Indonesian Journal of Electrical Engineering and Informatics (IJEEI)
Vol. 12, No. 1, March 2024, pp. 15~31
ISSN: 2089-3272, DOI: 10.52549/ijeei.v12i1.5170

An Exhaustive Survey on Authentication Classes in the IoT Environments

Souhayla Dargaoui[1], Mourade Azrour[2], Ahmad El Allaoui[3], Azidine Guezzaz[4], Abdulatif Alabdulatif [5], Abdullah Alnajim[6]
[1,2,3]Engineering science and technology laboratory, IDMS Team, Faculty of Sciences and Techniques, Moulay Ismail University of Meknes, Errachidia, Morocco
[4]Higher School Essaouira, Cadi Ayyad University, Morocco
[5]Department of Computer Science, College of Computer, Qassim University, Buraydah, 51452, Saudi Arabia
[6]Department of Information Technology, College of Computer, Qassim University, Buraydah 51452, Saudi Arabia

Article Info

Article history:

Received Nov 17, 2023
Revised Dec 15, 2023
Accepted Jan 6, 2024

Keywords:

Internet of Things
Attacks
Security
Cryptography
Authentication

ABSTRACT

In today's world, devices are interconnected across various fields, ranging from intelligent buildings and smart cities to Industry 4.0 and smart healthcare. IoT security is still the biggest obstacle to deployment despite the exponential growth of IoT usage in our world. The principal objective of IoT security is to warrant the accessibility of services offered by an IoT environment, protect privacy, and confidentiality, and ensure the safety of IoT users, infrastructures, data, and devices. Authentication has become a top priority for everyone because it is the first line of defense against security threats and can allow or prevent users from accessing resources according to their legitimacy. Consequently, studying and researching authentication issues within IoT is extremely important. Our paper provides a comparative study of current IoT security research; it analyzes recent authentication protocols from 2018 to 2024. This survey's goal is to provide an IoT security research summary, the biggest susceptibilities, and attacks, the appropriate technologies, and the most used simulators.

Corresponding Author:

Souhayla Dargaoui,
Engineering science and technology laboratory, IDMS Team, Faculty of Sciences and Techniques, Moulay Ismail University of Meknes, Errachidia, Morocco.
Email: s.dargaoui@edu.umi.ac.ma

1. INTRODUCTION

Recently, the IoT has become a widely known buzzword in the information technology field. IoT is a big network of intelligent goods interconnected and connected to the internet, that may visualize and control a big part of the world that surrounds us. The concept of IoT was born at Carnegie Mellon University in 1982. Some students decided to connect a Coca-Cola distributor to the web to allow consumers to track its contents from afar; know if there were beverages available and be sure of their proper temperature. Nevertheless, the Auto-ID Labs at MIT executive director, Kiven Ashton, used the term Internet of Things for the first time in 1999, to describe a system of connected devices[1]. In 1994, Steve Mann invented WearCam. In addition, in 2000 electronics giant LG announced its intention to construct an intelligent fridge, which would detect on its own whether or not the food stored in it is restocked [2]. Meanwhile, between 2008 and 2009 interconnected object numbers overtook the worldwide population for the first time.

IoT has no unique definition or universal standards. From his perspective, the ITU defines IoT as "a global infrastructure for the Information Society that enables advanced services by interconnecting objects (physical or virtual) through existing or evolving interoperable information and communication technologies." [3]. Nonetheless, the ISO and IEC describe it as "an infrastructure of interconnected objects, people, systems and information resources, as well as intelligent services that enable them to process and respond to physical

and virtual information." [4]. The Internet of Things is a revolutionary paradigm that combines a lot of technologies that can make things (physical and virtual) recognizable and able to communicate with each other. At first, it was inspired by RFID technology which is critical for remedying identity issues of objects around us. Over time, the IoT integrates other technologies such as wireless sensor networks (WSN), communication technologies (LoRa, Sigfox, ZigBee, etc.), and cloud computing [5]–[9].

Over the past few years, IoT has immersed increasingly in our daily lives [10]–[13]. Righetti et al. [14] show the predicted progress in IoT use in a Smart City context. For example, air goodness and acclimatization, trafficking control, intelligent parking management, smart surveillance, and smart homes. Jabbar et al. [15] present a cost-effective and hybrid (local and remote) IoT-based home automation system with a user-friendly interface for smartphones and laptops. They developed a mock-up with a procedure for monitoring the condition of the home and controlling household instruments on the web whenever and wherever which they called IoT@HoMe. Quy et al. [16] Propose an ordinary structural framework using fog computing for the Internet of Medical Things (Fo-IoHT) use. Additionally, they proved that there ARE enormous opportunities for cloud computing-based IoHT applications.

This big integration of IoT services anywhere and everywhere produces significant data flow generation. As a result, various kinds of obstacles must be overcome before we can fully use the potentiality of IoT globally. Since data transport requires good connectivity, we can say that connectivity is one of the most critical IoT network challenges. However, several factors cause connectivity problems such as bandwidth, energy consumption, signaling, and standards. Similarly, to ensure the best performance regarding the high rates and repairs of appliances the designer of an IoT solution must consider future technological changes and maintain an equilibrium between hardware and software.

On the other hand, regarding the limited computational power and memory storage of IoT devices, the secure treatment of IoT data has become a very sophisticated mission. Consequently, threats over IoT networks become of great quality, several, and complicated more and more over the past few years, which makes IoT user's data vulnerable to unauthorized access. Recent investigations show that this exponential increase in threats results from the weak security structures deployed in IoT ecosystems [17]–[20]. Enormous parameters make the security of IoT a heavy achievement, including the poor security of IoT devices, given that the manufacturers are less interested in conducting requisite analysis to involve security from the outset than in getting their products on the market immediately. Additionally, Wi-Fi and other wireless communication networks used in IoT are known to be vulnerable to massive interferences. In addition, the absence of a singular perspective of IoT and universal norms makes it more challenging to design a security scheme for an IoT network with heterogeneous equipment. Moreover, the introduction of a universal security mechanism can be impacted by the dynamic topology of networks, which increases the attack area.

Authentication is the most critical phase towards IoT environment security and privacy as a method of entity identity verification. It answers the question: "Are you that entity?". Overall, to guarantee that the source of data is legitimate, each node could authenticate all other nodes in the IoT network [21]. Authentication schemes are several, but all are based on or more of the knowledge, possession, and attribute factors.

Generally, the level of safety we provide increases with the number of factors we use. Multi-factor authentication schemes need a high power of computation, interesting memory storage, and much energy. Nonetheless, because of the limited nature of IoT devices, these conditions cannot be offered. During the last few years, enormous lightweight authentication schemes have been provided to overcome the limitations of IoT devices. The performance of provided schemes and their cost change underpinned the cryptographic mechanisms used, such as Advanced Encryption Standard (AES), Rivest–Shamir–Adleman (RSA), Elliptic Curve Cryptography (ECC), and so on [22].

Over the past few years, various authentication and key accord schemes have been proposed to assure security and confidentiality in IoT networks. To guide today's researchers by affording security obstacles, open challenges, and future directions, multiple comparison studies of IoT authentication are provided in the literature. Kumar et al. proposed an exhaustive exploration of Internet-of-Things authentication mechanisms [23]. They examined the potencies and the shortcomings of the current approaches. Furthermore, discussing the principles of authentication and its related threats, they interlinked the progress of the solution strategies and presented a taxonomy of IoT authentication. Finally, they discussed new research directions in this area. Trnka et al. [24] afford a guideline for following research, offering a survey of research published between 2017 and 2020. They classify implicated norms and techniques required in present methods to discover the taxonomy of IoT security solutions. Saqib and Moon Offered a systematic security assessment and examined the authentication approaches in IoT networks [25]. The purpose of their survey is to uncover and encapsulate security issues in IoT related to authentication tools and discover the current scheme's holes in various types of authentications. Firstly, they defined security and privacy obstacles and clarified the security alert throughout different IoT architecture levels. Secondly, they presented the countermeasures reachable for

dealing with security issues. In addition, they utilized distinct performance measures, including computational cost, communications costs, and energy use, for benchmarking a few of the current IoT authentication schemes.

Finally, they presented the simulators used to assess the power of authentication protocols. Bahache et al. [26] offered a detailed investigation of current authentication schemes in terms of security and performance. They also provided a new classification of authentication approaches in WMSNs as a function of its architecture. Ahmed et Mohammed [27] also synthesized identity control, lightweight authentication, and authorization research in IoT networks. As a result, they emphasized topical IoT security tendencies and their achievement.

To investigate the enhancement of IoT authentication can be made by the decentralized architecture of the Blockchain technology, provided a survey of access assessment of IoT devices utilizing access control approaches and decentralized authentication [28]. They studied current examinations of Blockchain applications and presented attempts to enhance security and confidentiality in Blockchain applications. Therefore, they outlined different security problems related to decentralized IoT authentication. Mohsin et al. [29] furnished effective information that can strengthen the comprehension of how authentication methods can be merged with Blockchain technology. They pull up a categorization of Blockchain technology for authentication in the IoT environments. At last, they analyzed problems surrounding Blockchain technology, proposed resolutions, and covered the following research orientations.

