Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.047625

REVIEW

Internet of Things Authentication Protocols: Comparative Study

Souhayla Dargaoui[1], Mourade Azrour[1,*], Ahmad El Allaoui[1], Azidine Guezzaz[2], Abdulatif Alabdulatif[3] and Abdullah Alnajim[4]

[1]Engineering Science and Technology Laboratory, IDMS Team, Faculty of Sciences and Techniques, Moulay Ismail University of Meknes, Errachidia, 52000, Morocco

[2]Higher School Essaouira, Cadi Ayyad University, Marrakesh, 44000, Morocco

[3]Department of Computer Science, College of Computer, Qassim University, Buraydah, 51452, Saudi Arabia

[4]Department of Information Technology, College of Computer, Qassim University, Buraydah, 51452, Saudi Arabia

*Corresponding Author: Mourade Azrour. Email: mo.azrour@umi.ac.ma

Received: 12 November 2023 Accepted: 22 February 2024 Published: 25 April 2024

ABSTRACT

Nowadays, devices are connected across all areas, from intelligent buildings and smart cities to Industry 4.0 and smart healthcare. With the exponential growth of Internet of Things usage in our world, IoT security is still the biggest challenge for its deployment. The main goal of IoT security is to ensure the accessibility of services provided by an IoT environment, protect privacy, and confidentiality, and guarantee the safety of IoT users, infrastructures, data, and devices. Authentication, as the first line of defense against security threats, becomes the priority of everyone. It can either grant or deny users access to resources according to their legitimacy. As a result, studying and researching authentication issues within IoT is extremely important. As a result, studying and researching authentication issues within IoT is extremely important. This article presents a comparative study of recent research in IoT security; it provides an analysis of recent authentication protocols from 2019 to 2023 that cover several areas within IoT (such as smart cities, healthcare, and industry). This survey sought to provide an IoT security research summary, the biggest susceptibilities, and attacks, the appropriate technologies, and the most used simulators. It illustrates that the resistance of protocols against attacks, and their computational and communication cost are linked directly to the cryptography technique used to build it. Furthermore, it discusses the gaps in recent schemes and provides some future research directions.

KEYWORDS

Attacks; cryptography; Internet of Things; security; authentication

1 Introduction

IoT is an extensive network of intelligent goods interconnected and connected to the Internet that may visualize and control a big part of the world surrounding us. Over the past few years, IoT has immersed increasingly in our daily lives [1–5]. This extensive integration of IoT services anywhere and everywhere generates significant data flow [6–10]. The limited nature of IoT appliances concerning computational capability, energy, and memory storage makes the processing of IoT data a

This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

very sophisticated task [11–13]. As a result, IoT users' data becomes susceptible to illegitimate use, and attacks against IoT networks become increasingly sophisticated, numerous, and of excellent quality. According to recent examinations, this increase is a direct result of poor security configurations placed throughout the IoT ecosystem [14–16]. Several factors make IoT security very hard to achieve, such as the absence of security configuration in IoT devices since the constructors are more interested in getting their devices on the market quicker than in conducting sufficient tests to include security from the outset [17–20]. In addition, wireless communication networks used in IoT, like Wi-Fi, are known for their vulnerability to enormous interferences. Furthermore, the lack of a unique perspective of IoT and universal standards may increase the difficulty of designing a security scheme for an IoT network with heterogeneous equipment. Moreover, high mobility and dynamic network topology may increase the attack area and complicate the implementation of a universal security scheme.

Authentication as a method of verifying and ensuring the identification of entities is the first step towards security and privacy assurance in an IoT environment. Generally, in IoT networks, each node should be able to distinguish and attest all other nodes in the network to ensure that the data comes from a legitimate source [21]. Authentication is a process that allows verification or authentication of a user's identity. It answers the question: "Are you that entity?". Authentication methods are diverse, but all are founded upon one or more of the knowledge, possession, and attribute factors.

Overall, the more factors we use, the higher the level of safety we provide. However, multi-factor authentication requires more computational power, storage memory, and energy, which cannot be ensured by IoT-embedded devices, known by their limitations. Over the past few years, several lightweight authentications have been proposed to overcome those limitations. The performance of proposed authentication schemes and their costs differ based on the cryptographic techniques used, such as Advanced Encryption Standard (AES), Rivest–Shamir–Adleman (RSA), Elliptic Curve Cryptography (ECC), and so on [22].

