2023 11th International Symposium on Digital Forensics and Security (ISDFS) | 979-8-3503-3698-6/23/$31.00 ©2023 IEEE | DOI: 10.1109/ISDFS58141.2023.10131870

Survey on IoT Multi-Factor Authentication Protocols: A Systematic Literature Review

Zein Al-Abidin Mohammad Fneish
Faculty of Computer Studies
Arab Open University
Beirut, Lebanon
zmf005lb@aou.edu.lb

Mohammad El-Hajj
Faculty of Electrical Engineering
Mathematics and Computer Science
University of Twente
Enschede, Netherlands
m.elhajj@utwente.nl

Khouloud Samrouth
Faculty of Computer Studies
Arab Open University
Beirut, Lebanon
ksamrouth@aou.edu.lb

***Abstract*—The Internet of Things (IoT) is a network of physical objects that is equipped with computers, electronics, applications, sensors, and other devices. As the number of IoT devices and apps increases, a range of security techniques should be applied to strengthen and enhance their immunity to cyber attacks as attackers have more capabilities and tools now focused on targeting the IoT networks. In this context, we study the nature of the Internet of Things infrastructure, especially some different Iot architecture layers, their security challenges and brief proposed solutions. For different IoT layers, authentication is a main security aspect affecting each layer separately. We provide a systematic literature review (SLR) methodology to locate existing multi-factor authentication protocols in the literature and evaluate their effectiveness. Then we provide an analysis of available multi-factor authentication protocols that are intended for IoT environments. Then some recommendations were provided based on the analysis. In conclusion, since the large range of IoT devices are resource- and power-limited, the nature of IoT settings requires lightweight protocols. Any of those proposed protocols can call for ongoing follow-up in the future to figure out upcoming weaknesses.**

Keywords— survey, Multi-Factor Authentication, IoT, Internet of Things, authentication

I. Introduction

The network of physical objects known as the Internet of Things (IoT) includes tools, equipment, vehicles, buildings and other things that are equipped with computers, electronics, applications, sensor systems, and networking capabilities. This technology allows these objects to gather and share data. In his first 1999 proposal, Kevin Ashton defined the Internet of Things (IoT) as a network of individually identifiable linked items using radio-frequency identification (RFID) technology. Yet, the precise definition for IoT continues to be developed and depends on the viewpoints used [1] [2]. The world's network currently hosts millions of devices. This is the result of recent technological advancements that forced users to be frequently connected to their devices to perform daily tasks [3]. As the number of IoT devices and apps increases, a range of security techniques should be applied to strengthen and enhance their immunity to cyber attacks [4]. The key problem in an IoT context is security-related challenges such as privacy, authorization, authentication, permissions, system configuration, data storage, and administration [5]. The unique characteristics of IoT devices made classic authentication methods impractical and ineffective. Cryptographic techniques intended for powerful devices do not fit resource-constrained IoT nodes. Lightweight authentication methods became popular as a result [6]. An element of cybersecurity that, if ignored, enables attackers to gain unauthorized access is authentication. Therefore, the demand for multi-factor authentication has increased as hackers capabilities are increasing [7].

Since hackers or other attackers may access critical sensor data, security has been a key challenge in the IoT, thus it's important to review current security protocols. Turning a blind eye to the importance of authentication in the IoT security field may allow attackers to gain unauthorized access to sensitive data, and as attackers are increasingly having more advanced tools, the need for more secure multi-factor authentication protocols is evolving [7]. In this context, we study the nature of the IoT infrastructure, especially some different IoT architecture layers, their security challenges, and a brief proposed solutions. Then we provide an analysis of available multi-factor authentication protocols in the literature that are intended for IoT environments. As for my acknowledgement, there is no survey for multi-factor authentication protocols for IoT systems in the literature, which encouraged me to achieve this study which may help researchers seeking for a list and summary of some of the available multi-factor authentication protocols, to have it between hands in an easy and clean way.

The rest of this paper is organized as follows, In Section II, we explain the research methodology followed in this paper. In Section III, we describe different architectures of IoT layers and the the proposed solution based on the security attacks listed per layer. Analysis and discussion of the results are presented in Section IV. The final recommendations and conclusions are given in Section V.

II. Research Methodology

A security-perspective IoT vision is marked by multi-factor authentication protocols in IoT systems, thus a systematic literature review (SLR) methodology is used to locate existing protocols and evaluate their effectiveness.

A. Research Questions

This paper summarizes the research effort and shows the recent publications and developments of IoT multi-factor authentication protocols. The following research questions are addressed by this survey.

The definition of research questions is the first stage in a systematic literature review. The study's research questions are below:

- **RQ1**. What are security challenges facing IoT?

979-8-3503-3698-6/23/$31.00 ©2023 IEEE

Authorized licensed use limited to: UNIVERSITY OF TWENTE.. Downloaded on November 15,2023 at 08:59:08 UTC from IEEE Xplore. Restrictions apply.

