Hindawi
Security and Communication Networks
Volume 2021, Article ID 5533843, 11 pages
https://doi.org/10.1155/2021/5533843

Review Article

Internet of Things Security: Challenges and Key Issues

Mourade Azrour,[1] **Jamal Mabrouki**,[2] **Azidine Guezzaz**,[3] **and Ambrina Kanwal**[4]

[1] *Computer Sciences Department, Faculty of Sciences and Techniques, Moulay Ismail University, Errachidia, Morocco*
[2] *Laboratory of Spectroscopy, Molecular Modeling, Materials, Nanomaterial, Water and Environment, CERNE2D, Mohammed V University, Faculty of Science, Rabat, Morocco*
[3] *Department of Computer Science and Mathematics, High School of Technology, Cadi Ayyad University, Essaouira 44000, Morocco*
[4] *Computer Science Department, Bahria University (Islamabad Campus), Islamabad, Pakistan*

Correspondence should be addressed to Mourade Azrour; mo.azrour@umi.ac.ma

Received 30 January 2021; Accepted 30 August 2021; Published 15 September 2021

Academic Editor: Habib Ullah Khan

Internet of Things (IoT) refers to a vast network that provides an interconnection between various objects and intelligent devices. The three important components of IoT are sensing, processing, and transmission of data. Nowadays, the new IoT technology is used in many different sectors, including the domestic, healthcare, telecommunications, environment, industry, construction, water management, and energy. IoT technology, involving the usage of embedded devices, differs from computers, laptops, and mobile devices. Due to exchanging personal data generated by sensors and the possibility of combining both real and virtual worlds, security is becoming crucial for IoT systems. Furthermore, IoT requires lightweight encryption techniques. Therefore, the goal of this paper is to identify the security challenges and key issues that are likely to arise in the IoT environment in order to guide authentication techniques to achieve a secure IoT service.

1. Introduction

In recent years, technology sector has known a real evolution. Furthermore, it has become an indispensable tool in our everyday life. Among these recent technologies, the Internet of Things (IoT) has been improved continuously and has attracted more and more people. This growth has positively impacted many sectors, including social security, agriculture, education, water management, house security, smart grid, and so on. Therefore, the number of connected devices is increasing day after day. According to Strategy Analytics, the connected objects will reach more than 38 billion by the end of 2025 and 50 billion by 2030 [1].

IoT is a new technology that allows the implementation of systems interconnecting several objects, either in the physical or virtual world [2, 3]. In fact, the evolution of the Internet began with the creation of a simple computer network linking personal computers and then moved on to client-server architecture networks, World Wide Web, e-mail, file sharing, etc. Subsequently, it now reaches a wide area network interconnecting billions of intelligent objects, which were embedded in sophisticated systems. Their operation is based on sensors and actuators designed for monitoring, controlling, and interacting with the physical environment where they exist.

Despite many advantages, IoT has three main problems that are data collection, data transmission, and data security. To collect data, many sensing tools have been introduced and adapted to the IoT devices. For transferring collected data, various protocols have been developed and adapted in order to enable to the IoT devices to connect to existed networks and exchange data. However, for the last one, it does not give the attention that it merits. Consequently, many classic and recent security issues are closely related to the IoT as well as authentication, data security, authorization, etc. Indeed, a weakness in authentication can lead to numerous attacks, including replay attack, Denning–Sacco attack, denial of service attack, password guessing attack, etc.

On the other hand, the authentication of IoT devices throughout heterogonous and interconnected protocols is a great challenge. Moreover, these protocols should take into account issues related to limitation of IoT devices as well as energy consumption, small memory size, and low processing capability [4–33].

In the literature review, previous studies [34–45] have surveyed the security of IoT technology. However, our study reveals some security challenges and issues of IoT. Consequently, the focus of this review paper is to categorize the security tasks and topics that are encountered in the IoT environment. Hence, we provide here a short guidance to researchers to accomplish secure IoT services like authentication, access control, and so on.

The remainder of this paper is organized as follows. In Section 2, IoT architecture is detailed. Section 3 is reserved for discussing IoT security issues. IoT security requirements are presented in Section 4. In Section 5, we compare some authentication approaches applied in IoT authentication environment. Finally, conclusions are given in Section 6.

2. IoT Architecture

The concept "Internet of Things" may be defined as a standard that refers to a large network connecting various sensors, actuators, and microcontrollers introduced in distinct objects. A large number of interconnected equipment such as smartphone, industrial machines, computers, vehicles, medical tools, irrigation system, TVs, or refrigerators can be part of the IoT [46]. Furthermore, IoT is a rather recent design that stands out from its antecedents, including all traditional, mobile, and sensor-based Internet networks. IoT includes a very large number of hybrid terminals. Since the majority of these devices can be connected to the Internet, they generally support common web techniques, including HTTP, JSON, XML, etc. One of the strengths of this technology is that it is well supported and can therefore be adapted to different existing infrastructures. Furthermore, some new protocols are especially considered for IoT, for example, CoAP and MQTT are alternatives to HTTP and 6LoWPAN is also an alternative of IPv4/IPv6.

Due to non-standardization of IoT, there are various architectures that are different [47]. However, we focus here on two known ones that are three- and five-layer architectures. As illustrated in Figure 1, the three-layer architecture consists of three layers including perception, networking, and application layers. The role of each layer is described in the following.

(i) The perception layer is the first layer of IoT architecture. It is connected to the physical world for sensing and collecting data from their environment. This layer consists of sensors and actuators to measure some values such as temperature, pH, light, gas, and so on, and to detect some functionality such as location and motion.

(ii) The network layer is the second layer; its role is to connect to various smart devices, gateways, and servers. It is responsible for transferring the captured values to other IoT network components. For these reasons, IoT uses several kinds of communication protocols and norms such as 4G/5G, Wi-Fi, ZigBee, Bluetooth, 6LoWPAN, WiMAX, and so on [48].

(iii) The application layer can offer the specific service requested by user. For instance, this application can provide doctors some health parameters of patients. This layer determines which applications can be installed, such as smart environment [49–52], smart homes [53–55], and water monitoring [56, 57].

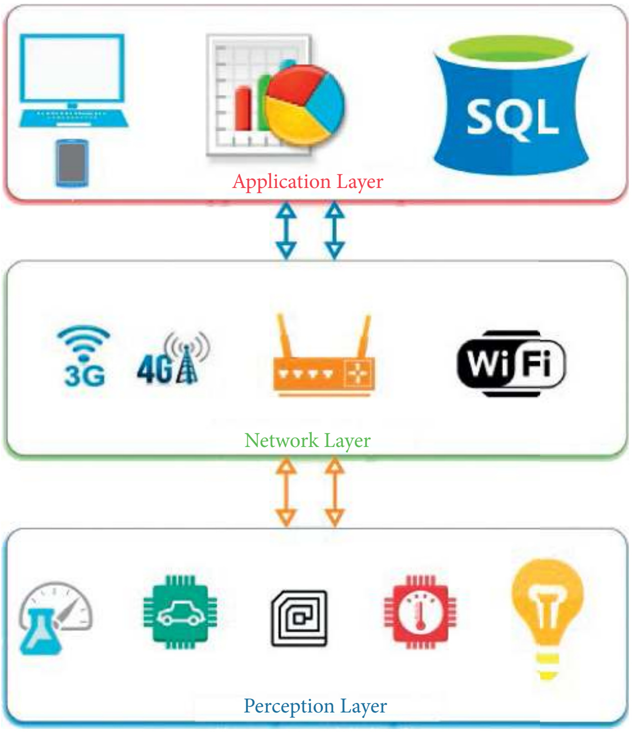

Figure 1: The three-layer architecture.