New researchers attend this survey as a guideline to enhance future research and opportunities. It offers the analysis of a comparison study between more than thirty current authentication protocols published from 2019 to 2023 based on the cryptographic mechanisms used, the provided security features, the resistance against most popular attacks, and the computation and communication cost. The contributions of this paper are as follows:

- We summarize and analyze recent research in the IoT authentication field to provide a comprehensive understanding of the current literature, providing the most used cryptographic techniques, and simulation tools.
- We present a simple taxonomy of IoT authentication schemes.
- We undertake a comparative analysis to determine if the current literature satisfies the security service requirements and resists well-known attacks.
- We pinpoint open challenges exploring gaps and weaknesses and afford new research directions.

The remainder of our survey is structured that way. The related works are introduced in section two. In the third section, the research methodology is presented. A simple taxonomy of authentication protocols is presented in section four. The comparison study is detailed in section five. The sixth section presents future research directions. Finally, the seventh section concludes the paper.

2 Related Work

Over the past few years, multiple authentication systems and key agreements have been offered to ensure privacy and security in IoT environments. Several authentication comparison studies are

offered in the literature to help future researchers by offering security issues, open challenges, and future scopes (see Table 1). Kumar et al. presented an exhaustive investigation of the Internet-of-Things authentication methods and their conjunctions [23]. They analyzed the potentialities and drawbacks of the existing approaches. Furthermore, discussing the fundamentals of authentication and its related raids, they interlinked the evolution of the solution strategies and offered a taxonomy of IoT authentication. Finally, they discussed the future opportunities in this area. Trnka et al. [24] offered a road map for future research, providing an overview of recent research from 2017 to 2020. They categorized implicated mechanics and norms requested in current approaches to finding the taxonomy of IoT security solutions. Saqib et al. afforded a methodical IoT security assessment and review concerning authentication [25]. Their review aims to discover and summarize security issues in IoT regarding authentication tools and identify available mechanisms and holes in several kinds of authentication. Firstly, they identified security and privacy issues and explained the security warning throughout multiple levels of the IoT architecture. Secondly, they mentioned the countermeasures attainable for handling security problems.

Table 1: Areas covered by some related works

Review	Key areas covered
Kumar et al. [23]	IoT layers, Security perspectives, and attacks, WSN-based authentication, IIoT authentication, IoMT authentication, VANET authentication, Non-specific applications of authentication, Lightweight authentication, Blockchain-based enablers, and open issues.
Trnka et al. [24]	Taxonomy of security solutions, topologies, communication types, and perspectives of IoT authentication and authorization.
Saqib et al. [25]	Security and privacy issues, security threats, and countermeasures, formal security evaluations, and network simulation tools.
Bahache et al. [26]	Architecture of WMSNs, Medical Sensors, Security and Privacy Requirements, Attacks on Authentication Schemes in WMSN, Formal Security Analysis Techniques, Classification of Authentication Schemes in WMSNs.
Ahmed et al. [27]	Identity management, lightweight authentication, and authorization.
Singh et al. [28]	Blockchain, decentralized authentication, and access management.
Mohsin et al. [29]	Taxonomy of blockchain technology in authentication, Blockchain technology challenges and proposed solutions, importance, capabilities, motivations, and challenges of blockchain technology.
Sodhro et al. [30]	Taxonomy for IoT-5G healthcare, IoT-5G authentication, and intelligent authentication of IoT-5G healthcare devices (using AI).
Jiang et al. [31]	5G-based Internet of Things, physical layer authentication (PLA) schemes using machine learning for the 5G-based IoT.
Wazid et al. [32]	5G-enabled IoT, security requirements and potential attacks, categories of security protocols in 5G-enabled IoT, and the challenging problem of the future in the security of 5G-enabled IoT.

(Continued)

Table 1 (continued)

Review	Key areas covered
Ferrag et al. [33]	Bio-features, trends of biometric technologies, Biometric Authentication, machine learning and data mining algorithms used by biometric-based authentication, Authentication and Authorization Schemes for Mobile IoT Devices Using Bio-features.
Yang et al. [34]	Biometric-based authentication and encryption for the IoT, classification of IoT-related biometric authentication systems, Challenges brought by the deployment of biometric systems in the IoT, and potential solutions.