TABLE I. SEARCH QUERIES

Source	Query	Areas
Google Scholar	(”Internet of Things”) AND (”Two OR Three OR multi”) intitle:”Factor Authentication”	N/A
IEEE	”Internet of Things” AND (”Two” OR ”Three” OR ”multi”) AND (”Factor Authentication” OR ”Factor-Authentication”)	N/A
SpringerLink	”Internet of Things” AND (Two OR Three OR Multi) AND ”Factor Authentication”	Computer Science & Engineering
ScienceDirect	(”IoT” OR ”Internet of Things”) AND (”Two” OR ”Three” OR ”Multi”) AND (”Factor Authentication”)	Computer Science & Engineering

- **RQ2**. What are proposed solutions for different IoT layers challenges?
- **RQ3**. What are multi-factor authentication protocols presented in the literature?

B. Search Queries

The search for appropriate papers on the study subject is the second stage in a systematic literature review. We identified four digital libraries: IEEE Xplore, SpringerLink, Google Scholar, and ScienceDirect, where main search was executed. Then, search queries were built and used to gather papers published related to the study topic. We first developed a set of keywords connected to our research topic: ”Internet of Things,” ”IoT,” ”Two,” ”Three,” and ”Multi,” ”Factor Authentication.”

Each search engine has its specific criteria. For Google Scholar, we used the ”intitle” feature in order to narrow down the search results, were results preferably has the ”Factor Authentication” in the paper’s title. For exporting the results, a tiny python script was developed to mimic Google Scholar’s search requests with ”GSP=CF=4” as a cookie parameter which will return the reference in BibTex format to be scraped from the response. As for IEEE and SpringerLink, they both provide a feature for exporting the results in various formats. However, SpringerLink’s export was limited to 1000 results, so they were exported in two phases by filtering by search area. Results from ScienceDirect were fetched by intercepting the HTTP requests and getting the search results as JSON object, then writing a tiny python parser to extract the DOIs of the results. All the results were processed as described in Section C. The used search queries are shown in Table I.

C. Used Tools

All the extracted sources were imported to ”Zotero” tool for processing. SpringerLink, ScienceDirect and IEEE’s exports weren’t compatible with Zotero, so DOIs were extracted and then imported to Zotero which will automatically retrieve all the available information for articles based on its DOI. The output was then exported in BibTex format and imported to ”Rayyan.ai” which is a web-based online tool for navigating easily through publications and their associated info such as abstracts, dates, etc... which will help filtering the publications for inclusion and exclusion.

TABLE II. IOT ARCHITECTURE LAYERS COMPARISON

Layer	Three-Layer	Four-Layer	Five-Layer
Perception	✓	✓	✓
Network	✓	✓	✓
Processing		✓	✓
Application	✓	✓	✓
Business			✓

D. Inclusion/Exclusion Criteria

The complete text, abstracts, titles, keywords, and selection criteria have all been used to make the final decision of publication filtration. We did not include the following sorts of papers:

- Publication duplication
- Non-English publications
- Were not published in the latest 10 years
- Publications unrelated to the specified search queries
- Not in the scope of IoT
- Survey publications as they are not dedicated to proposing or improving a scheme

The following components were considered to determine the research publications’ reliability for inclusion:

- Proposes a new multi-factor authentication scheme for IoT or improves a previous one
- The proposed schemes are aimed to WSN are accepted
- The paper gives a clear description of the proposed solution
- The research has been published in a reliable source with a good reputation

E. Publications Filtration

The publication filtration process is the last step to extract publications related to the defined search queries from the identified digital libraries and then choosing the appropriate publications based on the inclusion/exclusion criteria for further analysis. The result of this step is discussed in Section IV in answering to **RQ3**.

III. IoT Architecture Layers: Attacks & Solutions

In its simplest form, an IoT architecture is a collection of various components, such as sensing devices, protocols, operators, cloud services, and layers [8]. The Internet of Things (IoT) architectural layers are differentiated in order to track a system’s consistency across protocols and gateways in addition to sensors and devices [9]. Different architectures are proposed in the literature each with a different number of layers with more abstraction and specificity. The number of layers in an IoT architecture ranges from three layers to seven layers, we will be focusing on 3 [1], 4 [8] and 5 [10] layers architectures as in Figure 1 due to the overlapping between these layers [9].

To ensure the security of IoT, the same fundamental security principles - Confidentiality, Integrity, Availability, Authentication, Authorization, and Privacy - that apply to all communications involving computers and networks must be present. The diverse and widespread nature of the IoT, however, adds additional issues that need to be resolved with regard to a sense of security. In this section, we are going to discuss the security challenges facing each layer of the five-layer architecture.