On the other hand, the five-layer architecture includes processing and business layers in addition to the three previous ones. As depicted in Figure 2, the five layers are perception, transport, processing, application, and business layers. The responsibilities of perception, transport, and application layers are identical to the similar layers in three-layer architecture. The roles of the addition layers are detailed as follows:

(i) The processing layer is also recognized as the middleware layer. It is responsible for controlling, analyzing, processing, and storing received data. It can make decisions according to the processing data without human intervention. This layer benefits from existing solutions including cloud computing, big data, and databases.

(ii) The business layer has a responsibility to manage the whole IoT systems [47]. So, its role is to control applications, business, and profit models. Furthermore, the users' privacy can be managed by this layer.

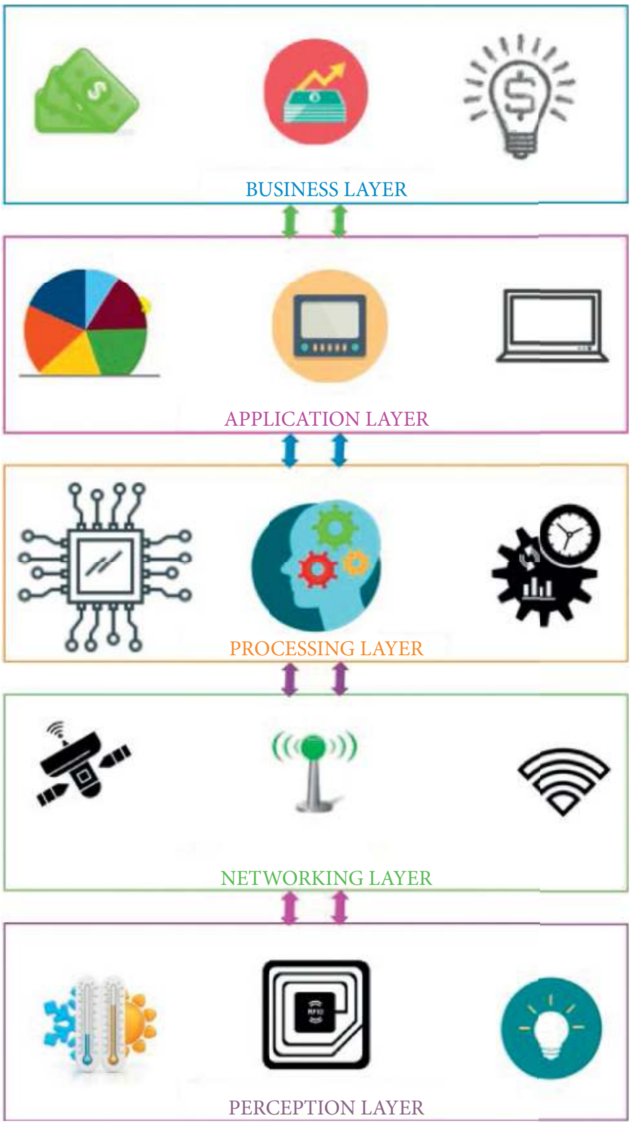

Figure 2: The five-layer architecture.

3. Security Issues in IoT

3.1. DOS. Denial of service (DOS) is a security attack that aims to prevent legitimate user and entity to have an authorized access to network resources. It is considered as the most popular and dominant attack. Generally, attackers can use flooding attack to exhaust system's resources including memory, CPU, and bandwidth [58–63]. Thus, he either prevents the system to provide service or he makes it ineffective. In this attack, pirates can use numerous skills such as sending unwanted packets or flooding network with multiple messages. Therefore, legitimate users are prevented from taking advantage of services.

3.2. Replay Attack. Replay attack is among old attacks on communication network, especially on authentication and key exchanging protocols. It allows the pirate to capture and store a fragment or the whole of captured session in a legitimate traffic [64, 65]. After gaining the trust in a public network, the attacker either sends the captured message to the entity that has participated in origin session or to another different destination [66]. Therefore, in IoT networks, replay attack is measured as a security weakness in which particular data are stored without any authorization before been sent back to the receiver. The goal of this attack is to trap the person in an unauthorized operation [67]. For example, in a smart home system, a temperature sensor is used to detect the temperature and then the measured values are sent to system controller. Based on these values, the system can run or stop the air conditioner to adapt the air temperature as desired by the personnel. However, if an attacker has pirated the sensor's temperature, he can save the day's values and send them at night. As result, the air conditioner will not be functioning normally.

To deal with replay attack, current solutions use three main mechanisms including timestamp, nonce, and response-challenge. The first one is the mechanism that helps to detect replay attack by checking the freshness of received message. Nonetheless, it is hard to assure time synchronization between IoT objects [68]. The second mechanism is the nonce, which is a series of random digits. However, the problem of this mechanism is that the node has no sufficient memory for keeping the list of received nonces. The last mechanism is the challenge-response. It has as objective to verify that the other party can resolve some challenges. But this technique necessitates that the two entities have a preshared secret.

3.3. Password Guessing Attack. Due to the importance of password in authentication process and its large adoption by numerous authentication protocols, pirates have invented various attacks to get the correct one. Hence, the most used attack is password guessing. Particularly, this attack can be executed either online or offline. In this attack, an attacker eavesdrops on the communication between two entities during authentication phase to get some useful values. Then, attacker must guess all probable passwords to succeed in the authentication [60, 69–75].

3.4. Spoofing Attack. In the network security context, spoofing attack is a situation when an unauthorized entity produces falsified parameter [76]. The goal of this attack is to make servers believe that the attacker is an authorized entity [62]. So, the pirate gains the trust of the authority. For example, in smart health, the pirate can send fake information to authentication server. So, if he performed the authentication phase successfully, he can request victim's sensor and then get the secret health information about this victim [38, 77–79].

3.5. Insider Attack. In cyber security field, insider attack occurs when a legitimate entity that has an authorized access tries to harm the system. The action of authorized entity can be either intentional or accidental [80–84]. In both cases, the system is considered vulnerable and we should find out the solution in the short term. According to [85], more than 57%

of confidential business data are targeted by insider attack. On the other hand, the study [86] confirms that more than 60% of existing attacks have been completed by insider.

4. Required Security Services for IoT

After debating various security attacks applied by attackers, this section mentions some security services. Thus, the objective of this section is to discuss the security requirements for IoT devices. As illustrated in Table 1, IoT solutions must come with some basic security services including authorization, authentication, confidentiality, availability, integrity, and non-repudiation.

4.1. Confidentiality. Generally, confidentiality can be defined as the capability and aptitude to prevent an unauthorized user to access private data. Therefore, it promises and guarantees that the personal information is only consulted, edited, or removed by authorized entity [38]. Particularly, in the Internet of Things network, confidentiality is one of the significant security services. However, the confidentiality is the most attacked service [87]. For example, viruses, spywares, and Trojans are considered as malware applications that attack the confidentiality of the user's private data. They can interact with system as executable codes or scripts with the aim to have an unauthorized access [88].