Additionally, they used different robustness parameters such as computational cost, communications costs, and energy use to benchmark some of the current standard authentication protocols developed for IoT. In the end, network simulators employed to estimate the efficiency of authentication approaches are covered. Bahache et al. [26] presented a comprehensive study of today's authentication protocols regarding security and achievement. They also offered new categorization of the authentication schemes in wireless medical sensor networks (WMSNs) based on their architecture. Ahmed et al. [27] also summarized existing research on identity management, lightweight authentication, and authorization in an IoT environment. As a result, they highlighted topical IoT security trends and their accomplishments.

To explore how Blockchain-based decentralized architecture can enhance IoT authentication, Singh et al. proposed a review of access management of IoT devices using access control mechanisms and decentralized authentication [28]. They analyzed existing studies on Blockchain applications and detailed efforts to improve security in IoT applications. Accordingly, they summarized various security issues related to decentralized authentication in the IoT environment. Mohsin et al. [29] also provided helpful information that may improve the comprehension of how authentication approaches may be blended with Blockchain technology. They came up with a taxonomy of Blockchain technology in IoT network authentication. At last, they surveyed issues related to Blockchain technology, presented solutions, and discussed future research directions.

Recently, IoT over 5G networks have improved healthcare applications. Sodhro et al. [30] produced an exhaustive review of authentication approaches for protecting IoT-5G appliances in the medical field. They reviewed, characterized, clustered, and classified IoT-5G appliance authentication, radio-frequency fingerprinting, and mutual authentication. Finally, they presented some artificial intelligence methods for developing authentication and recommendations for future research. Jiang et al. [31] briefly investigated machine learning-based physical layer authentication for the 5G-based Internet of Things. The paper also covered research directions of machine learning approaches applications in 5G-based IoT security. Wazid et al. [32] presented a survey detailing probable rules and raids in 5G-enabled IoT networks. They compared current security schemes that lead to future search obstacles, and orientations in 5G IoT environmental security.

Given that bio-features have become a vital agent in IoT device authentication. Ferrag et al. presented a survey about IoT mobile device authentication and authorization using bio-features [33]. They delivered distinct data mining and machine-learning approaches to authentication and authorization

mechanisms of IoT devices. Finally, analyzing the available biometrics authentication systems posed various issues for future investigation works. Yang et al. [34] presented a review to assist scientists in comprehending future problems with biometrics for IoT security and future research directions. They studied the existing studies in biometrics-based IoT security, specifically authentication, and encryption. Additionally, they classified the research about several biometric features and the number of biometric characteristics used in the mechanism.

3 Research Methodology

Our review was conducted between 2019 and 2023 since IoT authentication has received a lot of attention recently. The research published within the last five years presents the integration of emerging technologies and tendencies to enhance IoT authentication, the thing that helps to better understand the state of the art.

The research process consisted of several phases. Firstly, we collected papers using a pre-defined set of keywords (attacks, cryptography, Internet of Things, security, authentication). For this purpose, we navigated some digital sources such as:

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

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

Inclusion criteria

- Papers target IoT authentication.
- Papers afford a new IoT authentication scheme.
- Papers provide a security analysis section for the proposed scheme.
- Papers provide a performance evaluation section for the proposed scheme.
- Papers explore the challenges, issues, and shortcomings of IoT authentication.

Exclusion criteria

- Papers not written in the English language.
- Papers published before 2019.
- Papers duplicated.
- Papers that do not provide any new authentication protocol.

Then, reviewing the titles and keywords we excluded unrelated papers. Later, the analysis of each article's abstract was performed to decide their relevance and exclude irrelevant publications.

Finally, the quality of the papers was checked using three quality assessment questions, if the answer to at least two of these questions was "yes" the papers were concluded, else the papers were excluded from the review study, the questions are the following:

- Is there sufficient coverage of the relevant work and research subject in the paper?
- Is there enough information in the paper about the proposed authentication methodology?

• Is there a clear description, analysis, and evaluation of the findings?

In the end, we admit thirty-one papers as the subject of the comparison study.