Newly, the IoT-driven healthcare services have been boosted using 5G networks. An in-depth review of methods to safeguard IoT-5G appliances employed in medical applications was conducted by Sodhro et al. [30]. Their analysis included reviewing, characterizing, clustering, and categorizing IoT-5G appliance authentication, radio-frequency fingerprinting, and mutual authentication. In the end, they showed some artificial intelligence methods that can be utilized to develop authentication and give recommendations for the following research. A brief investigation was conducted by Jiang et al. [31] on how to authenticate Machine Learning Physical Layers in the 5G-based Internet of Things. The paper also outlined research orientations for machine learning approaches that can be used to secure 5G-based IoT. Wazid et al. [32] conducted a survey that revealed the regulations and attacks that are likely to occur in IoT networks that utilize 5G. They conducted a comparative analysis of today's security protocols to explore future search issues and directions in the security of 5G-enabled IoT environments.

As bio-features have become a crucial actor for IoT device authentication, Ferrag et al. have studied the use of bio-features for authentication and authorization in IoT mobile devices [33]. They presented the several data mining and machine-learning mechanisms required in the authentication and authorization of IoT devices. Ultimately, by analyzing the existing biometric authentication systems, they identified several types of problems that need to be addressed for future investigation. Yang et al. [34] provided a summary to help scientists comprehend potential challenges in biometrics-based IoT security and the direction of research going forward. They evaluated the actual biometrics-based IoT security research, especially authentication and encryption. Likewise, they categorized the studied approaches in terms of various biometric characteristics.

This survey is a road map for new researchers to improve IoT opportunities. It provides an exhaustive study of today's authentication research between 2018 and 2024; it covers more than thirty authentication schemes. The contributions of our paper are the following:

- ✓ We provide a simple categorization of authentication approaches in IoT environments.
- ✓ We survey and examine recent IoT authentication protocols based on the cryptographic mechanisms used, the provided security features, the resistance against most popular attacks, and the computational and communication cost to enable the understanding of the current literature.
- ✓ We highlight open challenges by examining holes in today's protocols and afford future research orientations.

The rest of our review is organized that way. The research method is introduced in section two. A simple taxonomy of IoT authentication schemes is provided in section three. The fourth section presents the comparison study results. Finally, the fifth section concludes the paper and discusses future research orientations.

2. RESEARCH METHOD

Our reviewing procedure included two parts. At first, we assembled articles using some preselected keywords (cryptography, IoT, attacks, authentication, security). To accomplish this stage, we browsed various numerical sources, including:

- Google Scholar (https://scholar.google.com/)
- ACM Digital Library (http://dl.acm.org)
- IEEE eXplore (http://ieeexplore.ieee.org)
- ScienceDirect (https://www.sciencedirect.com)

- Springer (https://link.springer.com/)
- MDPI (https://www.mdpi.com/)

Then, the articles were classified based on the following criteria:
Inclusion criteria:

- Papers focus on IoT authentication.
- Papers provide a novel protocol for IoT authentication.
- Papers offer a security examination of the provided article.
- Papers contain a section that evaluates the proposed scheme's performance.
- Papers investigate obstacles and disadvantages of authentication in IoT networks.

Exclusion criteria

- Papers published before 2018.
- Papers redundant.
- Papers that do not address IoT authentication schemes.

Finally, a simple analysis of the title and the abstract of each article eliminated those with poor quality. As a result, we admit thirty-one papers as a subject of the comparison study.

3. TAXONOMY OF IOT AUTHENTICATION PROTOCOLS

In this fraction, we show a classification of IoT authentication protocols according to several parameters [35], these parameters are pictured in Figure 1 and summarized as follows:

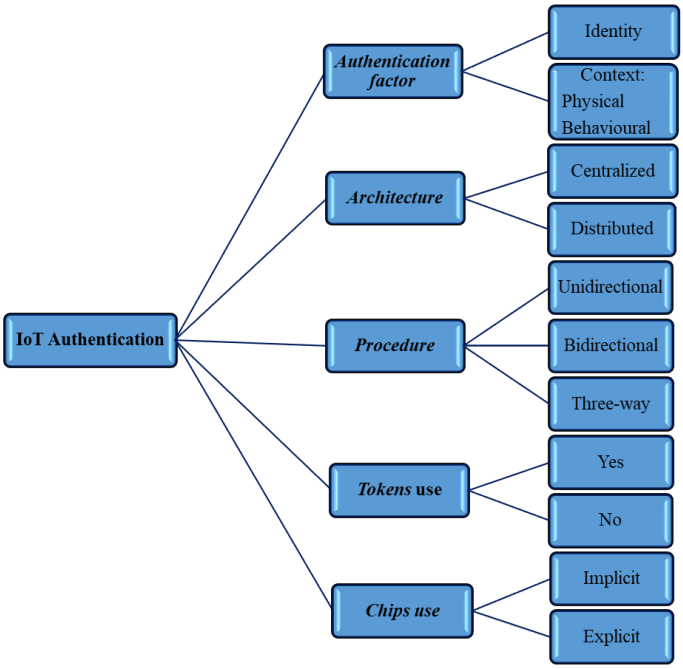


Figure 1. Categorization of IoT authentication schemes

Authentication factor. It may be either identity [36]–[40], which is information provided by one party to another to authenticate, or a feature [41]–[48], which can be physical like fingerprints or hand geometry, or behavioral like typing dynamics or voice prints.

Architecture. It can be distributed when a direct authentication approach circulated between the connecting nodes is used[49]–[56], or centralized [57], [58]when a confident authority that enables the identification data distribution and management is utilized for authentication.

Procedure. Which may be unidirectional when uniquely one node attests the other while the other is not attested. Bidirectional (mutual authentication[59]–[64]) whenever the two nodes certify to each other. Three-way authentication in case a confident authority authenticates both nodes and supports them in authenticating each other.

Tokens use. In token-based authentication protocols [65]–[70], the user certifies from a proof of identity (data) constituted by a server.

Chips use. That may be implicit, when it utilizes material physical characteristics to enhance authentication, such as physical unclonable functions [71]–[76], or explicit, where it utilizes chips that save and treat keys utilized for authentication.

4. COMPARATIVE STUDY

4.1. Comparison criteria

Resistance against attacks: It is a significant property in an authentication approach. The authentication scheme could hold out threats as much as possible to ensure the exchanged data security during the session. Accordingly, the better the resistance, the stronger the authentication.

Complexity: In IoT networks, energy may be the extremely critical limiting element related to the potentialities of a sensor. To prolong as much as possible the life of an IoT device and that of the IoT network, it is essential to manage its energy reservoir reasonably. Consequently, to construct a powerful authentication approach, it is mandatory to decline the number of operations accomplished.

Session Key Management: A session key is used to specify encryption between two entities to exchange data securely over a public network. The management of session keys is a critical challenge of IoT, which consists of various phases: generation, distribution, storage, updating, and destruction of keys. Generally, a key agreement scheme must be used to arrange a session key impacted by all communicating entities.

Factor number: Based on the number of factors considered to certify the user, we can identify three kinds of authentication protocols. A single-factor authentication (SFA) is when the customer authenticates based only on the password. A dual-factor authentication (2FA) is when the consumer utilizes a smart card and a keyword to certify. A multi-factor authentication (MFA) demands more factors, including location information, biometric features, etc.

Mutual authentication: It is a highly prominent notion in IoT authentication approaches. It enables an IoT device to certify the authenticity of the access demand submitted by an entity (human being or another system) to permit its access to network resources. On the other hand, the customer should also be sure of the authenticity of the appliance.

Cryptographic algorithm used: During the authentication phase, various cryptographic approaches can be exploited. Based on these approaches, we may categorize authentication protocols into four categories. The first category is based on symmetric approaches, given their low cost. The second class is built solely on asymmetric approaches that can be separated into two kinds: those using usual mechanisms (RSA [77]–[80]…) and those using elliptic curve cryptography (ECC[81]–[89]). The third class is hash functions-based protocols. The last class consists of hybrid schemes mixing two or all existing mechanisms.

4.2. Comparison of the studied protocols

This section offers the result of our comparison study between some of the recent authentication schemes. The protocols studied are proposed between 2018 and 2024. A major part of these schemes consists of four phases: the initialization stage, the registration stage, the login and authentication stage, and the password change stage. To fully understand and examine the schemes reviewed, we utilized various comparison criteria: cryptography algorithms, security, services offered, resistance against threats, computational complexity (execution time), and communication cost.

Cryptographic techniques.

