673, 2021.

[237] Diyawu Mumin, Lei-Lei Shi, Lu Liu, and John Panneerselvam. Data-driven diffusion recommendation in online social networks for the internet of people. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 52(1):166–178, 2022.

[238] Sahraoui Dhelim, Huansheng Ning, and Nyothiri Aung. Compath: User interest mining in heterogeneous signed social networks for internet of people. *IEEE Internet of Things Journal*, 8(8):7024–7035, 2021.

[239] Chunyou Zhang, Xiaoqiang Wu, Wei Yan, Lukun Wang, and Lei Zhang. Attribute-aware graph recurrent networks for scholarly friend recommendation based on internet of scholars in scholarly big data. *IEEE Transactions on Industrial Informatics*, 16(4):2707–2715, 2020.

[240] Jing Yue and Ming Xiao. Coding for distributed fog computing in internet of mobile things. *IEEE Transactions on Mobile Computing*, 20(4):1337–1350, 2021.

[241] Sangjun Eom, Haozhe Zhou, Upinder Kaur, Richard Voyles, and David Kusuma. Tupperwareearth: Bringing intelligent user assistance to the "internet of kitchen things". *IEEE Internet of Things Journal (Early Access Article)*, pages 1–1, 2021.

[242] Yongnan Liu, Xin Guan, Yu Peng, Hongyang Chen, Tomoaki Ohtsuki, and Zhu Han. Blockchain-based task offloading for edge computing on low-quality data via distributed learning in the internet of energy. *IEEE Journal on Selected Areas in Communications*, 40(2):657–676, 2022.

[243] Aya Sayed, Yassine Himeur, Abdullah Alsalemi, Faycal Bensaali, and Abbes Amira. Intelligent edge-based recommender system for internet of energy applications. *IEEE Systems Journal (Early Access Article)*, pages 1–1, 2021.

[244] Zehui Zhang, Cong Guan, Hui Chen, Xiangguo Yang, Wenfeng Gong, and Ansheng Yang. Adaptive privacy preserving federated learning for fault diagnosis in internet of ships. *IEEE Internet of Things Journal (Early Access Article)*, pages 1–1, 2021.

[245] Qubeijian Wang, Hong-Ning Dai, Qiu Wang, Mahendra K. Shukla, Wei Zhang, and Carlos Guedes Soares. On connectivity of uav-assisted data acquisition for underwater internet of things. *IEEE Internet of Things Journal*, 7(6):5371–5385, 2020.

[246] Chuan Lin, Guangjie Han, Jiaxin Du, Yuanguo Bi, Lei Shu, and Kaiguo Fan. A path planning scheme for auv flock-based internet-of-underwater-things systems to enable transparent and smart ocean. *IEEE Internet of Things Journal*, 7(10):9760–9772, 2020.

[247] Jing Yan, Yuan Meng, Xiaoyuan Luo, and Xinping Guan. To hide private position information in localization for internet of underwater things. *IEEE Internet of Things Journal*, 8(18):14338–14354, 2021.

[248] Debing Wei, Chenpei Huang, Xuanheng Li, Bin Lin, Minglei Shu, Jie Wang, and Miao Pan. Power efficient data collection scheme for auv assisted magnetic induction and acoustic hybrid internet of underwater things. *IEEE Internet of Things Journal (Early Access Article)*, pages 1–1, 2021.

[249] Mohammad Reza Khosravi and Sadegh Samadi. Reliable data aggregation in internet of visar vehicles using chained dual-phase adaptive interpolation and data embedding. *IEEE Internet of Things Journal*, 7(4):2603–2610, 2020.

[250] Cheng Cheng, Liang Guo, Tong Wu, Jinlong Sun, Guan Gui, Bamidele Adebisi, Haris Gacanin, and Hikmet Sari. Machine learning-aided trajectory prediction and conflict detection for internet of aerial vehicles. *IEEE Internet of Things Journal (Early Access Article)*, pages 1–1, 2021.

[251] Amartya Mukherjee, Debashis De, and Nilanjan Dey. Dewdrone: Dew computing for internet of drone things. *IEEE Consumer Electronics Magazine (Early Access Article)*, pages 1–1, 2021.

[252] Prosanta Gope and Biplab Sikdar. An efficient privacy-preserving authenticated key agreement scheme for edge-assisted internet of drones. *IEEE Transactions on Vehicular Technology*, 69(11):13621–13630, 2020.

[253] Basudeb Bera, Sourav Saha, Ashok Kumar Das, Neeraj Kumar, Pascal Lorenz, and Mamoun Alazab. Blockchain-envisioned secure data delivery and collection scheme for 5g-based iot-enabled internet of drones environment. *IEEE Transactions on Vehicular Technology*, 69(8):9097–9111, 2020.

[254] Sajid Hussain, Shehzad Ashraf Chaudhry, Osama Ahmad Alomari, Mohammed H. Alsharif, Muhammad Khurram Khan, and Neeraj Kumar. Amassing the security: An ecc-based authentication scheme for internet of drones. *IEEE Systems Journal*, 15(3):4431–4438, 2021.

[255] Chaosheng Feng, Bin Liu, Zhen Guo, Keping Yu, Zhiguang Qin, and Kim-Kwang Raymond Choo. Blockchain-based cross-domain authentication for intelligent 5g-enabled internet of drones. *IEEE Internet of Things Journal (Early Access Article)*, pages 1–1, 2021.