In an IoT context, for warranting and assuring the confidentiality of personal information captured by sensors and for preventing them from being discovered by the third party, the encryption algorithms and cryptographic methods can be used [89]. Therefore, all transmitted data between two devices must be encrypted. As a result, nobody can understand the message except legitimate entities [90].

4.2. Availability. An alternative required security service of IoT is the availability of resources to the legitimate entities independent of where and when they exist. Availability denotes that the resources and information must be easily reached by the legitimate user when he wants [91]. Moreover, in the IoT architecture, the sensor is available if it can communicate the sensed values in real time.

Likewise, the availability of an actuator means that it can execute user received commands immediately without any remarkable delay.

The availability of some particular resources could be interrupted as consequences of usage of dissimilar data transmission channel, networks, and protocols [46]. On the other hand, for damaging the availability, attackers may use three main malicious attacks including denial of service (DOS) attack, flooding attack, or black hole attack. For the first one, it is probably practiced in the availability situation. Pirates can use the simple denial of service (DOS) attack or distributed denial of service (DDOS) attack that necessitates the collaboration between various resources. For the flooding attack, the attacker can flood the networks by unwanted messages and commands for exhausting device resources. This attack not only targets bandwidth but also decreases CPU and memory capabilities. So, the device will not be reached or the communication will be slow [92].

Table 1: Security requirements for IoT basic layers.

Security services	IoT layers		
	Perception	Networking	Application
Authentication	✓	✓	✓
Authorization	✓	✓	✓
Confidentiality	✓		
Availability	✓	✓	
Integrity	✓	✓	✓
Non-repudiation		✓	

In order to guarantee the availability of appropriate resources, we can select distributed approach for operating the system and use numerous platforms which simplify the incorporation of various systems remotely [76].

4.3. Authentication. Authentication service is considered the biggest challenge in the IoT network. It includes verification of identity. On the one hand, in the authentication procedure, the devices must be able to check the validity and legitimacy of remote use in a public network. On the other hand, authentication prevents unauthorized person to take part in a private secured communication [38]. Previous authentication schemes are based on single factor that is a simple password. However, these schemes have to face various issues related to the password. First of all, users can easily forget the password. Secondly, users may have weak password. Finally, attackers are able to guess the correct password, either using exhaustive research attack or dictionary attack. Accordingly, password-based authentication is not enough to promise security. In our days, authentication schemes based on smart card offer multifactor authentication [4–9]. Typically, the system requires two factors including a valid smart card and correct preshared secret. Even so, it comprises the use of biometric print.

Due to the important position of authentication mechanism in the Internet of Things security, we have reserved the two following sections for discussing various techniques used for authentication in IoT and for studying some proposed IoT authentication schemes.

4.4. Authorization. With the growth of number of connected objects to the Internet network, authorization is becoming a critical issue in the IoT system. In fact, it refers to the security service responsible for determining user right and privileges (read, write, or delete). It identifies also the access control rules to allow or deny permissions to the IoT devices. Thus, the challenge is to prevent users with limited privileges to get additional ones to have an unauthorized access to devices and their data [93–97].

4.5. Integrity. Integrity means that the message was not reformed by an unauthorized entity in the transmission session. So, it guarantees that the receiver has received exactly what the source has sent. The main objective is to stop an unauthorized object doing illegal modification.

For sustaining the safety of smart devices in IoT network, the system should guarantee data integrity. Therefore, neither unauthorized objects nor user access should be granted. Besides, the cryptography and encryption mechanisms can be applied when the transmitted data are very important [37]. For instance, the authors of [98] suggested the usage of HMAC-SHA 256 algorithm for reassuring data integrity.

4.6. Non-Repudiation. Non-repudiation is one of the security aspects, which insures that communication members have ability to send or receive information in its integrality [99]. In addition, it makes confident that the transfer of data or identifications between two IoT objects is undeniable [100]. Non-repudiation guarantees to a source node to send its data, as well as to a receiving node to confirm that the received data are matching with data's source [34].

5. IoT Authentication Techniques

Due to the ability of IoT to access to all users' information, the user's private life must be protected against the malicious attacks. Furthermore, the devices should not be accessed by unauthorized users. So, it is necessary to check the user's identity before getting the authorization. Hence, the verification of user's identity can be done in many ways. Nevertheless, the most frequently used is authentication system, which is based on the prior sharing secrets, keys, or passwords. Consequently, in this section, we review the techniques that are applied for reinforcing the authentication in IoT environment.

5.1. One Time Password Authentication. One time password (OTP) which is also called dynamic password is a password that is valid for authentication in one transaction. In the literature survey, various OTP authentication protocols are proposed for securing the communication in IoT environment. These protocols are founded based on various mechanisms such as time synchronization, hash factions (MD5, SHA1, and SHA256), and cryptography RSA. Besides, they are all based on the OTP algorithm created by Lamport [101–104]. Unfortunately, these protocols are vulnerable against some attacks as described in [105–108].

On the other hand, for reinforcing the OTP authentication, Lee and Kim [109] proposed in 2013 an insider attack-resistant OTP scheme based on bilinear maps. However, it needs complex computation. Based on this problem, Shivraj et al. [110] proposed a robust OTP scheme for IoT. The proposed protocol uses the principles of lightweight identity-based elliptic curve cryptography and Lamport's OTP algorithm.

5.2. ECC-Based Mutual Authentication. Generally, IoT devices have a limited resources. Besides, the communication between sensors, actuators, objects, and nodes must be in real time. For these reasons, it is indispensable to propose a lightweight authentication protocol for IoT. Accordingly, Azrour et al. [71] proposed an efficient authentication scheme for IoT. This protocol is based on elliptic curve cryptography (ECC) which is measured better than the traditional RSA encryption algorithm. Furthermore, in addition, various authentication protocol based on ECC are proposed in [111–115]. Elliptic curve cryptography is considered more efficient and more secure especially for systems with limited memory and processing capabilities.

5.3. ID- and Password-Based Authentication. ID-based authentication is an approach for distinguishing authorized entities from illegal ones. According to ID, the user is either allowed or denied to access the resource. User ID refers to all attributes that can characterize one user form another, for instance, username, e-mail, phone number, IP address, etc. In IoT environment, numerous protocols are proposed [74, 116–118] based on this technique. However, this method is generally adopted in the server/client authentication architecture. In view of that, a server is required in IoT environment for storing user's ID and secret in server's database.

On the other hand, the usage of ID-based authentication approach has some issues that are detailed in following lines. Firstly, how user's data are stored in server? Is the server capable to protect them against stolen verifier attack and insider attack? Secondly, users may forget their authentication parameters. Therefore, they cannot perform the next authentication. In this case, it is not suitable to save personal ID in an electronic device (laptop, tablet, and smartphone), even if it is not connected to public network. Thirdly, the transmission of user ID in public network is another challenge. In this situation, the hash functions or cryptography algorithm are recommended.

5.4. Certificate-Based Authentication. For addressing problems of ID- and password-based authentication, an alternative approach was proposed [119]. This technique is called certificate-based authentication. Certificate-based authentication has been commonly adopted by multiple applications. For example, in order to verify user's identity in banking application, Hiltgen et al. [120] proposed a new certificate-based authentication scheme. This approach has been also used in IoT environment [120–124]. Although certificate-based authentication provides more security, device certificate processing and used algorithms necessitate a high processing resource, which is not always available in IoT devices. As a result, this approach is not suitable for IoT objects [125].