Table 1. Cryptography techniques

Protocol	Cryptography techniques	Factors number	simulator	others
[90]	Random numbers Hash function	2	-	-
[91]	Random numbers Hash function ECC	2	ProVerif	-
[92]	Random numbers Hash function ECC Encryption/Decryption	2	Scyther	-
[93]	Random numbers Hash function Encryption/Decryption Chebyshev's chaotic map	2	Random Oracle	-

Protocol	Cryptography techniques	Factors number	simulator	others
[94]	Random numbers Hash function Encryption/Decryption	2	ProVerif	-
[95]	Random numbers Hash function	2	AVISPA	-
[96]	Random numbers Hash function ECC	2	AVISPA	-
[97]	Random numbers Hash function Encryption/Decryption	2	-	-
[98]	Random numbers Hash function ECC	3	ProVerif	Fuzzy extractor
[99]	Random numbers Hash function Encryption/Decryption	3	-	Fuzzy extractor
[100]	Random numbers Hash function ECC Encryption/Decryption	3	AVISPA	Fuzzy extractor
[101]	Random numbers Hash function ECC	2	ProVerif	-
[102]	Random numbers Hash function	3	-	Fuzzy extractor
[103]	Random numbers Hash function Encryption/Decryption	3	AVISPA	Fuzzy extractor
[104]	Random numbers Hash function Chaotic map	2	Scyther	-
[105]	Random numbers Hash function	3	Scyther	Fuzzy extractor/PUF
[106]	Random numbers Hash function ECC	3	Scyther	Fuzzy extractor
[107]	Random numbers Hash function Encryption/Decryption	2	Scyther	-
[108]	Random numbers Hash function	3	-	Fuzzy extractor
[109]	Random numbers Hash function	2	-	-
[110]	Random numbers Hash function Encryption/Decryption	2	Scyther	Block chain
[111]	Random numbers Hash function Encryption/Decryption	2	Scyther	Block chain
[112]	Random numbers Hash function Encryption/Decryption	3	AVISPA	Fuzzy extractor/PUF
[113]	Random numbers Hash function	3	AVISPA	Fuzzy extractor
[114]	Random numbers Hash function ECC Encryption/Decryption	2	-	-
[115]	Random numbers Hash function ECC	3	Scyther	-
[116]	Random numbers Hash function ECC Encryption/Decryption	2	-	Hardware Chip

Protocol	Cryptography techniques	Factors number	simulator	others
[117]	Random numbers Hash function	3	-	Fuzzy extractor/ Symmetric bivariate polynomial
[118]	Random numbers Hash function ECC Encryption/Decryption	2	-	-
[119]	Random numbers Hash function ECC Encryption/Decryption	3		Fuzzy extractor
[120]	Random numbers Hash function	2	Scyther	-
[121]	Random numbers Hash function	2	AVISPA	-
[122]	Random numbers Hash function ECC	4	ProVerif	PUF
[123]	Random numbers Hash function	2	AVISPA	PUF
[124]	Random numbers Hash function Chaotic map Encryption/Decryption	3	Scyther	Fuzzy extractor
[125]	Random numbers Hash function	2	ProVerif	-

Table 1 shows the cryptographic techniques used in each protocol, Chen et al. [90], Oh et al. [95], Garg et al. [109], Azrour et al. [120], G. Sharma et al. [121], Z. Zhang et al. [123], and S. U. Jan et al. [125] presented seven different protocols based on two authentication factors using random numbers and hash functions. Finally, Oh et al. [95], G. Sharma et al. [121], and Z. Zhang et al. [123] used the AVISPA simulator to perform a formal analysis of their protocol. Nonetheless, Azrour et al. [120] and S. U. Jan et al. [125] used the Scyther simulator and the ProVerif tool, respectively, for formal security analysis.

Kaurl et al. [94], Dammak et al. [97], Yadav et al. [107], and Rostampour et al. [111] provided four dual-factor authentication protocols built on encryption and decryption algorithms, random numbers, and hash functions. The formal analysis of the schemes provided by Kaurl et al. [94] was carried out using the ProVerif simulator, as these of Yadav et al's protocol [107] and Rostampour et al's protocol [111] were carried out using Scyther.

Krishnasrija et al. [104] presented a two-factor authentication scheme, and M. Tanveer et al. [124] presented a three-factor authentication scheme using random numbers, hash functions, and chaotic maps. Kumar et al. [93] used also encryption and decryption algorithms. The formal analysis of the presented schemes was performed by exploiting Scyther and Random Oracle, respectively.

Hu et al. [91], Panda et al. [96], and Nyangaresi [101] used random numbers, hash functions, and elliptic curve cryptography (ECC) to build two-factor authentication protocols. When Azrour et al [92], Pirayesh et al. [114], and [116] Khan et al. [118] combined those mechanisms with encryption and decryption algorithms to build their schemes. Subsequently, Hu et al. [91] and Nyangaresi [101] used ProVerif, while Azrour et al. [92] and Panda et al. [96] used Scyther and AVISPA simulators respectively, to conduct a formal analysis.

Dwivedi et al. [110] suggested a two-factor authentication scheme using encryption and decryption algorithms, random numbers, hash functions, and Blockchain technology. The proposed scheme was formally analyzed using the Scyther simulator.

Cui et al. [102], Lee et al. [105], Bagga et al. [108], Khalid et al. [113], and Guo et al. [117] proposed five three-factor authentication protocols based only on random numbers and hash functions. In the end, Lee et al. [105] and Khalid et al. [113] used the Scyther and AVISPA simulators, respectively, to perform a formal analysis of their protocol.

Xie et al. [98], Kou et al. [99], Butt et al. [100], Yu et Park [103], [106], [112], Hajian et al. [115], and Yadav et al. [119] presented three-factor protocols that use the fuzzy extractor to extract numerical variables from user biometric information, random numbers, and hash functions. The difference between these protocols is that [99], [103], and [112] are based on encryption and decryption algorithms, [98], [106], [115], and [122] are based on ECC, however [100] and [119] combines both techniques. Afterward, Xie et al. [98],

P. Guo et al. [122] used ProVerif, Butt et al. [100], Yu et Park [103] and [112] used AVISPA, and [106] and Hajian et al [115] used Scyther to make a formal analysis of their schemes.

Security services.

Generally, to trust an authentication scheme, it should secure enormous security features, including mutual authentication, which is a security procedure that enables exchanging entities to check each other identities and trust the communicated data in an IoT network. Anonymity that protects the consumer's identity to overcome impersonation attacks. Intractability that secures users from the disclosure of confidential and sensitive data. Key agreement to generate a key, which may be used for encrypting the communicated data. Perfect forward secrecy that stops illegitimate entities from intercepting, deducting, or obtaining the key. Moreover, the key secret that maintains sensitive data secret. As it is clear from Table 2, the schemes [91], [93], [94], [101]–[105], [115], [118], [120], and [125] are the most effective protocols ensuring all security features, then the protocols [95], [97], [98], [106], [107], [111], [113], [116], [117], [119], [122], and [123] which do not ensure the key secret, and [108], [109] that do not ensure the perfect forward secrecy. However, scheme [112] secures mutual authentication, anonymity, intractability, and key agreement, and scheme [121] secures mutual authentication, anonymity, key agreement, and perfect forward secrecy. Protocols [99], [100], [114], and [124] allow mutual authentication, anonymity, and key agreement. Schemes [90] and [92] enable mutual authentication, key agreement, and key secret. Scheme [96] offers mutual authentication, key agreement, and perfect forward secrecy. Scheme [110] provides only anonymity and intractability.

Table 2. security features and resistance against attacks

Protocol	F_1	F_2	F_3	F_4	F_5	F_6	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8	A_9	A_{10}	A_{11}	A_{12}
[90]	✓	×	×	✓	×	✓	×	✓	-	-	✓	✓	-	×	×	✓	-	-
[91]	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	-	-	-	✓	✓	-	-	-
[92]	✓	-	-	✓	-	✓	-	✓	-	✓	✓	✓	✓	✓	-	-	-	-
[93]	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓	-	✓	✓	✓	-	-
[94]	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓	-	✓	✓	✓	-	-
[95]	✓	✓	✓	✓	✓	-	✓	✓	-	-	✓	-	-	✓	✓	-	✓	-
[96]	✓	-	-	✓	✓	-	✓	✓	-	-	✓	-	-	✓	-	-	✓	-
[97]	✓	✓	✓	✓	✓	-	✓	✓	✓	-	✓	✓	-	✓	-	-	-	✓
[98]	✓	✓	✓	✓	✓	-	✓	✓	✓	✓	✓	✓	-	✓	✓	-	✓	-
[99]	✓	✓	-	✓	-	-	✓	✓	-	✓	✓	✓	-	✓	✓	-	✓	-
[100]	✓	✓	-	✓	-	-	✓	✓	-	-	✓	-	-	✓	-	-	-	-
[101]	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	-	-	-	-	-	-	✓	-
[102]	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	-	-	✓	✓	-	✓	-
[103]	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓	-	✓	✓	-	✓	-
[104]	✓	✓	✓	✓	✓	✓	-	✓	-	-	✓	-	-	✓	✓	-	✓	-
[105]	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	-	✓	-	✓	✓	-	✓	-
[106]	✓	✓	✓	✓	✓	-	✓	✓	✓	-	✓	✓	-	✓	✓	-	✓	-
[107]	✓	✓	✓	✓	✓	-	✓	✓	-	-	✓	-	-	-	-	-	-	-
[108]	✓	✓	✓	✓	-	✓	✓	✓	-	-	✓	-	-	-	✓	-	✓	-
[109]	✓	✓	✓	✓	-	✓	✓	✓	✓	-	✓	-	-	-	✓	-	✓	-
[110]	×	✓	✓	-	-	-	✓	-	-	-	-	-	-	-	-	-	✓	-
[111]	✓	✓	✓	✓	✓	-	✓	✓	-	-	-	-	-	-	-	-	-	-
[112]	✓	✓	✓	✓	-	-	✓	✓	-	-	✓	-	-	✓	✓	-	-	-
[113]	✓	✓	✓	✓	✓	-	✓	-	-	-	-	-	-	-	✓	-	-	-
[114]	✓	✓	-	✓	-	-	✓	✓	-	×	-	✓	-	-	-	-	✓	-
[115]	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	-	-	-	-	-	✓	-
[116]	✓	✓	✓	✓	✓	-	✓	✓	-	-	✓	-	-	-	-	-	✓	-
[117]	✓	✓	✓	✓	✓	-	✓	✓	✓	-	✓	-	-	✓	✓	✓	✓	-
[118]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	-	✓	-	-	✓	-
[119]	✓	✓	✓	✓	✓	-	-	✓	-	-	-	-	-	-	✓	-	-	-

Protocol	F_1	F_2	F_3	F_4	F_5	F_6	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8	A_9	A_{10}	A_{11}	A_{12}
[120]	✓	✓	✓	✓	✓	✓	-	✓	-	✓	✓	✓	-	✓	✓	-	-	-
[121]	✓	✓	-	✓	-	✓	-	✓	-	-	✓	-	-	✓	✓	-	-	-
[122]	✓	✓	✓	✓	-	✓	-	✓	✓	-	✓	-	-	-	✓	✓	✓	-
[123]	✓	✓	✓	✓	-	✓	✓	✓	✓	-	✓	-	-	-	✓	-	✓	-
[124]	✓	✓	-	✓	-	-	✓	-	-	✓	✓	-	-	✓	-	-	✓	-
[125]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	-	-	-	-

F1: mutual authentication, F2: Anonymity, F3: unlinkability, F4: key agreement, F5: key secrecy, F6: perfect forward secrecy, A1: Impersonation attack, A2: reply attack, A3: node capture, A4: DoS attack, A5: Insider attack, A6: Stolen verifier, A7: Denning-ssaco attack, A8: password guessing, A9: smart card loss, A10: GWN bypassing, A11: men in the middle, A12: token modification.