The five layers are: perception, network (transport), processing, application and business layer. The three layer architecture is the most basic with perception, network and application layer. The four layer architecture has an additional processing (support) layer and the five layer architecture has another additional business layer as shown in Table II. The five layers are described as follows:

Authorized licensed use limited to: UNIVERSITY OF TWENTE.. Downloaded on November 15,2023 at 08:59:08 UTC from IEEE Xplore. Restrictions apply.

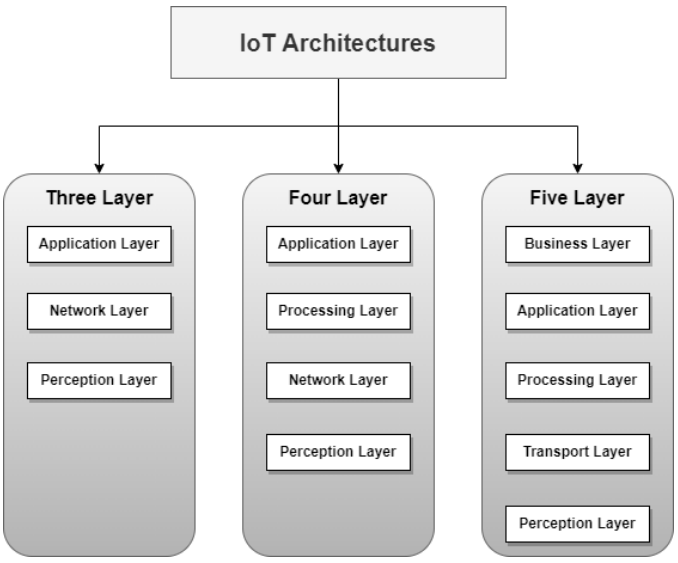

Fig. 1: Basic Architectures of IoT

A. Perception Layer

The Internet of Things' five senses characteristics make up the perception layer. It is used to recognize items, observe objects, gather data, and carry out automatic control [8]. It is directly connected to the actual world so that it can sense and gather data about surroundings such as temperature, smoke, motion, humidity, etc. This layer [9] is the first layer from the bottom and is a part of three-, four- and five-layer architectures [11].

The IoT's perception layer, also known as the "sensor layer," depends on physical resources. It gathers data using a variety of sensing tools and devices, converts that data to digital signals, and then sends those signals to the network layer. Some of the known attacks against this layer are: jamming attacks, sensor hijacking, false data inject attacks, impersonation attacks, cloning attacks, power exhaustion attacks, and IoT-based botnet attacks.

This layer is prone to various types of attacks [10] which can be solved by authentication, cryptography, distance limiting, rate limiting, key agreement and access control in order to avoid attacks which may lead to modifying or impersonating a node identity, predicting the encryption key [12], sending malicious data, etc. [13].

B. Application Layer

Its primary function is to provide the user with a specific service dependent on the type of application [8]. It outlines a variety of uses for the Internet of Things, including smart homes, intelligent transportation, and animal tracking [9]. This layer is part of all the proposed layers of architecture [11].

Since it works directly with end users, privacy and data theft are key issues in this layer: spear-phishing attacks, reprogramming attacks, malicious code injection attacks, service disruption attacks, and data and access control attacks.

We need to address the following aspects in order to address the application layer security issue [12]. User privacy protection is considered a central issue but it comes after the authentication and key agreement throughout the network environment [14]. Protecting user identities and other data from unauthorized disclosure is the goal of privacy protection [15].

C. Network Layer

Connecting to other smart objects, network devices, and servers is handled via the network layer. It is in charge of sending the relevant details and measurement items to other IoT network elements using a variety of communication protocols such as Wifi, Bluetooth, NFC, MQTT, etc. In a three-layer architecture, sensor data will be processed and transmitted in this layer [16]. However, data processing is handled by a separate layer in other architectures [8]. This layer is a part of all the architectures we are talking about [9].

Multiple types and categories of attacks apply when a communication occurs between IoT nodes and/or gateways and servers. Main categories of attacks are: traffic analysis attacks, eavesdropping, distributed/denial of Service attacks, routing attacks, and man in the middle attacks.

Authentication and authorization techniques are frequently used to solve a range of IoT risks on the network layer and other layers by avoiding illegal nodes [11]. Another technique is setting up filtering devices to avoid network blockage and intrusions [12]. Applying adequate encryption mechanisms is also required to protect the network communications [17].

D. Processing Layer

The processing layer is a part of four-layer and five-layer architectures [1]. It is responsible for converting raw data received from previous layers into useful data by controlling, examining, processing, and storing received data within the processing layer scope [8]. Without human involvement, it may make judgments based on data processing, to turn on an AC based on temperature for example [9]. Cloud computing, big data, and databases are examples of existing technologies that boost this layer [11].