5.5. Blockchain. Blockchain is a particular sort of database. It is different from a traditional database because of the specific way in which it stores data. Blockchains save data in a series of blocks that are then linked to each other. In recent years, different authors have taken advantage of this recent technology to propose authentication protocol for IoT [22, 31–33, 126, 127]. The sustainability and verification of the data stored in the blockchain provide

Table 2: Classification of some IoT authentication schemes.

Protocol	Proposed for securing		Method used			
	IoT	WSN	Encryption algorithm	Random number	Hash function	Others
[128]	—	✓	—	—	✓	—
[129]	✓	—	—	—	—	Time synchronization
[110]	✓	—	ECC	—	—	Lamport's OTP algorithm
[109]	—	—	—	✓	—	Zero-knowledge proof
[104]	—	—	AES-based MAC	—	—	—
[130]	✓	✓	ECC	—	✓	—
[131]	✓	✓	ECC	—	✓	Smart card
[132]	✓	—	ECC	✓	✓	—
[133]	✓	—	—	—	✓	—
[134]	✓	—	AES	—	—	—
[83]	✓	—	Symmetric encryption	—	—	—
[15]	✓	—	—	✓	✓	Fuzzy extractor mechanism
[20]	✓	—	ECC	✓	✓	Challenge-response
[135]	✓	—	Symmetric encryption	✓	✓	Blockchain machine learning
[136]	✓	—	ECC	✓	✓	-

ECC: elliptic curve cryptography; AES: Advanced Encryption Standard; OTP: one time password; WSN: wireless sensor network.

Table 3: Advantages and limitations in some IoT-based authentication schemes.

Protocol	Advantages	Limitations
[113]	Is lightweight	Uses only hash function
[114]	Can detect man-in-the-middle attacks	Uses certificates that need an important space in memory
[90]	Can be implemented in real-time IoT networks Based on two-factor authentication	Vulnerable
[89]	Can deal against insider attack based on bilinear maps	Needs complex computation
[84]	Surpasses HOTP	Is heavyweight Not efficient for IoT devices
[115]	Offers mutual authentication	Vulnerable against some attacks
[116]	Guarantees authentication and session key exchange	Does not cover all IoT service requirements
[74]	Can be used with cloud servers	Cannot resist all attacks
[117]	Very lightweight	Based only on one hash function
[118]	Lightweight mutual authentication	Operates only in CoAP-based IoT environment
[119]	Can be used for authentication protocol for IoT-based RFID systems	The running time of protocol is not very fast

the confidence to use accurately recorded data in the future and at the same time provide transparency, anonymity, and traceability.

Multiple and different authentication methods are used in the IoT environment. As demonstrated in Table 2, the majority of proposed IoT authentication protocols are based on encryption cryptography. In this situation, two types of cryptography are used. The first type is asymmetric encryption algorithm such as ECC, while the second one is symmetric encryption algorithm like AES. Furthermore, the hash functions are utilized in some authentication for hashing essential parameters. Finally, the random numbers are also adopted in certain protocol as they can be used to ensure the freshness of messages.

On the other hand, the advantages and limitations of some selected IoT authentication protocols are depicted in Table 3. As we can notice, the protocol is considered effective only if it is lightweight as well as fulfils all security requirements. To sum up, we can conclude that the running time and processing time are important due to the limitation capability of IoT devices.

6. Conclusions

Internet of Things has a significant role in the rapid development that recent technology has known recently. These technologies have made the exchange of data easier. However, the security of user's data should not be ignored. Accordingly, the study performed in this paper is mainly focused on the security of IoT technology. Hence, as we have mentioned before, IoT suffers from several attacks, namely, DOS, password guessing, replay, and insider attacks. Authentication is the first security services that IoT has to satisfy, so we have detailed the authentication approaches adopted for IoT. The most techniques used for rienforcing the authentication are one time password, ECC-based mutual authetication, ID-based authentication, certificate-based authentication, and blockchain. After comparing recent authentication protocols, we have concluded that the majority of them is based on encryption cryptography.

Finally, in our future work, we will try to enhance the security of IoT environment by proposing secure and efficient IoT authentication schemes.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

[1] "Strategy analytics: internet of things now numbers 22 billion devices but where is the revenue? strategy analytics online newsroom." https://news.strategyanalytics.com/press-release/iot-ecosystem/strategy-analytics-internet-things-now-numbers-22-billion-devices-where (accessed Feb. 23, 2020).

[2] K. K. Patel, S. M. Patel, and P. Scholar, "Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges," *International journal of engineering science and computing*, vol. 6, 2016.

[3] O. Vermesan and P. Friess, *Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems*, River publishers, Denmark, 2013.

[4] M. Rana, A. Shafiq, I. Altaf et al., "A secure and lightweight authentication scheme for next generation IoT infrastructure," *Computer Communications*, vol. 165, pp. 85–96, 2021.

[5] S. A. Chaudhry, K. Yahya, F. Al-Turjman, and M.-H. Yang, "A secure and reliable device access control scheme for IoT based sensor cloud systems," *IEEE Access*, vol. 8, pp. 139244–139254, 2020.

[6] A. Irshad, S. A. Chaudhry, O. A. Alomari, K. Yahya, and N. Kumar, "A novel pairing-free lightweight authentication protocol for mobile cloud computing framework," *IEEE Syst. J.*vol. 99, pp. 1–9, 2020.

[7] Z. Ali, S. A. Chaudhry, K. Mahmood, S. Garg, Z. Lv, and Y. B. Zikria, "A clogging resistant secure authentication scheme for fog computing services," *Computer Networks*, vol. 185, Article ID 107731, 2021.

[8] S. A. Chaudhry, M. S. Farash, N. Kumar, and M. H. Alsharif, "PFLUA-DIoT: a pairing free lightweight and unlinkable user access control scheme for distributed IoT environments," *IEEE Syst. J.*vol. 99, pp. 1–8, 2020.

[9] A. Irshad, M. Usman, S. A. Chaudhry, H. Naqvi, and M. Shafiq, "A provably secure and efficient authenticated key agreement scheme for energy internet-based vehicle-to-grid technology framework," *IEEE Transactions on Industry Applications*, vol. 56, no. 4, pp. 4425–4435, 2020.

[10] A. Khan, V. Kumar, M. Ahmad, S. Rana, and D. Mishra, "PALK: password-based anonymous lightweight key agreement framework for smart grid," *International Journal of Electrical Power & Energy Systems*, vol. 121, Article ID 106121, 2020.

[11] S. A. Chaudhry, I. L. Kim, S. Rho, M. S. Farash, and T. Shon, "An improved anonymous authentication scheme for distributed mobile cloud computing services," *Cluster Computing*, vol. 22, no. 1, pp. 1595–1609, 2019.

[12] A. Irshad, M. Usman, S. A. Chaudhry, A. K. Bashir, A. Jolfaei, and G. Srivastava, "Fuzzy-in-the-Loop-Driven low-cost and secure biometric user access to server," *IEEE Transactions on Reliability*, vol. 70, no. 3, 2020.