Resistance against attacks.

The comparison based on security services provided by each protocol may give an idea about the studied protocol; instead, it is not sufficient to evaluate it. For this reason, resistance against known attacks is examined in this section. Analyzing Table 2, security features and resistance against attacks, we can conclude the following results:

The scheme [98] is the most robust of the 31 studied; it is resistant to impersonation attacks, reply attacks, node capture attacks, password guessing, DoS attacks, stolen verifier attacks, insider attacks, stolen verifier attacks, man-in-the-middle, and smart card loss attacks. Nevertheless, [99] and [103] are resistant to all recent attacks except the node capture attacks. In addition, [93] and [94] resist GWN bypassing attacks and the same attacks as [98] except man-in-the-middle and node capture attacks. The protocol [106] resists in opposition to GWN bypassing attacks and the same attacks as [98] except for DoS attacks. The scheme [117] holds out GWN bypassing attacks and the same attacks as [98] apart from the stolen verifier, DoS.

The protocol [118] is resistant in the face of impersonation raids, reply attacks, node capture attacks, password guessing, stolen verifier attacks, DoS attacks, and man-in-the-middle attacks. The protocol [97] is resistant to insider attacks, token modification, and the same attacks as [118], aside from man-in-the-middle and Dos raids. The approach [102] resists impersonation attacks, reply attacks, node capture attacks, insider attacks, man-in-the-middle, password guessing, and smart card loss attacks. On the other side, [105] is resistant to all recent attacks except insider attacks together with Stolen verifier attacks.

The scheme [125] is strong against Impersonation attacks, replay attacks, node capture attacks, DoS attacks, Insider attacks, Stolen verifier attacks, and password guessing. The scheme [123] is strong against smart card loss, men-in-the-middle, and all the raids resisted by the scheme [125], excluding DoS attacks, Stolen verifier attacks, and password guessing. However, the scheme [122] resists replay attacks, node capture, Insider attacks, smart card loss, GWN bypassing, and men-in-the-middle attacks.

The protocol [92] is resilient in the face of reply attacks, Denning-ssaco, DoS attacks, password guessing, insider attacks, and stolen verifier attacks. However, [120] is resilient regarding smart card loss and the same attacks as [92] other than Denning-ssaco attacks. The mechanism [95] resists impersonation attacks, reply attacks, insider attacks, man-in-the-middle, password guessing, and smart card loss attacks. Even though the mechanism [109] is resistant to node capture attacks and the same attacks as [95], aside from password guessing.

The scheme [112] resists in the face of impersonation attacks, reply attacks, insider attacks, smart card loss, and password guessing. Nevertheless, the scheme [104] resists in the face of all later attacks, excluding impersonation attacks coupled with man-in-the-middle attacks. In addition, [91] also resists node capture attacks and all attacks resisted by the scheme [112], aside from insider attacks. The approach [108] seems strong against impersonation attacks, reply attacks, smart card loss, insider attacks, and man-in-the-middle attacks. However, the approach [115] can resist node capture attacks and attacks resisted by [108], apart from smart card loss. The scheme [96] also resists password guessing, and all attacks resisted by [108] excluding smart card loss.

The protocol [124] is resilient against Impersonation attacks, DoS attacks, Insider attacks, password guessing, and man-in-the-middle attacks. However, the protocol [121] is resilient against replay attacks, Insider attacks, password guessing, and smart card loss.

The mechanism [116] withstands man-in-the-middle, replay attacks, impersonation attacks, and insider attacks. At the same time, the mechanism [114] fights back stolen verifier attacks, and all attacks resisted by [116] but insider attacks. On the other hand, the mechanism, [101] counteracts DoS attacks as well as raids resisting by the mechanism [116], aside from insider attacks. The scheme [100] is resistant to impersonation attacks, insider attacks, replay attacks, and password guessing. Nonetheless, the protocol [90] is resilient to

insider attacks, replay attacks, GWN bypassing, and stolen verifier attacks. Additionally, the scheme [107] can hold out the same attacks as the scheme [116] apart from man-in-the-middle.

The schemes [110], [111], and [113] are resistant to impersonation attacks coupled with man-in-the-middle attacks, replay attacks, and smart card loss, respectively. Although, [119] fight back only smart card loss and replay attacks.

Computational cost.

In this section, we examine the computational needs of the studied schemes. The notation Th is defined as the temporal requisite of the hash function. Te is the temporal requisite of the elliptic curve point's multiplication. Tc is the temporal need of Chebyshev's chaotic map use. Ts is the temporal need of symmetric encryption/decryption. Tf is the temporal exigency of the fuzzy extractor. Tasym is the temporal need of asymmetric encryption/decryption. Tpuf is the temporal requirement of physical unclonable function. Tsig is the computational cost of the HECDSA signature algorithm. The cost of calculating the operation or exclusive is generally overlooked because it requires minimal calculations. According to [93] Th=0.0005 s, Tc=0.02102 s, Te=0.063075 s and Ts=0.0087 and according to [97] Tasym=Te=Tf=0.063075 s. Depending on [105] Th=1,91%* Tpuf, as a result, we consider Tpuf=0,02608s. Based on [93] and [114] Tsig= 0,47 s.

Table 3. Computational requirement of login and authentication phase

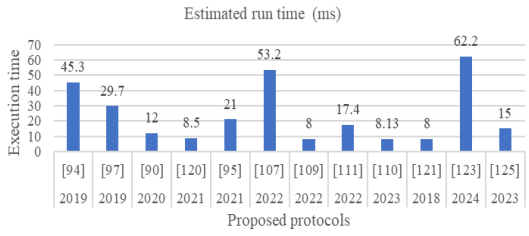
protocol	User	Getway	Sensor	total	Execution time (ms)	Communication cost(bits)
[90]	7Th	11Th	6Th	24Th	12	-
[91]	7Th+ 3Te	10Th+ Te	6Th+ 2Te	23Th+6Te	390	-
[92]	5Th	6Th+ 4Te	2Th+2Te	13Th+6Te	385	-
[93]	5Th+2Tc+2Ts	7Th+2Ts	3Th+2Tc	15Th + 4Tc + 4Ts	126,4	1408
[94]	8Th+ 2Ts	7Th+ 1Ts	6Th+ 1Ts	21Th+ 4Ts	45,3	2136
[95]	-	-	-	42Th	21	2080
[96]	-	5Th+4Te	4Th+4Te	9Th+8Te	67,57	1760
[97]	16Th	19Th+Ts	7Th	42Th+Ts	29,7	2272
[98]	7Th+3Te+1Tf	7Th+Te	4Th+2Te	18Th+6Te+Tf	390	-
[99]	7Th+Tf+2Ts	12Th+2Ts	6Th	25Th+Tf+4Ts	49,8	-
[100]	3Th+2Te+Tf+Ts	Th+2Te	Th+2Ts	5Th+4Te+Tf+3Ts	283,4	-
[101]	6Th	-	8Th+Te	13Th+2Te	132,6	2016
[102]	13Th+Tf	13Th	9Th	35Th+Tf	80,6	2496
[103]	-	-	-	15Th+Tf+2Ts	88	928
[104]	6Th+2Tc	8Th+Tc	6Th	20Th+3Tc	73	3510
[105]	11Th+Tf	16Th	7Th+Tf+Tpuf	34Th+2Tf+Tpuf	169,23	1837
[106]	9Th+ 3Te	9Th+ Te	7Th+ 2Te	25Th+ 6Te	390,9	3712
[107]	3Taes + T	3Taes + Th	-	6Taes + 2Th	53,2	896
[108]	16Th+Tf	13Th	-	29Th+Tf	77,6	4128
[109]	-	-	-	16Th	8	1792
[110]	-	-	-	6Th+9Ts	8,13	-
[111]	-	Ts	Ts	2Ts	17,4	278
[112]	8Th	11Th +1Ts	5Th+1Ts	24Th+2Ts	29,4	2000
[113]	4Th + 2Tf	11Th	3Th	18Th + 2Tf	135,1	2688
[114]	-	-	-	15Th + 2Tf+4Ts+ 2Tsig+6Te	1486	-
[115]	-	-	-	8 Te + 14 Th	133,1	1344
[116]	Ts + 2Tas + 3Th	Ts + 5Th	2Tas + 3Th	2Ts + 4Tasym +11Th	275,2	-
[117]	Tp + 8Th	Tp + 8Th	-	2Tp + 16Th+Tf	87,1	2112
[118]	5Th+3Te	5Th+2Te+Ts	3Th+3Te+Ts	13Th+8Te+2Ts	528,5	2880
[119]	-	-	-	Ts + 15Th+6Te	394,6	3680
[120]	6Th	8Th	3Th	17Th	8,5	-

protocol	User	Getway	Sensor	total	Execution time (ms)	Communication cost(bits)
[121]	-	-	-	16Th	8	-
[122]	12Th+Tpuf+3Tmul	12Th+Tmul	7Th+Tpuf+2Tmul	30Th+2Tpuf+5Tmul	382,5	2248
[123]	6Th+2Tpuf	8Th	6Th	20Th+2Tpuf	62,2	1760
[124]	4Th+4Tc+3Tasym	Th+Tc+Tasym	2Th+Tc+2Tasym	7Th+6Tc+6Tasym	508,1	896
[125]	11Th	15Th	4Th	30Th	15	3680