During the processing and storage phase of the data in the processing layer, these data are prone to various types of attacks: signature wrapping attacks, forged data source, man in the middle attacks, SQL injection, malicious insider attacks, cloud malware injection, and flooding attacks in cloud.

The processing layer requires a significant amount of security services design, including cloud services and secure clustered computation, strong encryption algorithms and protocols, and anti-virus [11]. The following security issues for the platform need to be taken into account: operating system security , data backup and data recovery methods, concurrent computing which represents the ability to handle high loads, and a method to deal with DoS and DDoS attacks [14].

E. Business Layer

It controls the whole Internet of Things (IoT) system [8], including the business and profit models, in a user-friendly manner while maintaining privacy [9]. This layer is a part of the five-layer architecture only [11].

Because the business layer is a specialized descendant of the application layer, it will be vulnerable to similar threats. The ability of the attacker to affect the operational or business components of the IoT system makes a difference [18].

IV. Analysis and Discussion

In this section we are going to discuss the appropriate results to our research questions. To answer the first two question **RQ1** and **RQ2**, we reviewed some papers in the literature discussing various architectures in IoT to find out possible security challenges facing each layer in these architectures. To answer **RQ1**, the attacks were summarized and shown in Table III. We have found out that some

Authorized licensed use limited to: UNIVERSITY OF TWENTE.. Downloaded on November 15,2023 at 08:59:08 UTC from IEEE Xplore. Restrictions apply.

TABLE III. SECURITY CHALLENGES/ATTACKS PER IOT LAYER

IoT Layer	Attacks
Perception Layer	Jamming, Sensor Hijacking, False Data Inject, Impersonation, Cloning, Power Exhaustion, and IoT-based Botnet Attacks.
Application Layer	Spear-Phishing, Reprogramming, Malicious Code Injection, Service Disruption, and Data and Access Control attacks.
Network Layer	Traffic Analysis, Eavesdropping, Distributed/Denial of Service, Routing, and Man in the Middle attacks
Processing Layer	Signature Wrapping, Forged Data Source, Man in the Middle, SQL injection, Malicious Insider attacks, Cloud Malware Injection, and Flooding Attacks in Cloud
Business Layer	Same as Application Layer

of the attacks may be found on two layers due to the abstraction of layers when the architecture is flattened. For example, attacks related to processing layer in 5-layer architecture may apply for network layer or application layer in 3-layer architecture.

Answering **RQ2** was also done in the sub sections of Section III were we identified that authentication may pose a great solution for vast majority of the attacks on all IoT architecture layers. However, authentication as-is being not secure enough in itself, multi-factor authentication became a demand to overcome the problem [7].

Through the SLR presented in Section II, we answered the main question **RQ3** and the list of the proposed multi-factor authentication protocols are shown in Table IV. 2058 papers were first chosen by using the search queries on the chosen library resources. The method for choosing a publication involves doing a tollgate approach-based filtering while taking the inclusion/exclusion criteria in Section D into consideration. Figure 2 displays a number of publications selecting applying the tollgate strategy.

237 duplicate publications that Zotero tool had discovered were removed. After inspecting the title of each publication and removing any publication that did not fall under the scope of our survey, we were left with 334 items. After reading the abstracts and eliminating out non-relevant publications in contrast to acceptance criteria we ended up choosing 50 publications for analysis.

The publishers of the filtered publications were then extracted and visualized as shown in Figure 3. 22 publications were chosen from IEEE, 10 from SpringerLink, 5 from ScienceDirect, 4 from MDPI, 3 from Hindawi, and 6 from others. The publications which came from digital libraries which we did not explicitly identify in the methodology were reputable results found via Google Scholar.

The tags and titles in combination with abstracts were also extracted from the chosen publications and a word cloud was generated for each as shown in Figure 4. The results show that most of the keywords are related to security.

The results showed that 56% of the proposed protocols were two-factor based (28 protocol) and 44% are three-factor based (22 protocols). PUF-based authentication factor is the most trendy in two-factor authentication protocols. 20 out of 22 surveyed three-factor authentication protocols use the exact ID/Password, Biometrics and Smart Card/Device combination as authentication factors, however, Biometrics is the most trending over all authentication factors.