[13] B. Alzahrani, A. Irshad, K. Alsubhi, and A. Albeshri, "A secure and efficient remote patient-monitoring authentication protocol for cloud-IoT," *International Journal of Communication Systems*, vol. 33, no. 11, Article ID e4423, 2019.

[14] S. Atiewi, A. Al-Rahayfeh, M. Almiani et al., "Scalable and secure big data IoT system based on multifactor authentication and lightweight cryptography," *IEEE Access*, vol. 8, pp. 113498–113511, 2020.

[15] M. Wazid, A. K. Das, V. Bhat K, and A. V. Vasilakos, "LAM-CIoT: lightweight authentication mechanism in cloud-based IoT environment," *Journal of Network and Computer Applications*, vol. 150, Article ID 102496, 2020.

[16] 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.

[17] M. Anuradha, T. Jayasankar, N. B. Prakash et al., "IoT enabled cancer prediction system to enhance the authentication and security using cloud computing," *Microprocessors and Microsystems*, vol. 80, Article ID 103301, 2021.

[18] M. Shahidinejad, G. Arani, A. Souri, M. Shojafar, and S. Kumari, "Light-edge: a lightweight authentication protocol for IoT devices in an edge-cloud environment," *IEEE Consumer Electronics Magazine*, vol. 2021, Article ID 3053543, 2021.

[19] M. Shahidinejad, G. Arani, A. Souri, M. Shojafar, and S. Kumari, "A technical report for light-edge: a lightweight authentication protocol for IoT devices in an edge-cloud environment," 2021, http://arxiv.org/abs/210106676.

[20] L. Loffi, C. M. Westphall, L. D. Grüdtner, and C. B. Westphall, "Mutual authentication with multi-factor in IoT-Fog-Cloud environment," *Journal of Network and Computer Applications*, vol. 176, Article ID 102932, 2021.

[21] B. D. Deebak and F. Al-Turjman, "Lightweight authentication for IoT/Cloud-based forensics in intelligent data computing," *Future Generation Computer Systems*, vol. 116, pp. 406–425, 2021.

[22] J. A. Alzubi, "Blockchain-based lamport merkle digital signature: authentication tool in IoT healthcare," *Computer Communications*, vol. 170, pp. 200–208, 2021.

[23] P. Kumar and L. Chouhan, "A privacy and session key based authentication scheme for medical IoT networks," *Computer Communications*, vol. 166, pp. 154–164, 2021.

[24] D. Deebak and F. Al-Turjman, "Secure-user sign-in authentication for IoT-based eHealth systems," *Complex & Intelligent Systems*, pp. 1–21, 2021.

[25] H. Luo, C. Wang, H. Luo, F. Zhang, F. Lin, and G. Xu, "G2F: a secure user authentication for rapid smart home IoT management," *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10884–10895, 2021.

[26] P. Kumar and L. Chouhan, "A secure authentication scheme for IoT application in smart home," *Peer-to-Peer Networking and Applications*, vol. 14, no. 1, pp. 420–438, 2021.

[27] B. Alemu, R. Kumar, D. Sinwar, and G. Raghuwanshi, "Fingerprint based authentication architecture for accessing multiple cloud computing services using single user credential in IOT environments," *Journal of Physics: Conference Series*, vol. 1714, no. 1, Article ID 012016, 2021.

[28] M. I. Ahmed and G. Kannan, "Cloud-based remote RFID authentication for security of smart internet of things applications," *Journal of Information and Knowledge Management*, vol. 20, Article ID 2140004, 2021.

[29] M. Torabi and A. Shahidinejad, "A mutual authentication protocol for IoT users in cloud environment," *Electron Cyber Defense*, vol. 9, 2021.

[30] M. B. Mu'azu, "SIMP-REAUTH: a simple multilevel real user remote authentication scheme for mobile cloud computing," in *Proceedings of the Information and Communication Technology and Applications: Third International Conference, ICTA 2020*, November 2020.

[31] C. M. S. Ferreira, C. T. B. Garrocho, R. A. R. Oliveira, J. S. Silva, and C. F. M. d. C. Cavalcanti, “IoT registration and authentication in smart city applications with blockchain,” *Sensors*, vol. 21, no. 4, 1323 pages, 2021.

[32] U. Narayanan, V. Paul, and S. Joseph, “Decentralized blockchain based authentication for secure data sharing in Cloud-IoT,” *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–19, 2021.

[33] H. Honar Pajooh, M. Rashid, F. Alam, and S. Demidenko, “Multi-layer blockchain-based security architecture for internet of things,” *Sensors*, vol. 21, no. 3, 772 pages, 2021.

[34] D. Airehrour, J. Gutierrez, and S. K. Ray, “Secure routing for internet of things: a survey,” *Journal of Network and Computer Applications*, vol. 66, pp. 198–213, 2016.

[35] M. Ammar, G. Russello, and B. Crispo, “Internet of things: a survey on the security of IoT frameworks,” *Journal of Information Security and Applications*, vol. 38, pp. 8–27, 2018.

[36] Y. Atwady and M. Hammoudeh, “A survey on authentication techniques for the internet of things,” in *Proceedings of the International Conference on Future Networks and Distributed Systems*, Cambridge, United Kingdom, July 2017.

[37] S. Hong, “Authentication techniques in the internet of things environment: a survey,” *International Journal of Security and Networks*, vol. 21, no. 3, pp. 462–470, 2019.

[38] S. Panchiwala and M. Shah, “A comprehensive study on critical security issues and challenges of the IoT world,” *Journal of Digital Information Management*, vol. 2, no. 4, pp. 257–278, 2020.

[39] P. P. Ray, “A survey on internet of things architectures,” *Journal of King Saud University - Computer and Information Sciences*, vol. 30, no. 3, pp. 291–319, 2018.

[40] M. Heydari, A. Mylonas, V. H. F. Tafreshi, E. Benkhelifa, and S. Singh, “Known unknowns: indeterminacy in authentication in IoT,” *Future Generation Computer Systems*, vol. 111, pp. 278–287, 2020.

[41] F. H. Al-Naji and R. Zagrouba, “A survey on continuous authentication methods in Internet of Things environment,” *Computer Communications*, vol. 163, pp. 109–133, 2020.

[42] R. Yugha and S. Chithra, “A survey on technologies and security protocols: reference for future generation IoT,” *Journal of Network and Computer Applications*, vol. 169, Article ID 102763, 2020.

[43] M. Mehta and K. Patel, “A review for IOT authentication - current research trends and open challenges,” *Materials Today: Proceedings*, Article ID S2214785320384960, 2020.

[44] N. Yousefnezhad, A. Malhi, and K. Främling, “Security in product lifecycle of IoT devices: a survey,” *Journal of Network and Computer Applications*, vol. 171, Article ID 102779, 2020.

[45] K. Sha, T. A. Yang, W. Wei, and S. Davari, “A survey of edge computing-based designs for IoT security,” *Digital Communications and Networks*, vol. 6, no. 2, pp. 195–202, 2020.

[46] S. Kumar, P. Tiwari, and M. Zymbler, “Internet of things is a revolutionary approach for future technology enhancement: a review,” *Journal of Big Data*, vol. 6, no. 1, 111 pages, 2019.

[47] M. Burhan, R. Rehman, B. Khan, and B.-S. Kim, “IoT elements, layered architectures and security issues: a comprehensive survey,” *Sensors*, vol. 18, no. 9, 2796 pages, 2018.