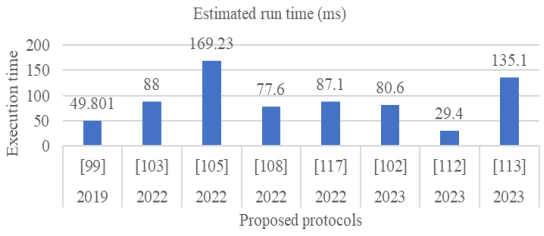
Table 3 shows the computational requirement pf the studied authentication schemes. The two-factor lightweight authentication protocols [90], [94], [95], [97], [107], [109], [110], [111], [120], [121], [123], and [125] need 24Th, 21Th+ 4Ts, 42Th, 42Th+Ts, 6Taes + 2Th, 16Th, 6Th+9Ts, 2Ts, 17Th, 16Th, 20Th+2Tpuf, and 30Th respectively. The three-factor lightweight authentication protocols [99], [102], [103], [105], [108], [112], [113], and [117] require 25Th+Tf+4Ts, 35Th+Tf, 15Th+Tf+2Ts, 34Th+2Tf+Tpuf, 29Th+Tf, 24Th+2Ts, 18Th + 2Tf, and 2Tp + 16Th+Tf respectively. Nevertheless, The two-factor hybrid authentication schemes [91], [92], [93], [96], [101], [104], [114], [116], and [118] demand 23Th+6Te, 13Th+6Te, 15Th + 4Tc + 4Ts, 9Th+8Te, 13Th+2Te, 20Th+3Tc, 15Th + 2Tf+4Ts+ 2Tsig+6Te, 2Ts + 4Tasym +11Th, and 13Th+8Te+2Ts severally. While, The three-factor hybrid authentication schemes [98], [100], [106], [115], [119], [122], and [124] demand 18Th+6Te+Tf, 5Th+4Te+Tf+3Ts, 25Th+ 6Te, 8 Te + 14 Th, Ts + 15Th+6Te, 30Th+2Tpuf+5Tmul, and 7Th+6Tc+6Tasym severally. Figure 2 illustrates the estimated run time for each scheme.

Communication cost

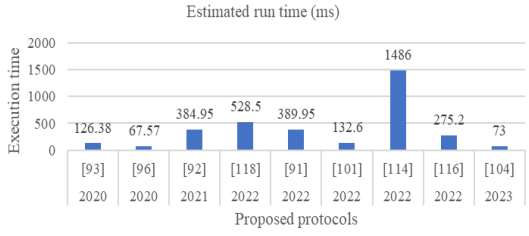
To enhance communication efficiency, the communication costs of an authentication scheme must be reduced. Based on the graphs in Fig. 3, the schemes in [104], [106], [108], [119], and [125] incur the highest communication overheads. This is followed by the protocols in [93]–[102], [105], [109], [112], [113], [115], [117], and [118]. Notwithstanding, the schemes [103] [107], [111], and [124] require the lowest communication costs, they are weak against the majority of known attacks, and as has been mentioned before, they cannot ensure perfect forward secrecy.



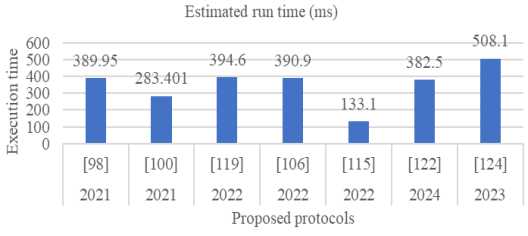
Two-factor Lightweight authentication schemes



Three-factor Lightweight authentication schemes



Two-factor Hybrid authentication schemes



Three-factor Hybrid authentication schemes

Figure 2. login and identity verification estimated run time.

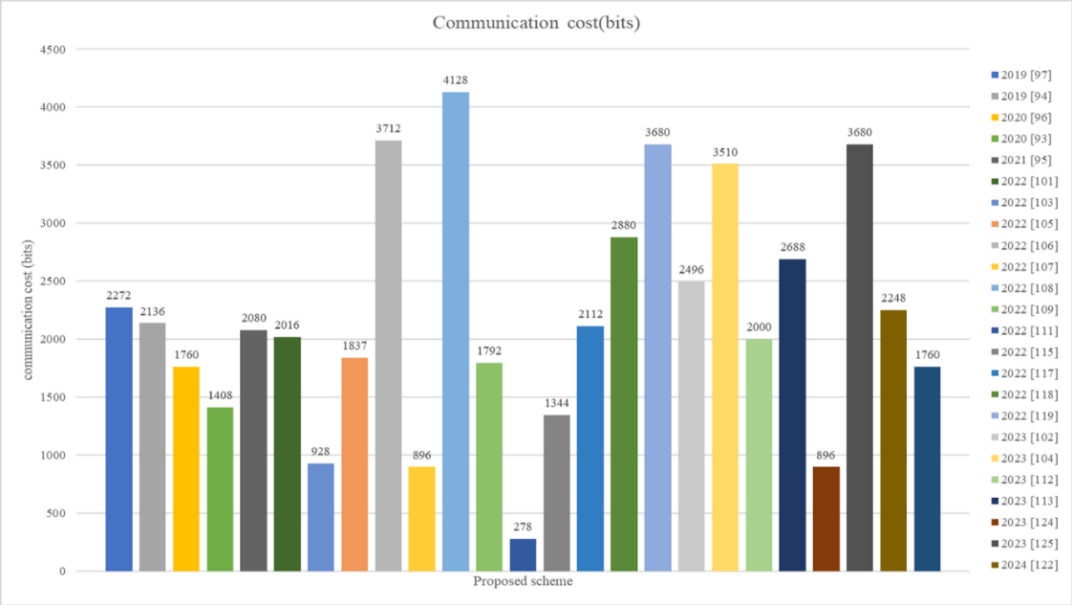


Figure 3. login and identity verification estimated storage.

4.3. Classification of the studied protocols

In this section, we classify the protocols we have studied into two classes. Based on the cryptographic algorithms, we identify lightweight schemes that use random numbers, hash function, and encryption mechanisms, and hybrid schemes that require the previous mechanisms combined with elliptic curve cryptography, chaotic maps, or both. According to the authentication factors, we detect dual-factor schemes which use possession and knowledge, and three-factor schemes which need possession, knowledge, and attribute. The results of the classification in terms of cryptographic algorithms and authentication factors are presented in Table 4. It illustrates four classes two-factor lightweight authentication protocols, three-factor lightweight authentication protocols, two-factor hybrid authentication, and three-factor hybrid authentication schemes. By analyzing the result of the classification correlated with the login and identity verification estimated run time presented in Figure 2. we observe that no matter the number of authentication factors used, the lightweight schemes seem faster than the hybrid schemes. Moreover, the two-factor hybrid authentication schemes require less computation power than three-factor hybrid authentication. Finally, we conclude that the addition of the third factor and additional cryptography techniques increases, partially, the computational cost and the energy consumption.

Table 4. Authentication schemes classification.

protocol	Lightweight authentication	Hybrid authentication
Two-factor authentication	C.-T. Chen et al. [90] D. Kaur et al. [94] J. Oh et al. [95] M. Dammak et al. [97] A. K. Yadav et al. [107] N. Garg et al. [109] S. K. Dwivedi et al. [110] S. Rostampour et al. [111] M. Azrour et al. [120] G. Sharma and S. Kalra[121] Z. Zhang et al. [123] S. U. Jan et al. [125]	B. Hu et al. [91] M. Azrour et al. [92] D. Kumar et al. [93] P. K. Panda et al. [96] V. O. Nyangaresi et al. [101] R. Krishnasrija et al. [104] J. Pirayesh et al. [114] C. Patel et al. [116] M. A. Khan et al. [118]
Three-factor authentication	L. Kou et al. [99] J. Cui et al. [102] S. Yu and K. Park [103] J. Lee et al. [105] P. Bagga et al. [108] R. Kumar et al. [112] B. Khalid et al. [113] Y. Guo et al. [117]	Q. Xie et al. [98] T. M. Butt et al. [100] X. Wang et al. [106] R. Hajian et al. [115] A. K. Yadav et al. [119] P. Guo et al. [122] M. Tanveer et al. [124]

5. CONCLUSION

This paper provides a detailed description of the Internet of Things authentication literature, considering authentication is the most critical agent in network security. First, we categorized the IoT authentication mechanisms. Then, we evaluated some current authentication schemes based on various criteria, including cryptographic mechanisms used and the deployment cost. The advantages and weaknesses of the studied schemes are presented by their resistance against attacks and their cost. The analysis of the examination results illustrates that the backbend of authentication may be the ECC, encryption mechanisms, chaotic map, or only random numbers and hash functions in the case of lightweight schemes. The robustness and the cost of each scheme are linked directly to the backbend and the number of authentication factors used. Generally, lightweight authentication and two-factor authentication require less computation power than hybrid schemes and three-factor schemes. However, the more we use factors and strong cryptographic methods, the more robust the scheme we provide. Despite the robustness of today's authentication schemes, various attacks require more interest, such as node capture, DoS attack, stolen verifier, denning-ssaco attack, and GWN bypassing. The limited character of centralized authentication approaches leads researchers to discover new research directions, such as Blockchain-based authentication, Post-quantum Cryptography, and Machine learning.