4 Taxonomy of the IoT Authentication Protocols

We classify IoT authentication protocols in this fraction according to several parameters [35]. These parameters are pictured in Fig. 1 and summarized as follows:

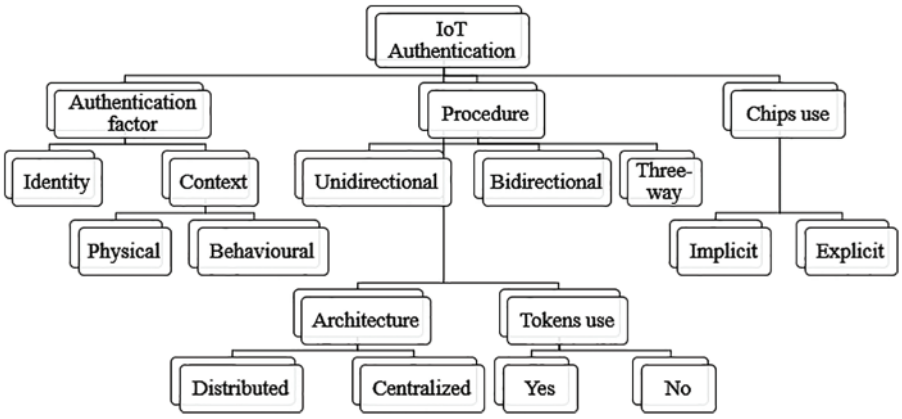

Figure 1: Classification of IoT authentication protocols

Authentication factor: Can be either identity [36–40], which is information (Username, password) presented by one party to another to authenticate, or an attribute [41–44] (what we need to be), that can be physical like fingerprints or hand geometry, or behavioral like typing dynamics or voice prints [45–48].

Architecture: This is distributed when a direct authentication method distributed between the communicating parties is used [49–53], or centralized [54–58] when a trusted authority that allows us to distribute and manage identification data used during authentication is used.

Procedure: This can be unidirectional in case only one party authenticates to the other while the other is not authenticated. Bidirectional (mutual authentication [59–61]) whenever the two items attest to each other. Three-way authentication once a trusted power certificates both items and assists them to certificate each other [62–64].

Tokens use: In token-based authentication schemes [65–69], the user authenticates from a proof of identity (data) established by a server [70].

The chips use: That may be implicit, whether it uses material physical features to improve authentication, including physical unclonable functions [71–75], or explicit, where it uses chips that store and process keys used for authentication [76].

5 Comparative Study

5.1 Comparative Criteria

Resistance against attacks: This is a notable feature in an authentication scheme. The authentication protocol must resist attacks as much as possible to secure the data exchanged during the session. As a result, the stronger the resistance, the better the authentication.

Complexity: In IoT networks, energy is the most critical limiting factor relative to the capabilities of a sensor node. To extend as much as possible, the life of a sensor and that of the network, it is necessary to manage its energy reserve reasonably. Therefore, to build an effective authentication mechanism, it is necessary to limit the number of operations performed.

Session key management: A session key is used to define encryption between two parties to communicate securely over an open network. The management of session keys is a crucial issue of IoT, which includes several steps: Generation, distribution, storage, updating, and destruction of keys. Generally, a key agreement protocol should be used to negotiate a session key influenced by all communicating parties.

Factor number: We can distinguish between three authentication schemes depending on the number of factors considered to authenticate the user. A single-factor authentication (SFA) is where the user authenticates using the password only. A dual-factor authentication (2FA) is where the customer uses a smart card and a keyword to authenticate. Multi-factor authentication (MFA) requires additional factors such as location information and biometrics.

Mutual authentication: Is an essential concept in the IoT authentication systems. It allows an IoT device to verify the legitimacy of the access request made by an entity (human being or another system) to authorize its access to network resources. On the other hand, the user must also be sure of the device's legitimacy.

Cryptographic algorithm used: Several cryptographic algorithms can be used during authentication. Based on these algorithms, we can classify authentication schemes into four classes. The first class is built on symmetric algorithms, given their low cost. The second category is based solely on asymmetric algorithms that may be separated into two types: Those using usual algorithms (RSA [77–80]) and those using elliptic curve cryptography (ECC [81–84]). The third category is hash functions-based schemes. The last category consists of hybrid solutions mixing two or all existing methods [85–89].

5.2 Comparison of the Studied Protocols

This section provides the comparison result between some of the latest authentication protocols, especially the protocols proposed between 2019 and 2023. Most of these protocols have four steps: The initialization step, the registration step, the login and authentication step, and the password change step. To fully understand and evaluate the protocols studied, we used several comparison criteria: Cryptography techniques, security services provided, resistance against attacks, computational complexity (execution time), and communication cost.