[48] H. F. Atlam, R. J. Walters, and G. B. Wills, “Internet of things: state-of-the-art, challenges, applications, and open issues,” *International Journal of Intelligent Computing Research*, vol. 9, no. 3, pp. 928–938, 2018.

[49] J. Mabrouki, M. Azrour, G. Fattah, D. Dhiba, and S. E. Hajjaji, “Intelligent monitoring system for biogas detection based on the internet of things: mohammedia, Morocco city landfill case,” *Big Data Mining and Analytics*, vol. 4, no. 1, pp. 10–17, 2021.

[50] J. Mabrouki, M. Azrour, D. Dhiba, Y. Farhaoui, and S. E. Hajjaji, “IoT-based data logger for weather monitoring using arduino-based wireless sensor networks with remote graphical application and alerts,” *Big Data Mining and Analytics*, vol. 4, no. 1, pp. 25–32, 2021.

[51] P. Visconti, N. I. Giannoccaro, R. d. Fazio, S. Strazzella, and D. Cafagna, “IoT-oriented software platform applied to sensors-based farming facility with smartphone farmer app,” *Bulletin of Electrical Engineering and Informatics*, vol. 9, no. 3, pp. 1095–1105, Article ID 3, 2020.

[52] H. Andrianto, S. Suhardi, and A. Faizal, “Performance evaluation of low-cost IoT based chlorophyll meter,” *Bulletin of Electrical Engineering and Informatics*, vol. 9, no. 3, pp. 956–963, Article ID 3, 2020.

[53] M. Alilou, B. Tousi, and H. Shayeghi, “Home energy management in a residential smart micro grid under stochastic penetration of solar panels and electric vehicles,” *Solar Energy*, vol. 212, pp. 6–18, 2020.

[54] M. S. Aliero, K. N. Qureshi, M. F. Pasha, and G. Jeon, “Smart home energy management systems in internet of things networks for green cities demands and services,” *Environmental Technology & Innovation*, vol. 22, Article ID 101443, 2021.

[55] H. Kim, H. Choi, H. Kang, J. An, S. Yeom, and T. Hong, “A systematic review of the smart energy conservation system: from smart homes to sustainable smart cities,” *Renewable and Sustainable Energy Reviews*, vol. 140, Article ID 110755, 2021.

[56] J. Mabrouki, M. Azrour, Y. Farhaoui, and S. El Hajjaji, “Intelligent system for monitoring and detecting water quality,” in *Big Data And Networks Technologies*, Y. Farhaoui, Ed., vol. 81, pp. 172–182, Springer International Publishing, Cham, 2020.

[57] J. Mabrouki, M. Azrour, and S. El, “Use of internet of things for monitoring and evaluation water’s quality: comparative study,” *International Journal of Cloud Computing*, 2021, In press.

[58] S. Prabhakar, “Network security in digitalization: attacks and defence,” *International Journal of Research in Computer Applications and Robotics*, vol. 5, no. 5, pp. 46–52, 2017.

[59] 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.

[60] H. C. Hasan, F. N. Yusof, and M. Daud, “Comparison of authentication methods in internet of things technology,” *International Journal of Computer and Systems Engineering*, vol. 12, no. 3, pp. 231–234, 2018.

[61] A. Ahmed, R. Latif, S. Latif, H. Abbas, and F. A. Khan, “Malicious insiders attack in IoT based multi-cloud e-healthcare environment: a systematic literature review,” *Multimedia Tools and Applications*, vol. 77, no. 17, pp. 21947–21965, 2018.

[62] K. C. Archana and N. Harini, “Mitigation of spoofing attacks on IOT home networks,” *International Journal of Engineering and Advanced Technology*, vol. 9, no. 1S, pp. 240–245, 2019.

[63] Y. Javed, A. S. Khan, A. Qahar, and J. Abdullah, “Preventing DoS attacks in IoT using AES,” *Journal of Telecommunication, Electronic and Computer Engineering*, vol. 9, no. 3–11, pp. 3–11, 2017.

[64] H. C. A. van Tilborg and S. Jajodia, *Encyclopedia of Cryptography and Security*, Springer US, Boston, MA, 2011.

[65] M. Conti, N. Dragoni, and V. Lesyk, “A survey of man in the middle attacks,” *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2027–2051, 2016.

[66] S. Behrooz and S. Marsh, “A trust-based framework for information sharing between mobile health care applications,” *Trust Management X*, in *Proceedings of the IFIP International Conference on Trust Management*, pp. 79–95, Darmstadt, Germany, July 2016.

[67] P. Rughoobur and L. Nagowah, “A lightweight replay attack detection framework for battery depended IoT devices designed for healthcare,” in *Proceedings of the 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions)(ICTUS)*, pp. 811–817, Dubai, United Arab Emirates, December 2017.

[68] Y. Feng, W. Wang, Y. Weng, and H. Zhang, “A replay-attack resistant authentication scheme for the internet of things,” in *Proceedings of the 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, pp. 541–547, Guangzhou, China, July 2017.

[69] M. Azrour, Y. Farhaoui, and M. Ouanan, “Cryptanalysis of farash et al.’s SIP authentication protocol,” *International Journal of Dynamical Systems and Differential Equations*, vol. 8, no. 1/2, 2018.

[70] M. Azrour, Y. Farhaoui, and A. Guezzaz, “Experimental validation of new SIP authentication protocol,” in *Big Data And Networks Technologies*, Y. Farhaoui, Ed., vol. 81, pp. 1–11, Springer International Publishing, Cham, 2020.

[71] M. Azrour, J. Mabrouki, A. Guezzaz, and Y. Farhaoui, “New enhanced authentication protocol for internet of things,” *Big Data Mining and Analytics*, vol. 4, no. 1, pp. 1–9, 2021.

[72] P. K. Roy, K. Parai, and A. Hasnat, “User authentication with session key interchange for wireless sensor network,” in *Methodologies and Application Issues of Contemporary Computing Framework*, J. K. Mandal, S. Mukhopadhyay, P. Dutta, and K. Dasgupta, Eds., Springer Singapore, Singapore, pp. 153–165, 2018.

[73] J. Moon, T. Song, D. Lee, Y. Lee, and D. Won, “Cryptanalysis of chaos-based 2-party key agreement protocol with provable security,” in *Advances in Human Factors in Cybersecurity*, D. Nicholson, Ed., vol. 593, pp. 72–77, Springer International Publishing, Cham, 2018.

[74] K. Park, S. Lee, Y. Park, and Y. Park, “An ID-based remote user authentication scheme in IoT,” *Journal of Korea Multimedia Society*, vol. 18, no. 12, pp. 1483–1491, 2015.

[75] J. Ryu, H. Lee, H. Kim, and D. Won, “Improvement of Wu et al.’s three-factor user authentication scheme for wireless sensor networks,” , 2018.

[76] K. Somasundaram and K. Selvam, “Iot - attacks and challenges,” *International Journal of Engineering and Technical Research (IJETR)*, vol. 8, no. 9, pp. 9–12, 2018.

[77] R. Z. Naeem, S. Bashir, M. F. Amjad, H. Abbas, and H. Afzal, “Fog computing in internet of things: practical applications and future directions,” *Peer-to-Peer Networking and Applications*, vol. 12, no. 5, pp. 1236–1262, 2019.