REFERENCES

[1] M. U. Farooq, M. Waseem, S. Mazhar, A. Khairi, and T. Kamal, "A review on internet of things (IoT)," *International journal of computer applications*, vol. 113, no. 1, pp. 1–7, 2015.

[2] P. Suresh, J. V. Daniel, V. Parthasarathy, and R. H. Aswathy, "A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment," in *2014 International conference on science engineering and management research (ICSEMR)*, IEEE, 2014, pp. 1–8.

[3] "Présentation générale de l'Internet des objets, secteur de la normalisation des télécommunications de l'UIT, 06-2012.

[4] "Architecting a connected future," ISO. Accessed: Feb. 03, 2023. [Online]. Available: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/news/2019/01/Ref2361.html

[5] N. Islam, M. M. Rashid, F. Pasandideh, B. Ray, S. Moore, and R. Kadel, "A review of applications and communication technologies for internet of things (Iot) and unmanned aerial vehicle (uav) based sustainable smart farming," *Sustainability*, vol. 13, no. 4, p. 1821, 2021.

[6] H. Landaluce, L. Arjona, A. Perallos, F. Falcone, I. Angulo, and F. Muralter, "A review of IoT sensing applications and challenges using RFID and wireless sensor networks," *Sensors*, vol. 20, no. 9, p. 2495, 2020.

[7] S. Dargaoui, M. Azrour, A. El Allaoui, A. Guezzaz, and S. Benkirane, "Authentication in Internet of Things: State of Art," in *Proceedings of the 6th International Conference on Networking, Intelligent Systems & Security*, 2023, pp. 1–6.

[8] S. Dargaoui *et al.*, "Security Issues in Internet of Medical Things," 2023, pp. 77–91. doi: 10.1201/9781003438779-5.

[9] S. Dargaoui *et al.*, "Applications of Blockchain in Healthcare:," 2023, pp. 1–12. doi: 10.1201/9781003430735-1.

[10] J. Mabrouki *et al.*, "Smart system for monitoring and controlling of agricultural production by the IoT," in *IoT and Smart Devices for Sustainable Environment*, Springer, 2022, pp. 103–115.

[11] J. Mabrouki, M. Azrour, and S. E. Hajjaji, "Use of internet of things for monitoring and evaluating water's quality: a comparative study," *International Journal of Cloud Computing*, vol. 10, no. 5–6, pp. 633–644, 2021.

[12] G. Fattah, J. Mabrouki, F. Ghrissi, M. Azrour, and Y. Abrouki, "Multi-Sensor System and Internet of Things (IoT) Technologies for Air Pollution Monitoring," in *Futuristic Research Trends and Applications of Internet of Things*, CRC Press, 2022, pp. 101–116.

[13] S. Dargaoui *et al.*, "An Overview of the Security Challenges in IoT Environment," in *Advanced Technology for Smart Environment and Energy*, J. Mabrouki, A. Mourade, A. Irshad, and S. A. Chaudhry, Eds., in Environmental Science and Engineering. , Cham: Springer International Publishing, 2023, pp. 151–160. doi: 10.1007/978-3-031-25662-2_13.

[14] F. Righetti, C. Vallati, and G. Anastasi, "IoT applications in smart cities: A perspective into social and ethical issues," in *2018 IEEE International Conference on Smart Computing (SMARTCOMP)*, IEEE, 2018, pp. 387–392.

[15] W. A. Jabbar *et al.*, "Design and fabrication of smart home with internet of things enabled automation system," *IEEE access*, vol. 7, pp. 144059–144074, 2019.

[16] V. K. Quy, N. V. Hau, D. V. Anh, and L. A. Ngoc, "Smart healthcare IoT applications based on fog computing: architecture, applications and challenges," *Complex & Intelligent Systems*, vol. 8, no. 5, pp. 3805–3815, 2022.

[17] M. Azrour, J. Mabrouki, A. Guezzaz, and A. Kanwal, "Internet of things security: challenges and key issues," *Security and Communication Networks*, vol. 2021, pp. 1–11, 2021.

[18] M. Mohy-eddine, A. Guezzaz, S. Benkirane, and M. Azrour, "An effective intrusion detection approach based on ensemble learning for IIoT edge computing," *Journal of Computer Virology and Hacking Techniques*, pp. 1–13, 2022.

[19] M. Douiba, S. Benkirane, A. Guezzaz, and M. Azrour, "An improved anomaly detection model for IoT security using decision tree and gradient boosting," *The Journal of Supercomputing*, pp. 1–20, 2022.

[20] C. Hazman, A. Guezzaz, S. Benkirane, and M. Azrour, "lIDS-SIoEL: intrusion detection framework for IoT-based smart environments security using ensemble learning," *Cluster Computing*, pp. 1–15, 2022.
[21] W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," *Computer networks*, vol. 148, pp. 283–294, 2019.
[22] 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*, IEEE, 2012, pp. 648–651.
[23] A. Kumar, R. Saha, M. Conti, G. Kumar, W. J. Buchanan, and T. H. Kim, "A comprehensive survey of authentication methods in Internet-of-Things and its conjunctions," *Journal of Network and Computer Applications*, p. 103414, 2022.
[24] M. Trnka, A. S. Abdelfattah, A. Shrestha, M. Coffey, and T. Cerny, "Systematic review of authentication and authorization advancements for the Internet of Things," *Sensors*, vol. 22, no. 4, p. 1361, 2022.
[25] M. Saqib and A. H. Moon, "A Systematic Security Assessment and Review of Internet of Things in the context of Authentication," *Computers & Security*, p. 103053, 2022.
[26] A. N. Bahache, N. Chikouche, and F. Mezrag, "Authentication Schemes for Healthcare Applications Using Wireless Medical Sensor Networks: A Survey," *SN Computer Science*, vol. 3, no. 5, p. 382, 2022.
[27] W. K. Ahmed and R. S. Mohammed, "Lightweight Authentication Methods in IoT: Survey," in *2022 International Conference on Computer Science and Software Engineering (CSASE)*, IEEE, 2022, pp. 241–246.
[28] I. Singh and B. Singh, "Access management of IoT devices using access control mechanism and decentralized authentication: A review," *Measurement: Sensors*, p. 100591, 2022.
[29] A. H. Mohsin *et al.*, "Blockchain authentication of network applications: Taxonomy, classification, capabilities, open challenges, motivations, recommendations and future directions," *Computer Standards & Interfaces*, vol. 64, pp. 41–60, 2019.
[30] A. H. Sodhro, A. I. Awad, J. van de Beek, and G. Nikolakopoulos, "Intelligent authentication of 5G healthcare devices: A survey," *Internet of Things*, p. 100610, 2022.
[31] J.-R. Jiang, "Short survey on physical layer authentication by machine-learning for 5G-based Internet of Things," in *2020 3rd IEEE International Conference on Knowledge Innovation and Invention (ICKII)*, IEEE, 2020, pp. 41–44.
[32] M. Wazid, A. K. Das, S. Shetty, P. Gope, and J. J. Rodrigues, "Security in 5G-enabled internet of things communication: issues, challenges, and future research roadmap," *IEEE Access*, vol. 9, pp. 4466–4489, 2020.
[33] M. A. Ferrag, L. Maglaras, and A. Derhab, "Authentication and authorization for mobile IoT devices using biofeatures: Recent advances and future trends," *Security and Communication Networks*, vol. 2019, 2019.
[34] W. Yang, S. Wang, N. M. Sahri, N. M. Karie, M. Ahmed, and C. Valli, "Biometrics for internet-of-things security: A review," *Sensors*, vol. 21, no. 18, p. 6163, 2021.
[35] 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.
[36] W. Akram, K. Mahmood, X. Li, M. Sadiq, Z. Lv, and S. A. Chaudhry, "An energy-efficient and secure identity based RFID authentication scheme for vehicular cloud computing," *Computer Networks*, vol. 217, p. 109335, 2022.
[37] O. Salman, S. Abdallah, I. H. Elhajj, A. Chehab, and A. Kayssi, "Identity-based authentication scheme for the Internet of Things," in *2016 IEEE Symposium on Computers and Communication (ISCC)*, IEEE, 2016, pp. 1109–1111.
[38] B. B. Gupta, A. Gaurav, K. T. Chui, and C.-H. Hsu, "Identity-based authentication technique for iot devices," in *2022 IEEE International Conference on Consumer Electronics (ICCE)*, IEEE, 2022, pp. 1–4.
[39] X. Jia *et al.*, "IRBA: an identity-based cross-domain authentication scheme for the internet of things," *Electronics*, vol. 9, no. 4, p. 634, 2020.
[40] A. G. Reddy, D. Suresh, K. Phaneendra, J. S. Shin, and V. Odelu, "Provably secure pseudo-identity based device authentication for smart cities environment," *Sustainable cities and society*, vol. 41, pp. 878–885, 2018.
[41] Y. Ashibani and Q. H. Mahmoud, "A behavior profiling model for user authentication in IoT networks based on app usage patterns," in *IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society*, IEEE, 2018, pp. 2841–2846.
[42] Z. Zhang, H. Ning, F. Farha, J. Ding, and K.-K. R. Choo, "Artificial intelligence in physiological characteristics recognition for internet of things authentication," *Digital Communications and Networks*, 2022.
[43] M. A. Ferrag, L. Maglaras, and A. Derhab, "Authentication and authorization for mobile IoT devices using biofeatures: Recent advances and future trends," *Security and Communication Networks*, vol. 2019, 2019.
[44] Y. Liang, S. Samtani, B. Guo, and Z. Yu, "Behavioral biometrics for continuous authentication in the internet-of-things era: An artificial intelligence perspective," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 9128–9143, 2020.
[45] V. Kumar and S. Ray, "Continuous Behavioral Authentication System for IoT Enabled Applications," in *International Conference on Network Security and Blockchain Technology*, Springer, 2022, pp. 51–63.
[46] W. Li, W. Meng, and S. Furnell, "Exploring touch-based behavioral authentication on smartphone email applications in IoT-enabled smart cities," *Pattern Recognition Letters*, vol. 144, pp. 35–41, 2021.
[47] S. Duraibi, "Voice biometric identity authentication model for IoT devices," *International Journal of Security, Privacy and Trust Management (IJSPTM) Vol*, vol. 9, 2020.
[48] N. Ghosh, S. Chandra, V. Sachidananda, and Y. Elovici, "SoftAuthZ: a context-aware, behavior-based authorization framework for home IoT," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10773–10785, 2019.