5.2.1 IoT Authentication Schemes Review

Table 2 shows the cryptographic techniques used in each protocol [90–120]. Hence, Chen et al. [90, 95,109,120] presented four different protocols based on two authentication factors using random numbers and hash functions. Finally, Oh et al. [95] and Azrour et al. [120] used the Automated Validation of Internet Security Protocols and Applications AVISPA and Scyther simulators, respectively, to formally analyze their protocol.

Table 2: Authentication schemes review

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	–
[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

(Continued)

Table 2 (continued)

Protocol	Cryptography techniques	Factors number	Simulator	Others
[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

(Continued)

Table 2 (continued)

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	–

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

Krishnasrija et al. [104] presented a scheme using two authentication factors, random numbers, hash functions, and Chebyshev's chaotic map. At the same time, Kumar et al. [93] also used encryption and decryption algorithms. The formal analysis of the presented schemes was performed by exploiting Scyther and Random Oracle, respectively.

Hu et al. [91,96,101] used random numbers, hash functions, and ECC to build two-factor authentication protocols. Azrour et al. [92,114,116,118] 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, 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. [102,105,108,113,117] 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 to perform a formal analysis of their protocol.

Xie et al. [98–100,103,106,112,115,119] 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 [99,103,112] are based on encryption and decryption algorithms, [98,106,115] are based on ECC, however, references [100,119] combined both techniques. Afterward, Xie et al. used ProVerif, Butt et al. [100], Yu et al. [103,112] used AVISPA, and Wang et al. [106] and Hajian et al. [115] used Scyther to make a formal analysis of their schemes.

Cryptography Techniques

The backbone of the authentication scheme is the cryptographic technique used to build it. It is the key element to establish authenticity, and the most critical factor that can construct the characteristics of the scheme; especially, its security and efficiency. The schemes examined in this review employ several cryptology technologies as shown in Table 2.

The hash function has been used in all the studied protocols, mathematically it is a one-way function that maps arbitrary-size data to fixed-size values. In authentication schemes, the utility of hash functions is to hide and protect confidential parameters from attacks.

ECC brings together a group of cryptographic techniques that take advantage of one or more attributes of elliptical curves. Given $Q = k * P$ where P is an elliptic curve point, the most crucial feature of ECC is the impossibility of recovering the value of k when only P and Q are known. Using this feature, the ECC can be used to interchange keys and secret parameters in the Diffie-Hellman manner or to verify authenticity using an elliptic curve digital signature algorithm and so on.

Encryption and decryption are popular techniques that may be used in authentication schemes to exchange confidential parameters securely in public channels or even store identity data safely in smart cards.

The chaotic map is an evolution function with some kind of chaotic behavior. It has an important characteristic that makes it suitable for security implementation; given Tu(x) and x, u is hard to compute. Considering this characteristic chaotic map may be used for key exchange or the authenticity warranty in the Diffie-Hellman approach.

Random numbers as it is clear from their name, are the numbers selected unexpectedly, randomly from a group of numbers. They play critical roles in the authentication schemes, hence they ensure untraceability and secure the scheme against freshness and replay attacks.

Formal Security Verification Tool

Authentication schemes are mathematical processes, the application of those procedures safely requires their verification and analysis. The formal analysis may reduce the computational cost, the communication cost, and even some time memory demand by detecting and eliminating unnecessary steps. Furthermore, the verification may lead to protocols enhancing by exploring their vulnerabilities. Table 2 shows that in the reviewed schemes the most used simulators are the following.

ProVerif which is a formal verification tool enables the verification of the security properties of cryptographic techniques. It runs the protocol only for an unlimited number of sessions and can reconstruct attacks. This tool accepts Horn clauses and Pi calculus codes as input and provides the same output in both cases. Furthermore, it does not demand any such specification or particular code in cases of schemes lacking freshness attacks. It necessitates the specification of communication channels and it only examines attacks that have the 'query' defined in the code [25].

AVISPA is a push-button tool introduced by Armando et al. as a toolkit for the validation of internet security protocols and applications. It affords four back-ends: The On-the-Fly Model-Checker, the Constraint-Logic-based Attack Searcher, the SAT-based Model Checker, and the TA4SP protocol analyzer. AVISPA tool can analyze all the components of the scheme at the same time, detect the protocol's flaws, and check the robustness against replay and man-in-the-middle attacks. However, it is rather difficult to use, demands solid knowledge of the verified schemes, and requires the learning of the High-Level Protocol Specification Language (HLPSL) [25].