[78] T. Sherasiya, H. Upadhyay, and H. B. Patel, “A survey: intrusion detection system for internet of things,” *International Journal of Computer Science and Engineering (IJCSE)*, vol. 5, 2006.

[79] M. Nikooghadam and H. Amintoosi, “Secure communication in CloudIoT through design of a lightweight authentication and session key agreement scheme,” *International Journal of Communication Systems*, Article ID e4332, 2020.

[80] F. Kammüller, J. R. C. Nurse, and C. W. Probst, “Attack tree analysis for insider threats on the IoT using isabelle,” in *Human Aspects of Information Security, Privacy, and Trust*, T. Tryfonas, Ed., vol. 9750, Springer International Publishing, Lecture Notes in Computer Science, pp. 234–246, 2016.

[81] G. Sharma and S. Kalra, “Identity based secure authentication scheme based on quantum key distribution for cloud computing,” *Peer-to-Peer Networking and Applications*, vol. 11, no. 2, pp. 220–234, 2018.

[82] S.-Q. Cao, Q. Sun, and L.-L. Cao, “Security analysis and enhancements of a remote user authentication scheme,” *IOP Conference Series: Materials Science and Engineering*, vol. 719, Article ID 012004, 2019.

[83] K. Mansoor, A. Ghani, S. A. Chaudhry, S. Shamshirband, S. A. K. Ghayyur, and E. Salwana, “Securing IoT based RFID systems: a robust authentication protocol using symmetric cryptography,” *Mathematics & Computer Science*, vol. 19, Article ID 4752, 2019.

[84] S. Holger, “Insider threat report,” *Cybersecurity Insiders*, Accessed: Aug. 13, 2020. [Online, 2019.

[85] I. B. M. X-Force® Research, *Cyber Security Intelligence Index*, Accessed: Jun. 02, 2017. [Online, 2016.

[86] N. Ye, Y. Zhu, R.-c. Wang, R. Malekian, and L. Qiao-min, “An efficient authentication and access control scheme for perception layer of internet of things,” *Applied Mathematics & Information Sciences*, vol. 8, no. 4, pp. 1617–1624, 2014.

[87] R. Canzanese, M. Kam, and S. Mancoridis, “Toward an automatic, online behavioral malware classification system,” in *Proceedings of the IEEE 7th International Conference on Self-Adaptive and Self-Organizing Systems (SASO)*, pp. 111–120, Philadelphia, PA, USA, September 2013.

[88] Y. Javed, A. S. Khan, A. Qahar, and J. Abdullah, “Preventing DoS attacks in IoT using AES,” *J. Telecommun. Electron. Comput. Eng. JTEC*, vol. 9, no. 3–11, pp. 3–11, 2017.

[89] G. Sharma and S. Kalra, “A lightweight multi-factor secure smart card based remote user authentication scheme for cloud-IoT applications,” *Journal of Information Security and Applications*, vol. 42, pp. 95–106, 2018.

[90] M. Azrour, Y. Farhaoui, and M. Ouanan, “A server spoofing attack on Zhang et al. SIP authentication protocol,” *Int. J. Tomogr. Simulation^{TM}*, vol. 30, no. 3, pp. 47–58, 2017.

[91] M. Domb, “Smart home systems based on internet of things,” *in Internet of Things (IoT) for Automated and Smart Applications*, IntechOpen, London, UK, 2019.

[92] T. Shah and S. Venkatesan, “Authentication of IoT device and IoT server using secure vaults,” in *Proceedings of the 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, pp. 819–824, New York, NY, USA, August 2018.

[93] O. Garcia-Morchon, S. Kumar, and M. Sethi, “Internet of Things (IoT) security: state of the art and challenges,” *RFC Editor*, vol. RFC8576, 2019.

[94] M. Wu, J. Chen, and R. Wang, “An enhanced anonymous password-based authenticated key agreement scheme with formal proof,” *IJ Network Security*, vol. 19, no. 5, pp. 785–793, 2017.

[95] A. Drissi and A. Asimi, “Behavioral and security study of the OHFGC hash function,” *ReCALL*, vol. 1, no. 0, 2017.

[96] C.-W. Liu, C.-Y. Tsai, and M.-S. Hwang, “Cryptanalysis of an efficient and secure smart card based password authentication scheme,” in *Recent Developments in Intelligent Systems and Interactive Applications*, F. Xhafa, S. Patnaik, and Z. Yu, Eds., vol. 541, pp. 188–193, Springer International Publishing, Cham, 2017.

[97] A. Jebrane, A. Toumanari, N. Meddah, and M. Bousseta, “A new efficient authenticated and key agreement scheme for sip using digital signature algorithm on elliptic curves,” *Journal of Telecommunications and Information Technology*, vol. 2, pp. 62–68, 2017.

[98] J. Ni, K. Zhang, X. Lin, and X. Shen, “Securing fog computing for internet of things applications: challenges and solutions,” *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 601–628, 2018.

[99] V. Umadevi, R. Chezhian, and Z. U. Khan, “Security requirements in mobile ad-hoc networks,” *Int J Adv Res Comput Commun*, vol. 1, no. 2, 2012.

[100] M. G. Samaila, M. Neto, D. A. B. Fernandes, M. M. Freire, and P. R. M. Inácio, “Challenges of securing internet of things devices: a survey,” *Security and Privacy*, vol. 1, no. 2, e20 pages, 2018.

[101] D. M’Raihi, S. Machani, M. Pei, and J. Rydell, “Totp: time-based one-time password algorithm,” *Internet Req. Comments*, 2011.

[102] D. M’Raihi, M. Bellare, F. Hoornaert, D. Naccache, and O. Ranen, “Hotp: an hmac-based one-time password algorithm,” *Internet Soc. Netw. Work. Group RFC4226*, 2005.

[103] B. Hamdane, A. Serhrouchni, A. Montfaucon, and S. Guemara, “Using the hmac-based one-time password algorithm for tls authentication,” in *Proceedings of the 2011 Conference on Network and Information Systems Security*, pp. 1–8, La Rochelle, France, May 2011.

[104] S.-D. Park, J.-C. Na, Y.-H. Kim, and D.-K. Kim, “Efficient OTP (one time password) generation using AES-based MAC,” *J. Korea Multimed. Soc.*vol. 11, no. 6, pp. 845–851, 2008.

[105] P.-A. Fouque, G. Leurent, and P. Q. Nguyen, “Full key-recovery attacks on HMAC/NMAC-MD4 and NMAC-MD5,” in *Proceedings of the Annual International Cryptology Conference*, pp. 13–30, Santa Barbara, CA, USA, August 2007.

[106] E. Lee, D. Chang, J. Kim, J. Sung, and S. Hong, “Second preimage attack on 3-pass HAVAL and partial key-recovery attacks on HMAC/NMAC-3-pass HAVAL,” in *Proceedings of the International Workshop on Fast Software Encryption*, pp. 189–206, Lausanne, Switzerland, February 2008.

[107] J. Kim, A. Biryukov, B. Preneel, and S. Hong, “On the security of HMAC and NMAC based on HAVAL, MD4, MD5, SHA-0 and SHA-1 (extended abstract),” in *Proceedings of the International Conference on Security and Cryptography for Networks*, pp. 242–256, Lecture Notes in Computer Science, Maiori, Italy, September 2006.