[49] D. Li, W. Peng, W. Deng, and F. Gai, "A blockchain-based authentication and security mechanism for IoT," in *2018 27th International Conference on Computer Communication and Networks (ICCCN)*, IEEE, 2018, pp. 1–6.
[50] U. Khalid, M. Asim, T. Baker, P. C. Hung, M. A. Tariq, and L. Rafferty, "A decentralized lightweight blockchain-based authentication mechanism for IoT systems," *Cluster Computing*, vol. 23, no. 3, pp. 2067–2087, 2020.
[51] S. Guo, X. Hu, S. Guo, X. Qiu, and F. Qi, "Blockchain meets edge computing: A distributed and trusted authentication system," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 1972–1983, 2019.
[52] S. Kakei, Y. Shiraishi, M. Mohri, T. Nakamura, M. Hashimoto, and S. Saito, "Cross-certification towards distributed authentication infrastructure: A case of hyperledger fabric," *IEEE Access*, vol. 8, pp. 135742–135757, 2020.
[53] B. K. Mohanta, A. Sahoo, S. Patel, S. S. Panda, D. Jena, and D. Gountia, "Decauth: Decentralized authentication scheme for iot device using ethereum blockchain," in *TENCON 2019-2019 IEEE Region 10 Conference (TENCON)*, IEEE, 2019, pp. 558–563.
[54] A. Yazdinejad, G. Srivastava, R. M. Parizi, A. Dehghantanha, K.-K. R. Choo, and M. Aledhari, "Decentralized authentication of distributed patients in hospital networks using blockchain," *IEEE journal of biomedical and health informatics*, vol. 24, no. 8, pp. 2146–2156, 2020.
[55] D. Díaz-Sánchez, A. Marín-Lopez, F. Almenárez Mendoza, and P. Arias Cabarcos, "DNS/DANE collision-based distributed and dynamic authentication for microservices in IoT," *Sensors*, vol. 19, no. 15, p. 3292, 2019.
[56] P. Sudhakaran, "Energy efficient distributed lightweight authentication and encryption technique for IoT security," *International Journal of Communication Systems*, vol. 35, no. 2, p. e4198, 2022.
[57] G. Pathak, J. Gutierrez, A. Ghobakhlou, and S. U. Rehman, "LPWAN Key Exchange: A Centralised Lightweight Approach," *Sensors*, vol. 22, no. 13, p. 5065, 2022.
[58] U. Verma and D. Bhardwaj, "CMAKM-FIoT: centralised mutual authentication and key management scheme for fog computing-enabled IoT network," *International Journal of Electronic Business*, vol. 17, no. 4, pp. 407–427, 2022.
[59] Z. Li, Q. Miao, S. A. Chaudhry, and C.-M. Chen, "A provably secure and lightweight mutual authentication protocol in fog-enabled social Internet of vehicles," *International Journal of Distributed Sensor Networks*, vol. 18, no. 6, p. 15501329221104332, 2022.
[60] S. Farooq and P. Chawla, "A Novel Approach of Mutual Authentication in Fog Computing," in *Proceedings of First International Conference on Computational Electronics for Wireless Communications*, Springer, 2022, pp. 567–581.
[61] A. Gupta, M. Tripathi, S. Muhuri, G. Singal, and N. Kumar, "A secure and lightweight anonymous mutual authentication scheme for wearable devices in Medical Internet of Things," *Journal of Information Security and Applications*, vol. 68, p. 103259, 2022.
[62] A. B. Amor, S. Jebri, M. Abid, and A. Meddeb, "A Secure Lightweight Mutual Authentication Scheme in Social Industrial IoT Environment," 2022.
[63] I. Alshawish and A. Al-Haj, "An efficient mutual authentication scheme for IoT systems," *The Journal of Supercomputing*, pp. 1–32, 2022.
[64] U. Jain, S. Pirasteh, and M. Hussain, "Lightweight, secure, efficient, and dynamic scheme for mutual authentication of devices in Internet-of-Things-Fog environment," *Concurrency and Computation: Practice and Experience*, vol. 35, no. 1, p. e7428, 2023.
[65] H. Park, M. Kim, and J. Seo, "IoT Multi-Phase Authentication System Using Token Based Blockchain," *KIPS Transactions on Computer and Communication Systems*, vol. 8, no. 6, pp. 139–150, 2019.
[66] B. B. Rao and A. A. Waoo, "DESIGN A NOVEL APPROACH FOR TOKEN BASED AUTHENTICATION IN IOT NETWORKS.," *Ilkogretim Online*, vol. 20, no. 4, 2021.
[67] B. B. Rao and A. A. Waoo, "Advanced System to Identify Users and Devices in IoT using Token-Based Authentication".
[68] L. Sasirega and C. Shanthi, "LIGHTWEIGHT ECC AND TOKEN BASED AUTHENTICATION MECHANISM FOR WSN-IOT," *Научно-технический вестник информационных технологий, механики и оптики*, vol. 22, no. 2, pp. 332–338, 2022.
[69] Z. Xu, W. Liang, K.-C. Li, J. Xu, A. Y. Zomaya, and J. Zhang, "A Time-sensitive Token-Based Anonymous Authentication and Dynamic Group Key Agreement Scheme for Industry 5.0," *IEEE Transactions on Industrial Informatics*, 2021.
[70] N. S. Yadav, M. Rao, D. V. Parameswari, K. L. S. Soujanya, and C. M. Latha, "Accessing Cloud Services Using Token based Framework for IoT Devices.," *Webology*, vol. 18, no. 2, 2021.
[71] P. Klimushyn, T. Solianyk, O. Mozhaev, V. Nosov, T. Kolisnyk, and V. Yanov, "HARDWARE SUPPORT PROCEDURES FOR ASYMMETRIC AUTHENTICATION OF THE INTERNET OF THINGS," *Innovative Technologies and Scientific Solutions for Industries*, no. 4 (18), pp. 31–39, 2021.
[72] Y.-H. Chuang and C.-L. Lei, "PUF Based Authenticated Key Exchange Protocol for IoT Without Verifiers and Explicit CRPs," *IEEE Access*, vol. 9, pp. 112733–112743, 2021.
[73] P. Mall, R. Amin, A. K. Das, M. T. Leung, and K.-K. R. Choo, "PUF-based authentication and key agreement protocols for IoT, WSNs and smart grids: a comprehensive survey," *IEEE Internet of Things Journal*, 2022.
[74] A. Braeken, "PUF-Based Authentication and Key Exchange for Internet of Things," *IoT Security: Advances in Authentication*, pp. 185–204, 2020.
[75] K. Lounis and M. Zulkernine, "Lessons Learned: Analysis of PUF-based Authentication Protocols for IoT," *Digital Threats: Research and Practice*, 2021.