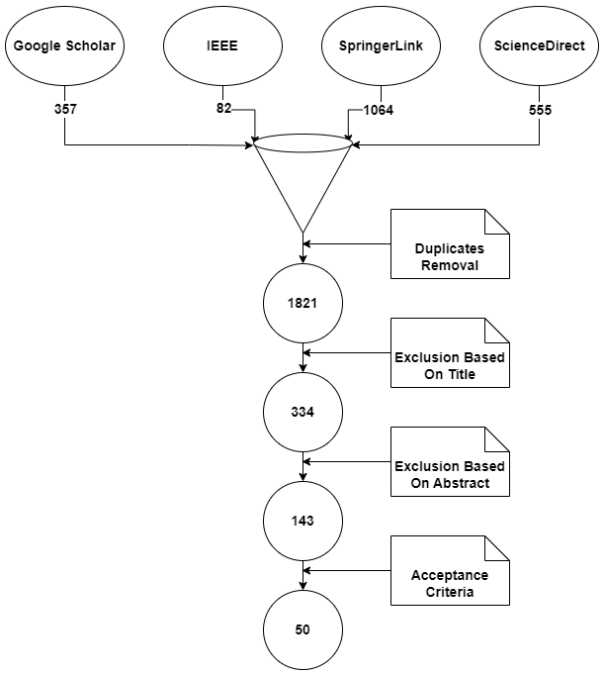

Fig. 2: Filtering Based on Tollgate Approach

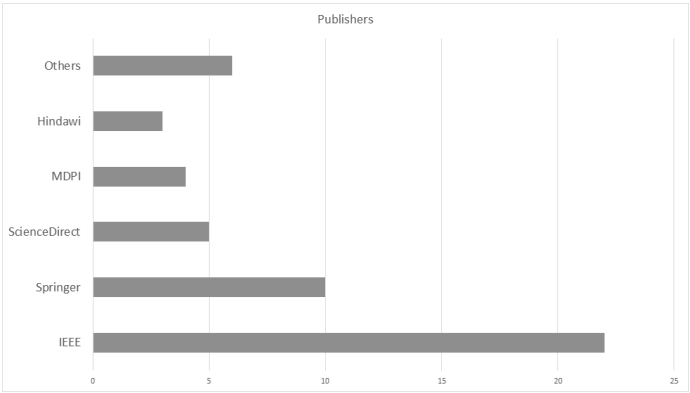

Fig. 3: Articles per Source

TABLE IV. ANALYZED PAPERS PER YEAR

Year	Paper
2014	[19]
2015	[20]
2016	[21] [22]
2017	[23] [24] [25] [26] [27] [28]
2018	[29] [30] [31] [32] [33] [34] [35]
2019	[36] [37] [38] [39] [40] [41] [42] [43] [44] [45] [46] [47] [48]
2020	[49] [50] [51] [52] [53] [54] [55] [56] [57] [58]
2021	[59] [60] [61] [62] [63] [64]
2022	[65] [66] [67] [68]

Authorized licensed use limited to: UNIVERSITY OF TWENTE.. Downloaded on November 15,2023 at 08:59:08 UTC from IEEE Xplore. Restrictions apply.

(a) Tags Cloud

(b) Titles/Abstracts Cloud

Fig. 4: Word Clouds Based on Titles/Abstracts and Tags

V. Conclusion and Recommendations

This research gave a thorough survey of the most recent developments in terms of security challenges in IoT systems. It also gives a comprehensive discussion on each IoT architectural layer and its own security attacks and challenges and possible solutions. Authentication was a key solution among others, however, basic authentication schemes are not enough to provide tough security. Though multi-factor authentication protocols which are meant for IoT environments tackles the limitations of single factor authentication protocols. However, the nature of IoT environments require lightweight protocols as the wide variety of IoT sensors and devices are resource-constrained and power-limited. Not all of the proposed protocols proved resilience against various attacks due to the nature of encryption used, hashing functions applied, calculations, fuzzy extractors used, etc.. Other protocols were proven to be robust and efficient to be applied and used in real-life IoT systems such as the proposed protocols in [31], [64], [57] and [54]. In addition, some of the proposed two-factor authentication protocols have also proven efficiency and suitability for IoT environments. Knowing that vast majority of the analysed two-factor protocols rely on ID/Password and smart card factors, [46] seems to be the most robust two-factor authentication protocol but it relies on biometrics as a second factor rather than a smart card. However, if smart card irrevocability is not a problem for your application, [51] can also be used. Some protocols may provide some optimistic approaches but requires special hardware which do not fit in the current and legacy IoT devices. Using any of the proposed protocols may require continuous follow-up in the future as some of the proposed protocols which claim to be resilient providing proofs were later proven to be prone to various types of attacks after undergoing focused cryptanylisis.

References

[1] P. Gokhale, O. Bhat, and S. Bhat, "Introduction to iot," *International Advanced Research Journal in Science, Engineering and Technology*, vol. 5, no. 1, pp. 41–44, 2018.

[2] S. Sarma, D. Brock, and K. Ashton, "The networked physical world: proposals for the next generation of computing commerce, and automatic identification," *AutoID Center White Paper*, 1999.

[3] A. Gazis, "What is iot? the internet of things explained," *Academia Letters*, p. 2, 2021.

[4] M. A. Sadeeq, S. R. Zeebaree, R. Qashi, S. H. Ahmed, and K. Jacksi, "Internet of things security: a survey," in *2018 International Conference on Advanced Science and Engineering (ICOASE)*. IEEE, 2018, pp. 162–166.