[256] Muhammad Tanveer, Abd Ullah Khan, Neeraj Kumar, and Mohammad Mehedi Hassan. Ramp-iod: A robust authenticated key management protocol for the internet of drones. *IEEE Internet of Things Journal*, 9(2):1339–1353, 2022.

[257] Jae Yeol Jeong, Jin Wook Byun, and Ik Rae Jeong. Key agreement between user and drone with forward unlinkability in internet of drones. *IEEE Access (Early Access Article)*, pages 1–1, 2022.

[258] Cong Pu and Logan Carpenter. Psched: A priority-based service scheduling scheme for the internet of drones. *IEEE Systems Journal*, 15(3):4230–4239, 2021.

[259] Nasir Saeed, Mohamed-Slim Alouini, and Tareq Y. Al-Naffouri. Accurate 3-d localization of selected smart objects in optical internet of underwater things. *IEEE Internet of Things Journal*, 7(2):937–947, 2020.

[260] Weina Niu, Jian'An Xiao, Xiyue Zhang, Xiaosong Zhang, Xiaojiang Du, Xiaoming Huang, and Mohsen Guizani. Malware on internet of uavs detection combining string matching and fourier transformation. *IEEE Internet of Things Journal*, 8(12):9905–9919, 2021.

[261] Di Zhou, Min Sheng, Jiaxin Wu, Jiandong Li, and Zhu Han. Gateway placement in integrated satellite-terrestrial networks: Supporting communications and internet of remote things. *IEEE Internet of Things Journal (Early Access Article)*, pages 1–1, 2021.

[262] Ahan Kak and Ian F. Akyildiz. Towards automatic network slicing for the internet of space things. *IEEE Transactions on Network and Service Management (Early Access Article)*, pages 1–1, 2021.

[263] Chen Han, Liangyu Huo, Xinhai Tong, Haichao Wang, and Xian Liu. Spatial anti-jamming scheme for internet of satellites based on the deep reinforcement learning and stackelberg game. *IEEE Transactions on Vehicular Technology*, 69(5):5331–5342, 2020.

[264] Patrick Gage Kelley, Saranga Komanduri, Michelle L Mazurek, Richard Shay, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Julio Lopez. Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. In *2012 IEEE symposium on security and privacy*, pages 523–537. IEEE, 2012.

[265] Gianpiero Costantino, Antonio La Marra, Fabio Martinelli, and Ilaria Matteucci. Candy: A social engineering attack to leak information from infotainment system. In *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*, pages 1–5. IEEE, 2018.

[266] Neil Zhenqiang Gong and Di Wang. On the security of trustee-based social authentications. *IEEE Trans. Inf. Forensics Secur.*, 9(8):1251–1263, 2014.

[267] SN Maitri, Mayur Agnihotri, Ashutosh Borde, and Pratik Salvi. Security of trustee based social authentication. *International Research Journal of Engineering and Technology*, 2017.

[268] Alana Libonati, Apu Kapadia, and Michael K Reiter. Social security: Combating device theft with community-based video notarization. Technical report, Tech. Rep., 2013.[Online]. Available: https://techreports.cs.unc.edu/papers/13-003.pdf, 2013.

[269] Vicki Bruce, Zoë Henderson, Craig Newman, and A Mike Burton. Matching identities of familiar and unfamiliar faces caught on cctv images. *Journal of Experimental Psychology: Applied*, 7(3):207, 2001.

[270] Justus Thies, Michael Zollhofer, Marc Stamminger, Christian Theobalt, and Matthias Nießner. Face2face: Real-time face capture and reenactment of rgb videos. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 2387–2395, 2016.

[271] Catherine Stupp. Fraudsters used ai to mimic ceo's voice in unusual cybercrime case. *The Wall Street Journal*, 30(08), 2019.

[272] Noura Alomar, Mansour Alsaleh, and Abdulrahman Alarifi. Social authentication applications, attacks, defense strategies and future research directions: a systematic review. *IEEE Communications Surveys & Tutorials*, 19(2):1080–1111, 2017.

[273] Christina Katsini, Marios Belk, Christos Fidas, Nikolaos Avouris, and George Samaras. Security and usability in knowledge-based user authentication: A review. In *Proceedings of the 20th Pan-Hellenic conference on informatics*, pages 1–6, 2016.

[274] Haipeng Wang, Feng Zheng, Zhuoming Chen, Yi Lu, Jing Gao, and Renjia Wei. A CAPTCHA design based on visual reasoning. In *2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 1967–1971. IEEE, 2018.

[275] Bojia Zi, Minghao Chang, Jingjing Chen, Xingjun Ma, and Yu-Gang Jiang. Wilddeepfake: A challenging real-world dataset for deepfake detection. In *Proceedings of the 28th ACM international conference on multimedia*, pages 2382–2390, 2020.

[276] Cristina Timón López, Ignacio Alamillo Alamillo Domingo, and Julián Valero Valero Torrijos. Which authentication method to choose. a legal perspective on user-device authentication in iot ecosystems. In *Proceedings of the 16th International Conference on Availability, Reliability and Security*, pages 1–6, 2021.