Scyther is a simulator that provides automated verification, falsification, and analysis of security mechanisms. It has three usage modes: Claim verification to determine if the security claims made in the description are true or not, automatic claims to automatically elaborate and certify suitable claims for a protocol, and characterization to characterize and analyze the security mechanism and create a finite trace depicting the execution of the protocol role. Scyther tool offers a graphical user interface and provides graphs of attacks which facilitate understanding the security mechanism. More than that it can execute the protocol for a limited or unlimited number of sessions, and it may check all the used variables. Nevertheless, this tool requires a compromised module to detect that a previous session has been captured in case of a mechanism vulnerable to freshness threats, also it cannot check the quality of any variables the thing that obligates the user to simplify the protocol before the simulation [25].

5.2.2 Security Services

Generally, to trust an authentication protocol, it must ensure various security characteristics, such as mutual authentication, a security process that allows communicating parties to verify each other identities and trust the exchanged data in an IoT network. The anonymity secures the user's identity to overcome impersonation attacks; untraceability protects persons from disclosing confidential and sensitive information. Key agreement to generate a key, which may be used for encrypting the exchanged data. Perfect forward secrecy blocks unauthorized individuals from intercepting, deducting, or obtaining the key. Moreover, key secret, guards sensitive data secretly. As it is clear from Table 3 the schemes [91,93,94,101–105,115,118,120] are the most effective schemes providing all security services, then the schemes [95,97,98,106,107,111,113,116,117,119] which do not guarantee the key secret, and [108,109] that do not guarantee the perfect forward secrecy. However, protocol [112] offers mutual authentication, anonymity, untraceability, and key agreement. Protocols [99,100,114] allow mutual authentication, anonymity, and key agreement. Protocols [90,92] enable mutual authentication, key agreement, and key secret. Protocol [96] provides mutual authentication, key agreement, and perfect forward secrecy. Protocol [110] ensures only anonymity and untraceability.

Table 3: 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]	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓	-	✓	✓	-	✓	-

(Continued)

Table 3 (continued)

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}
[104]	✓	✓	✓	✓	✓	✓	-	✓	-	-	✓	-	-	✓	✓	-	✓	-
[105]	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	-	✓	-	✓	✓	-	✓	-
[106]	✓	✓	✓	✓	✓	-	✓	✓	✓	-	✓	✓	-	✓	✓	-	✓	-
[107]	✓	✓	✓	✓	✓	-	✓	✓	-	-	✓	-	-	-	-	-	-	-
[108]	✓	✓	✓	✓	-	✓	✓	✓	-	-	✓	-	-	-	✓	-	✓	-
[109]	✓	✓	✓	✓	-	✓	✓	✓	✓	-	✓	-	-	-	✓	-	✓	-
[110]	×	✓	✓	-	-	-	✓	-	-	-	-	-	-	-	-	-	✓	-
[111]	✓	✓	✓	✓	✓	-	✓	✓	-	-	-	-	-	-	-	-	-	-
[112]	✓	✓	✓	✓	-	-	✓	✓	-	-	✓	-	-	✓	✓	-	-	-
[113]	✓	✓	✓	✓	✓	-	✓	-	-	-	-	-	-	-	✓	-	-	-
[114]	✓	✓	-	✓	-	-	✓	✓	-	×	-	✓	-	-	-	-	✓	-
[115]	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	-	-	-	-	-	✓	-
[116]	✓	✓	✓	✓	✓	-	✓	✓	-	-	✓	-	-	-	-	-	✓	-
[117]	✓	✓	✓	✓	✓	-	✓	✓	✓	-	✓	-	-	✓	✓	✓	✓	-
[118]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	-	✓	-	-	✓	-
[119]	✓	✓	✓	✓	✓	-	-	✓	-	-	-	-	-	-	✓	-	-	-
[120]	✓	✓	✓	✓	✓	✓	-	✓	-	✓	✓	✓	-	✓	✓	-	-	-

Note: F1: Mutual authentication, F2: Anonymity, F3: Unlinkability, F4: Key agreement, F5: Key secrecy, F6: Perfect forward secrecy, A1: Impersonation attack, A2: Replay 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. ✓: Resist (attacks)/possess (features), ×: Suffer (attacks)/no (properties), -: No information available.