[76] A. Shamsoshoara, A. Korenda, F. Afghah, and S. Zeadally, "A survey on physical unclonable function (PUF)-based security solutions for Internet of Things," *Computer Networks*, vol. 183, p. 107593, 2020.
[77] C. Wang, D. Wang, G. Xu, and D. He, "Efficient privacy-preserving user authentication scheme with forward secrecy for industry 4.0," *Science China Information Sciences*, vol. 65, no. 1, pp. 1–15, 2022.
[78] M. Mumtaz, J. Akram, and L. Ping, "An RSA based authentication system for smart IoT environment," in *2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, IEEE, 2019, pp. 758–765.
[79] 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, p. 1962, 2020.
[80] X. Wang, X. She, L. Bai, Y. Qing, and F. Jiang, "A novel anonymous authentication scheme based on edge Computing in Internet of vehicles," *Computers, Materials & Continua*, vol. 67, no. 3, pp. 3349–3361, 2021.
[81] A. Tewari and B. B. Gupta, "A novel ECC-based lightweight authentication protocol for internet of things devices," *International Journal of High Performance Computing and Networking*, vol. 15, no. 1–2, pp. 106–120, 2019.
[82] 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.
[83] S. Hussain, S. A. Chaudhry, O. A. Alomari, M. H. Alsharif, M. K. Khan, and N. Kumar, "Amassing the security: An ECC-based authentication scheme for Internet of drones," *IEEE Systems Journal*, vol. 15, no. 3, pp. 4431–4438, 2021.
[84] A. Lohachab, "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.
[85] S. Rostampour, M. Safkhani, Y. Bendavid, and N. Bagheri, "ECCbAP: A secure ECC-based authentication protocol for IoT edge devices," *Pervasive and Mobile Computing*, vol. 67, p. 101194, 2020.
[86] S. Gabsi, Y. Kortli, V. Beroulle, Y. Kieffer, A. Alasiry, and B. Hamdi, "Novel ECC-based RFID mutual authentication protocol for emerging IoT applications," *IEEE Access*, vol. 9, pp. 130895–130913, 2021.
[87] A. K. Das, M. Wazid, A. R. Yannam, J. J. Rodrigues, and Y. Park, "Provably secure ECC-based device access control and key agreement protocol for IoT environment," *IEEE Access*, vol. 7, pp. 55382–55397, 2019.
[88] 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.
[89] P. K. Dhillon and S. Kalra, "Secure and efficient ECC based SIP authentication scheme for VoIP communications in internet of things," *Multimedia Tools and Applications*, vol. 78, no. 16, pp. 22199–22222, 2019.
[90] C.-T. Chen, C.-C. Lee, and I.-C. Lin, "Correction: Efficient and secure three-party mutual authentication key agreement protocol for WSNs in IoT environments," *Plos one*, vol. 15, no. 6, p. e0234631, 2020.
[91] B. Hu, W. Tang, and Q. Xie, "A Two-factor Security Authentication Scheme for Wireless Sensor Networks in IoT Environments," *Neurocomputing*, 2022.
[92] 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.
[93] D. Kumar, S. Chand, and B. Kumar, "Cryptanalysis and improvement of a user authentication scheme for wireless sensor networks using chaotic maps," *IET Networks*, vol. 9, no. 6, pp. 315–325, 2020.
[94] D. Kaur, D. Kumar, K. K. Saini, and H. S. Grover, "An improved user authentication protocol for wireless sensor networks," *Transactions on Emerging Telecommunications Technologies*, vol. 30, no. 10, p. e3745, 2019.
[95] J. Oh, S. Yu, J. Lee, S. Son, M. Kim, and Y. Park, "A secure and lightweight authentication protocol for IoT-based smart homes," *Sensors*, vol. 21, no. 4, p. 1488, 2021.
[96] P. K. Panda and S. Chattopadhyay, "A secure mutual authentication protocol for IoT environment," *Journal of Reliable Intelligent Environments*, vol. 6, no. 2, pp. 79–94, 2020.
[97] M. Dammak, O. R. M. Boudia, M. A. Messous, S. M. Senouci, and C. Gransart, "Token-based lightweight authentication to secure IoT networks," in *2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, IEEE, 2019, pp. 1–4.
[98] Q. Xie, Z. Ding, and B. Hu, "A secure and privacy-preserving three-factor anonymous authentication scheme for wireless sensor networks in Internet of Things," *Security and Communication Networks*, vol. 2021, 2021.
[99] 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.
[100] T. M. Butt, R. Riaz, C. Chakraborty, S. S. Rizvi, and A. Paul, "Cogent and energy efficient authentication protocol for wsn in iot," *Comput. Mater. Contin*, vol. 68, pp. 1877–1898, 2021.
[101] V. O. Nyangaresi, "Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography," *Journal of Systems Architecture*, vol. 133, p. 102763, 2022.
[102] J. Cui, F. Cheng, H. Zhong, Q. Zhang, C. Gu, and L. Liu, "Multi-factor based session secret key agreement for the Industrial Internet of Things," *Ad Hoc Networks*, vol. 138, p. 102997, 2023.
[103] S. Yu and K. Park, "ISG-SLAS: Secure and lightweight authentication and key agreement scheme for industrial smart grid using fuzzy extractor," *Journal of Systems Architecture*, vol. 131, p. 102698, 2022.
[104] R. Krishnasrija, A. K. Mandal, and A. Cortesi, "A lightweight mutual and transitive authentication mechanism for IoT network," *Ad Hoc Networks*, vol. 138, p. 103003, 2023.

[105] J. Lee *et al.*, "PUFTAP-IoT: PUF-Based Three-Factor Authentication Protocol in IoT Environment Focused on Sensing Devices," *Sensors*, vol. 22, no. 18, p. 7075, 2022.
[106] X. Wang, Y. Teng, Y. Chi, and H. Hu, "A Robust and Anonymous Three-Factor Authentication Scheme Based ECC for Smart Home Environments," *Symmetry*, vol. 14, no. 11, p. 2394, 2022.
[107] A. K. Yadav, M. Misra, P. K. Pandey, and M. Liyanage, "An EAP-based mutual authentication protocol for WLAN connected IoT devices," *IEEE Transactions on Industrial Informatics*, 2022.
[108] P. Bagga, A. Mitra, A. K. Das, P. Vijayakumar, Y. Park, and M. Karuppiah, "Secure biometric-based access control scheme for future IoT-enabled cloud-assisted video surveillance system," *Computer Communications*, vol. 195, pp. 27–39, 2022.
[109] N. Garg, R. Petwal, M. Wazid, D. P. Singh, A. K. Das, and J. J. Rodrigues, "On the design of an AI-driven secure communication scheme for internet of medical things environment," *Digital Communications and Networks*, 2022.
[110] S. K. Dwivedi, R. Amin, and S. Vollala, "Design of secured blockchain based decentralized authentication protocol for sensor networks with auditing and accountability," *Computer Communications*, vol. 197, pp. 124–140, 2023.
[111] S. Rostampour, N. Bagheri, Y. Bendavid, M. Safkhani, S. Kumari, and J. J. Rodrigues, "An authentication protocol for next generation of constrained Iot systems," *IEEE Internet of Things Journal*, vol. 9, no. 21, pp. 21493–21504, 2022.
[112] R. Kumar, S. Singh, and P. K. Singh, "A secure and efficient computation based multifactor authentication scheme for Intelligent IoT-enabled WSNs," *Computers and Electrical Engineering*, vol. 105, p. 108495, 2023.
[113] B. Khalid, K. N. Qureshi, K. Z. Ghafoor, and G. Jeon, "An improved biometric based user authentication and key agreement scheme for intelligent sensor based wireless communication," *Microprocessors and Microsystems*, vol. 96, p. 104722, 2023.
[114] J. Pirayesh, A. Giaretta, M. Conti, and P. Keshavarzi, "A PLS-HECC-based device authentication and key agreement scheme for smart home networks," *Computer Networks*, p. 109077, 2022.
[115] R. Hajian, A. Haghighat, and S. H. Erfani, "A Secure Anonymous D2D Mutual Authentication and Key Agreement Protocol for IoT," *Internet of Things*, vol. 18, p. 100493, 2022.
[116] C. Patel, A. K. Bashir, A. A. AlZubi, and R. H. Jhaveri, "EBAKE-SE: A novel ECC-based authenticated key exchange between industrial IoT devices using secure element," *Digital Communications and Networks*, 2022.
[117] Y. Guo, Z. Zhang, and Y. Guo, "SecFHome: Secure remote authentication in fog-enabled smart home environment," *Computer Networks*, vol. 207, p. 108818, 2022.
[118] M. A. Khan, B. A. Alzahrani, A. Barnawi, A. Al-Barakati, A. Irshad, and S. A. Chaudhry, "A resource friendly authentication scheme for space–air–ground–sea integrated Maritime Communication Network," *Ocean Engineering*, vol. 250, p. 110894, 2022.
[119] A. K. Yadav, M. Misra, P. K. Pandey, K. Kaur, S. Garg, and X. Chen, "A Provably Secure ECC-based Multi-factor 5G-AKA Authentication Protocol".
[120] M. Azrour, J. Mabrouki, and R. Chaganti, "New efficient and secured authentication protocol for remote healthcare systems in cloud-iot," *Security and Communication Networks*, vol. 2021, 2021.
[121] 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.
[122] P. Guo, W. Liang, and S. Xu, "A privacy preserving four-factor authentication protocol for internet of medical things," *Computers & Security*, p. 103632, 2023.
[123] Z. Zhang *et al.*, "PRLAP-IoD: A PUF-based Robust and Lightweight Authentication Protocol for Internet of Drones," *Computer Networks*, vol. 238, p. 110118, 2024.
[124] M. Tanveer, A. Badshah, H. Alasmary, and S. A. Chaudhry, "CMAF-IIoT: Chaotic map-based authentication framework for Industrial Internet of Things," *Internet of Things*, vol. 23, p. 100902, 2023.
[125] S. U. Jan, A. Ghani, A. Alzahrani, S. M. Saqlain, K. Yahya, and H. Sajjad, "Bandwidth and Power Efficient Lightweight Authentication Scheme for Healthcare Systeme," *Journal of King Saud University-Computer and Information Sciences*, p. 101601, 2023.