[5] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of things security: A survey," *Journal of Network and Computer Applications*, vol. 88, pp. 10–28, 2017.

[6] M. El-Hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, "A survey of internet of things (iot) authentication schemes," *Sensors*, vol. 19, no. 5, p. 1141, 2019.

[7] U. Gupta, "Application of multi factor authentication in internet of things domain," *arXiv preprint arXiv:1506.03753*, 2015.

[8] N. M. Kumar and P. K. Mallick, "The internet of things: Insights into the building blocks, component interactions, and architecture layers," *Procedia Computer Science*, vol. 132, pp. 109–117, 2018, international Conference on Computational Intelligence and Data Science. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050918309049

[9] M. Lombardi, F. Pascale, and D. Santaniello, "Internet of things: A general overview between architectures, protocols and applications," *Information*, vol. 12, no. 2, p. 87, 2021.

[10] T. Yousuf, R. Mahmoud, F. Aloul, and I. Zualkernan, "Internet of things (iot) security: current status, challenges and countermeasures," *International Journal for Information Security Research (IJISR)*, vol. 5, no. 4, pp. 608–616, 2015.

[11] S. Vashi, J. Ram, J. Modi, S. Verma, and C. Prakash, "Internet of things (iot): A vision, architectural elements, and security issues," in *2017 international conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*. IEEE, 2017, pp. 492–496.

[12] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: a review," in *2012 international conference on computer science and electronics engineering*, vol. 3. IEEE, 2012, pp. 648–651.

[13] K. Aarika, M. Bouhlal, R. A. Abdelouahid, S. Elfilali, and E. Benlahmar, "Perception layer security in the internet of things," *Procedia Computer Science*, vol. 175, pp. 591–596, 2020.

[14] C.-K. Wu, "Iot processing layer security," in *Internet of Things Security*. Springer, 2021, pp. 125–136.

[15] R. Khader and D. Eleyan, "Survey of dos/ddos attacks in iot," *Sustainable Engineering and Innovation*, vol. 3, no. 1, pp. 23–28, 2021.

[16] P. Sethi and S. R. Sarangi, "Internet of things: architectures, protocols, and applications," *Journal of Electrical and Computer Engineering*, vol. 2017, 2017.

[17] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying iot security: An exhaustive survey on iot vulnerabilities and a first empirical look on internet-scale iot exploitations," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019.

[18] M. Briland, "Addressing false data injection attacks in iot systems with a domain specific language within an industrial context," Ph.D. dissertation, Université Bourgogne Franche-Comté, 2021.

[19] M. Sarvabhatla and C. S. Vorugunti, "A secure biometric-based user authentication scheme for heterogeneous wsn," in *2014 Fourth international conference of emerging applications of information technology*. IEEE, 2014, pp. 367–372.

[20] P. H. Griffin, "Security for ambient assisted living: Multi-factor authentication in the internet of things," in *2015 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 2015, pp. 1–5.

Authorized licensed use limited to: UNIVERSITY OF TWENTE.. Downloaded on November 15,2023 at 08:59:08 UTC from IEEE Xplore. Restrictions apply.

[21] M. A. Crossman and H. Liu, "Two-factor authentication through near field communication," in *2016 IEEE Symposium on Technologies for Homeland Security (HST)*. IEEE, 2016, pp. 1–5.

[22] S. M. Sujatha and Y. U. Devi, "Design and implementation of iot testbed with three factor authentication," in *2016 International Conference on Communication and Electronics Systems (ICCES)*. IEEE, 2016, pp. 1–5.

[23] J. Murphy, G. Howells, and K. D. McDonald-Maier, "Multi-factor authentication using accelerometers for the internet-of-things," in *2017 Seventh International Conference on Emerging Security Technologies (EST)*. IEEE, 2017, pp. 103–107.

[24] P. K. Dhillon and S. Kalra, "Secure multi-factor remote user authentication scheme for internet of things environments," *International Journal of Communication Systems*, vol. 30, no. 16, p. e3323, 2017.

[25] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari, "A robust ecc-based provable secure authentication protocol with privacy preserving for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3599–3609, 2017.

[26] Q. Jiang, N. Kumar, J. Ma, J. Shen, D. He, and N. Chilamkurti, "A privacy-aware two-factor authentication protocol based on elliptic curve cryptography for wireless sensor networks," *International Journal of Network Management*, vol. 27, no. 3, p. e1937, 2017.

[27] X. Li, J. Peng, J. Niu, F. Wu, J. Liao, and K.-K. R. Choo, "A robust and energy efficient authentication protocol for industrial internet of things," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1606–1615, 2017.

[28] P. K. Dhillon and S. Kalra, "A lightweight biometrics based remote user authentication scheme for iot services," *Journal of Information Security and Applications*, vol. 34, pp. 255–270, 2017.