5.2.3 Resistance against Attacks

The comparison based on security services provided by each protocol may give an idea about the studied protocol; instead, more is needed to evaluate it. For this reason, resistance against known attacks is examined in this section. Analyzing Table 3, 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, replay attacks, node capture attacks, password guessing, DoS attacks, stolen verifier attacks, insider attacks, stolen verifier attacks, a man in the middle, and smart card loss attack. Nevertheless, references [99,103] resist all recent attacks except the node capture attack. In addition, references [93,94] 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 the DoS attack. The scheme [117] protects against GWN bypassing attacks and the same attacks as [98], apart from the stolen verifier, DoS.

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

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

The scheme [112] resists in the face of impersonation attacks, replay attacks, insider attacks, smart card loss, and password guessing. Nevertheless, the scheme [104] resists man-in-the-middle attacks coupled with all later attacks excluding impersonation attacks. In addition, reference [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, replay attacks, smart card loss, insider attacks, and man-in-the-middle attacks. However, the approach [115] can resist counter-node capture attacks and attacks resisted by [108] apart from the smart card loss. The scheme [96] also resists password guessing, and all attacks resisted by [108] exclude 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 are restrained by [116] but insider attacks. On the other hand, the mechanism [101] resists DoS attacks and raids resisting by the mechanism [116] aside from insider attacks. The scheme [100] resists impersonation attacks, insider attacks, replay attacks, and password-guessing attacks. Nonetheless, the protocol [90] resists insider attacks, replay attacks, GWN bypassing, and stolen verifier attacks. The scheme [107] can also resist the same attacks as the scheme [116] apart from the man in the middle.

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

5.2.4 Computational Cost

In this section, we examine the computational needs of the studied schemes. The notation Th is defined as the temporal requirements of the hash function. Te is the temporal requirement 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 the physically unclonable function. Tsig is the computational cost of a Hyperelliptic Curve-based Digital Signature Arithmetic signature generation/verification execution. 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 s and according to [97], Tasym = Te = Tf = 0.063075 s. Depending on [105] Th = 1.91%∗ Tpuf, as a result, we consider Tpuf = 0,02608 s. Based on [93,114], Tsig = 0.47 s.

As mentioned in Table 4, two-factor lightweight authentication schemes, [90,95,109,120], require 24Th, 42Th, 16Th, and 17Th, respectively. However, three-factor lightweight authentication schemes, [102,105,108,113,117] need 35Th+Tf, 34Th+2Tf+Tpuf, 29Th+Tf, 18Th+2Tf, and 2Tp+16Th+Tf, respectively.

Table 4: 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

(Continued)

Table 4 (continued)

Protocol	User	Getway	Sensor	Total	Execution time (ms)	Communication cost (bits)
[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	–

ECC-based schemes [91,96,98,101,106,115] demand 23Th + 6Te, 9Th + 8Te, 18Th + 6Te + Tf, 13Th + 2Te, 25Th + 6Te, and 8Te + 14Th severally. Symmetric encryption/decryption-based authentication schemes [94,97,99,103,107,110,111,112] necessitate 21Th + 4Ts, 42Th + Ts, 25Th + Tf + 4Ts, 15Th + Tf + 2Ts, 6Ts + 2Th, 6Th + 9Ts, 2Ts, and 24Th + 2Ts individually. In addition, [104] requires 20Th + 3Tc. While hybrid authentication schemes [92,93,100,114,116,118,119] stipulate 13Th + 6Te, 15Th+4Tc+4Ts, 5Th+4Te+Tf+3Ts, 15Th+2Tf+4Ts+2Tsig,2Ts+4Tasym+11Th, 13Th+8Te+2Ts, and Ts + 15Th + 6Te, respectively.

Fig. 2 shows that the protocols [90,95,97,109–112,120] are very fast compared to the schemes [91,92,96,98,100,106,114,118,119], for the simple reason that those letters use elliptic curve cryptography that is very overpriced compared to the hash functions that are used in schematics [90,95,97,109–112,120].