[108] X. Wang, H. Yu, W. Wang, H. Zhang, and T. Zhan, “Cryptanalysis on hmac/nmac-md5 and md5-mac,” *Advances in Cryptology - EUROCRYPT 2009*, in *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 121–133, Zagreb, Croatia, April 2009.

[109] Y. Lee and H. Kim, “Insider attack-resistant otp (one-time password) based on bilinear maps,” *International Journal of Computer and Communication Engineering*, vol. 2, no. 3, pp. 304–308, 2013.

[110] V. L. Shivraj, M. A. Rajan, M. Singh, and P. Balamuralidhar, “One time password authentication scheme based on elliptic curves for Internet of Things (IoT),” in *Proceedings of the 2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW)*, pp. 1–6, Riyadh, Saudi Arabia, February 2015.

[111] M. Safkhani, N. Bagheri, S. Kumari, H. Tavakoli, S. Kumar, and J. Chen, “RESEAP: an ECC-based authentication and key agreement scheme for IoT applications,” *IEEE Access*, vol. 8, pp. 200851–200862, 2020.

[112] S. Chatterjee and S. G. Samaddar, “A robust lightweight ECC-based three-way authentication scheme for IoT in cloud,” in *Smart Computing Paradigms: New Progresses And Challenges*, pp. 101–111, Springer, Singapore, 2020.

[113] B. Hammi, A. Fayad, R. Khatoun, S. Zeadally, and Y. Begriche, “A lightweight ECC-based authentication scheme for Internet of Things (IoT),” *IEEE Systems Journal*, vol. 14, no. 3, pp. 3440–3450, 2020.

[114] A. Lohachab and Karambir, “ECC based inter-device authentication and authorization scheme using MQTT for IoT networks,” *Journal of Information Security and Applications*, vol. 46, pp. 1–12, 2019.

[115] M. A. Khan, M. T. Quasim, N. S. Alghamdi, and M. Y. Khan, “A secure framework for authentication and encryption using improved ECC for IoT-based medical sensor data,” *IEEE Access*, vol. 8, pp. 52018–52027, 2020.

[116] S. N. Swamy, D. Jadhav, and N. Kulkarni, “Security threats in the application layer in IOT applications,” in *Proceedings of the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, pp. 477–480, Palladam, India, February 2017.

[117] W.-q. Jiang, Z.-q. Huang, Y.-x. Yang, J. Tian, and L. Li, “ID-based authentication scheme combined with identity-based encryption with fingerprint hashing,” *The Journal of China Universities of Posts and Telecommunications*, vol. 15, no. 4, pp. 75–120, 2008.

[118] O. Salman, S. Abdallah, I. H. Elhajj, A. Chehab, and A. Kayssi, “Identity-based authentication scheme for the internet of things,” in *Proceedings of the 2016 IEEE Symposium on Computers and Communication (ISCC)*, pp. 1109–1111, Messina, Italy, June 2016.

[119] S. A. Nauroze, J. G. Hester, B. K. Tehrani et al., “Additively manufactured RF components and modules: toward empowering the birth of cost-efficient dense and ubiquitous IoT implementations,” *Proceedings of the IEEE*, vol. 105, no. 4, pp. 702–722, 2017.

[120] A. Hiltgen, T. Kramp and T. Weigold, Secure internet banking authentication,” *IEEE Security and Privacy Magazine*, vol. 4, no. 2, pp. 21–29, 2006.

[121] S. Malani, J. Srinivas, A. K. Das, K. Srinathan, and M. Jo, “Certificate-based anonymous device access control scheme for IoT environment,” *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 9762–9773, 2019.

[122] J. Choi, J. Cho, H. Kim, and S. Hyun, “Towards secure and usable certificate-based authentication system using a secondary device for an industrial internet of things,” *Applied Sciences*, vol. 10, no. 6, 1962 pages, 2020.

[123] Q. Zhang, K. Zhao, X. Kuang et al., “Multidomain security authentication for the Internet of things,” *Concurrency and Computation: Practice and Experience*, Article ID e5777, 2020.

[124] I. Ullah, N. U. Amin, M. A. Khan, H. Khattak, and S. Kumari, “An efficient and provable secure certificate-based combined signature, encryption and signcryption scheme for Internet

of Things (IoT) in Mobile Health (M-Health) system," *Journal of Medical Systems*, vol. 45, no. 1, pp. 1–14, 2021.

[125] Shuang and Y. Zhou, "A study of autonomous method of IoT component," in *Proceedings of the 5th International Conference on New Trends in Information Science and Service Science*, vol. 2, pp. 294–298, Macao, China, October 2011.

[126] P. Bagga, A. K. Sutrala, A. K. Das, and P. Vijayakumar, "Blockchain-based batch authentication protocol for internet of vehicles," *Journal of Systems Architecture*, vol. 113, Article ID 101877, 2021.

[127] W. Meng, W. Li, S. Tug, and J. Tan, "Towards blockchain-enabled single character frequency-based exclusive signature matching in IoT-assisted smart cities," *Journal of Parallel and Distributed Computing*, vol. 144, pp. 268–277, 2020.

[128] C.-H. Ling, C.-C. Lee, C.-C. Yang, and M.-S. Hwang, "A secure and efficient one-time password authentication scheme for WSN," *International Journal on Network Security*, vol. 19, no. 2, pp. 177–181, 2017.

[129] C. Tae-Ho and J. Garam-Moe, "A method for detecting man-in-the-middle attacks using time synchronization one time password in interlock protocol based internet of things," *Journal of Applied and Physical Sciences*, vol. 2, no. 2, pp. 37–41, 2016.

[130] H.-L. Yeh, T.-H. Chen, P.-C. Liu, T.-H. Kim, and H.-W. Wei, "A secured authentication protocol for wireless sensor networks using elliptic curves cryptography," *Sensors*, vol. 11, no. 5, pp. 4767–4779, 2011.

[131] A. Maurya and V. N. Sastry, "Fuzzy extractor and elliptic curve based efficient user authentication protocol for wireless sensor networks and internet of things," *Information*, vol. 8, no. 4, 136 pages, 2017.

[132] S. Kumari, M. Karuppiah, A. K. Das, X. Li, F. Wu, and N. Kumar, "A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers," *The Journal of Supercomputing*, vol. 74, no. 12, pp. 6428–6453, 2018.

[133] M. Bayat, M. Beheshti-Atashgah, M. Barari, and M. R. Aref, "Cryptanalysis and improvement of a user authentication scheme for internet of things using elliptic curve cryptography," *IJ Netw. Secur*, vol. 21, no. 6, pp. 897–911, 2019.

[134] M. A. Jan, P. Nanda, X. He, Z. Tan, and R. P. Liu, "A robust authentication scheme for observing resources in the internet of things environment," in *Proceedings of the 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 205–211, Washington, DC, USA, September 2014.

[135] H. Al-Naji and R. Zagrouba, "CAB-IoT: continuous authentication architecture based on blockchain for internet of things," *J. King Saud Univ.-Comput. Inf. Sci.*, 2020.

[136] S. Lu and X. Li, "Quantum-resistant lightweight authentication and key agreement protocol for fog-based microgrids," *IEEE Access*, vol. 9, pp. 27588–27600, 2021.