[29] M. N. Aman, M. H. Basheer, and B. Sikdar, "Two-factor authentication for iot with location information," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3335–3351, 2018.

[30] P. Gope and B. Sikdar, "Lightweight and privacy-preserving two-factor authentication scheme for iot devices," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 580–589, 2018.

[31] P. K. Dhillon and S. Kalra, "Multi-factor user authentication scheme for iot-based healthcare services," *Journal of Reliable Intelligent Environments*, vol. 4, no. 3, pp. 141–160, 2018.

[32] G. Xu, S. Qiu, H. Ahmad, G. Xu, Y. Guo, M. Zhang, and H. Xu, "A multi-server two-factor authentication scheme with un-traceability using elliptic curve cryptography," *Sensors*, vol. 18, no. 7, p. 2394, 2018.

[33] M. A. Gurabi, O. Alfandi, A. Bochem, and D. Hogrefe, "Hardware based two-factor user authentication for the internet of things," in *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*. IEEE, 2018, pp. 1081–1086.

[34] L. Wu, X. Du, W. Wang, and B. Lin, "An out-of-band authentication scheme for internet of things using blockchain technology," in *2018 International conference on computing, networking and communications (ICNC)*. IEEE, 2018, pp. 769–773.

[35] S. Shin and T. Kwon, "Two-factor authenticated key agreement supporting unlinkability in 5g-integrated wireless sensor networks," *IEEE Access*, vol. 6, pp. 11 229–11 241, 2018.

[36] H. N. Noura, R. Melki, and A. Chehab, "Secure and lightweight mutual multi-factor authentication for iot communication systems," in *2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*. IEEE, 2019, pp. 1–7.

[37] A. A. Ahmed and W. A. Ahmed, "An effective multifactor authentication mechanism based on combiners of hash function over internet of things," *Sensors*, vol. 19, no. 17, p. 3663, 2019.

[38] M. Karthigaiveni and B. Indrani, "An efficient two-factor authentication scheme with key agreement for iot based e-health care application using smart card," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–12, 2019.

[39] W. Li and P. Wang, "Two-factor authentication in industrial internet-of-things: Attacks, evaluation and new construction," *Future Generation Computer Systems*, vol. 101, pp. 694–708, 2019.

[40] J. Lee, M. Kim, S. Yu, K. Park, and Y. Park, "A secure multi-factor remote user authentication scheme for cloud-iot applications," in *2019 28th International Conference on Computer Communication and Networks (ICCCN)*. IEEE, 2019, pp. 1–2.

[41] Q. Jiang, X. Zhang, N. Zhang, Y. Tian, X. Ma, and J. Ma, "Two-factor authentication protocol using physical unclonable function for iov," in *2019 IEEE/CIC International Conference on Communications in China (ICCC)*. IEEE, 2019, pp. 195–200.

[42] A. J. Mohammed and A. A. Yassin, "Efficient and flexible multi-factor authentication protocol based on fuzzy extractor of administrator's fingerprint and smart mobile device," *Cryptography*, vol. 3, no. 3, p. 24, 2019.

[43] L. Kou, Y. Shi, L. Zhang, D. Liu, and Q. Yang, "A lightweight three-factor user authentication protocol for the information perception of iot," *CMC-Computers, Materials & Continua*, vol. 58, no. 2, pp. 545–565, 2019.

[44] S. Yu, K. Park, and Y. Park, "A secure lightweight three-factor authentication scheme for iot in cloud computing environment," *Sensors*, vol. 19, no. 16, p. 3598, 2019.

[45] E. Alharbi and D. Alghazzawi, "Two factor authentication framework using otp-sms based on blockchain," *Transactions on Machine Learning and Artificial Intelligence*, vol. 7, no. 3, pp. 17–27, 2019.

[46] M. A. Kiran, S. K. Pasupuleti, and R. Eswari, "A lightweight two-factor mutual authentication scheme for cloud-based iot," in *2019 4th International Conference and Workshops on Recent Advances and Innovations in Engineering (ICRAIE)*. IEEE, 2019, pp. 1–6.

[47] X. Li, J. Peng, M. S. Obaidat, F. Wu, M. K. Khan, and C. Chen, "A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems," *IEEE Systems Journal*, vol. 14, no. 1, pp. 39–50, 2019.

[48] L. Xu and F. Wu, "A lightweight authentication scheme for multi-gateway wireless sensor networks under iot conception," *Arabian Journal for Science and Engineering*, vol. 44, no. 4, pp. 3977–3993, 2019.

[49] R. Melki, H. N. Noura, and A. Chehab, "Lightweight multi-factor mutual authentication protocol for iot devices," *International Journal of Information Security*, vol. 19, no. 6, pp. 679–694, 2020.

[50] F. Wu, X. Li, L. Xu, P. Vijayakumar, and N. Kumar, "A novel three-factor authentication protocol for wireless sensor networks with iot notion," *IEEE Systems Journal*, vol. 15, no. 1, pp. 1120–1129, 2020.

[51] G. Sharma and S. Kalra, "Advanced lightweight multi-factor remote user authentication scheme for cloud-iot applications," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 4, pp. 1771–1794, 2020.

[52] M. Nikravan and A. Reza, "A multi-factor user authentication and key agreement protocol based on bilinear pairing for the internet of things," *Wireless Personal Communications*, vol. 111, no. 1, pp. 463–494, 2020.

[53] F. Wang, G. Xu, G. Xu, Y. Wang, and J. Peng, "A robust iot-based three-factor authentication scheme for cloud computing resistant to session key exposure," *Wireless Communications and Mobile Computing*, vol. 2020, 2020.

[54] H. Lee, D. Kang, J. Ryu, D. Won, H. Kim, and Y. Lee, "A three-factor anonymous user authentication scheme for internet of things environments," *Journal of Information Security and Applications*, vol. 52, p. 102494, 2020.

[55] Q. Jiang, N. Zhang, J. Ni, J. Ma, X. Ma, and K.-K. R. Choo, "Unified biometric privacy preserving three-factor authentication and key agreement for cloud-assisted autonomous vehicles," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 9, pp. 9390–9401, 2020.

[56] M. C. I. Putri, P. Sukarno, and A. A. Wardana, "Two factor authentication framework based on ethereum blockchain with dapp as token generation system instead of third-party on web application," *Register: Jurnal Ilmiah Teknologi Sistem Informasi*, vol. 6, no. 2, pp. 74–85, 2020.

[57] J. Lee, S. Yu, M. Kim, Y. Park, and A. K. Das, "On the design of secure and efficient three-factor authentication protocol using honey list for wireless sensor networks," *IEEE Access*, vol. 8, pp. 107 046–107 062, 2020.

[58] S. Yu, K. Park, Y. Park, H. Kim, and Y. Park, "A lightweight three-factor authentication protocol for digital rights management system," *Peer-to-peer Networking and Applications*, vol. 13, no. 5, pp. 1340–1356, 2020.

[59] M. Saqib, B. Jasra, and A. H. Moon, "A lightweight three factor authentication framework for iot based critical applications," *Journal of King Saud University-Computer and Information Sciences*, 2021.

[60] M. F. Ayub, K. Mahmood, S. Kumari, A. K. Sangaiah *et al.*, "Lightweight authentication protocol for e-health clouds in iot-based applications through 5g technology," *Digital Communications and Networks*, vol. 7, no. 2, pp. 235–244, 2021.

[61] J. Zhang, C. Shen, H. Su, M. T. Arafin, and G. Qu, "Voltage over-scaling-based lightweight authentication for iot security," *IEEE Transactions on Computers*, vol. 71, no. 2, pp. 323–336, 2021.

[62] S. Zou, Q. Cao, C. Wang, Z. Huang, and G. Xu, "A robust two-factor user authentication scheme-based ecc for smart home in iot," *IEEE Systems Journal*, 2021.

Authorized licensed use limited to: UNIVERSITY OF TWENTE.. Downloaded on November 15,2023 at 08:59:08 UTC from IEEE Xplore. Restrictions apply.

[63] S. S. Sahoo, S. Mohanty, and B. Majhi, "A secure three factor based authentication scheme for health care systems using iot enabled devices," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 1, pp. 1419–1434, 2021.
[64] H. Abdi Nasib Far, M. Bayat, A. Kumar Das, M. Fotouhi, S. M. Pournaghi, and M.-A. Doostari, "Laptas: lightweight anonymous privacy-preserving three-factor authentication scheme for wsn-based iiot," *Wireless Networks*, vol. 27, no. 2, pp. 1389–1412, 2021.
[65] K. S. Roy and H. K. Kalita, "An authentication protocol for iot network based on cloud computing environment using two factor authentication."
[66] N. Radhakrishnan and A. P. Muniyandi, "Dependable and provable secure two-factor mutual authentication scheme using ecc for iot-based telecare medical information system," *Journal of Healthcare Engineering*, vol. 2022, 2022.
[67] A. K. Agrahari, S. Varma, and S. Venkatesan, "Two factor authentication protocol for iot based healthcare monitoring system," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–18, 2022.
[68] C.-M. Chen, S. Liu, X. Li, S. Kumari, and L. Li, "Design and analysis of a provable secure two-factor authentication protocol for internet of things," *Security and Communication Networks*, vol. 2022, 2022.

Authorized licensed use limited to: UNIVERSITY OF TWENTE.. Downloaded on November 15,2023 at 08:59:08 UTC from IEEE Xplore. Restrictions apply.