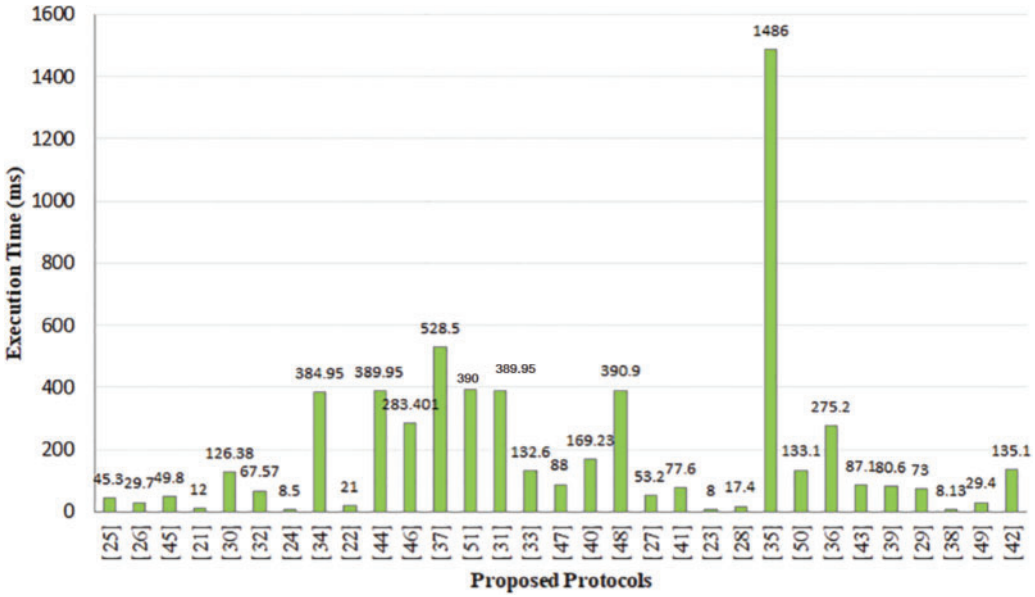

Figure 2: Login and identity verification estimated run time

5.2.5 Communication Cost

To enhance communication efficiency, the communication cost of an authentication scheme must be reduced as it as possible. Based on the graphs in Fig. 3, the schemes in [104,106,108,118,119] incur the highest communication overheads. Then there are the protocols in [94–102,105,109,112,113, 115,117], and the schemes in [103,107,111] with acceptable costs. While the schemes [107,111] require the lowest communication cost, and they are weak against the majority of known attacks, as has been mentioned before, more than that, they cannot ensure perfect forward secrecy.

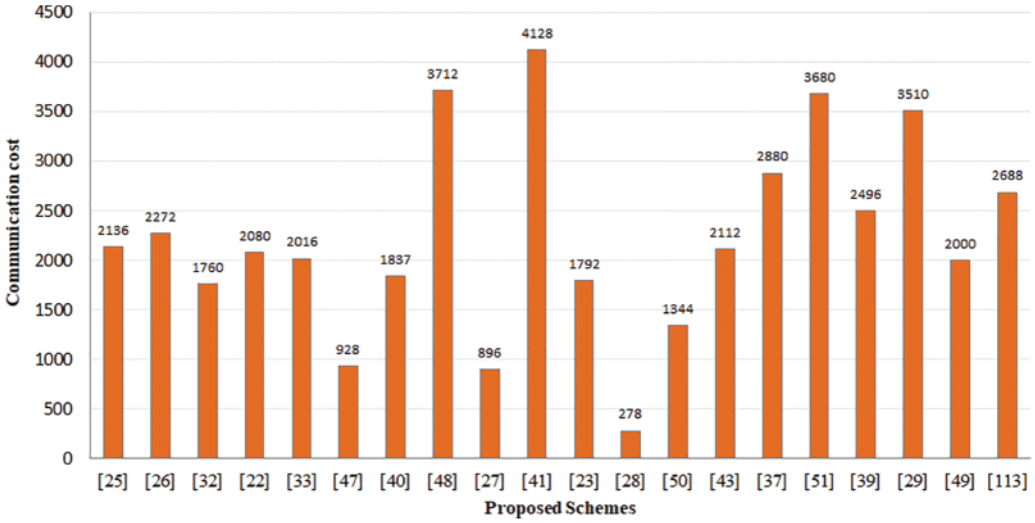

Figure 3: Login and identity verification estimated storage

5.3 *Classification of the Studied Protocols*

This section classifies the protocols we have studied into two categories. According to cryptographic algorithms, we distinguish lightweight schemes that are based only on hash functions, random numbers, and in some cases encryption and decryption algorithms, and hybrid schemes which combine the techniques used in the lightweight authentication schemes with one or more of the following mechanisms: Elliptic curve cryptography, chaotic maps, and encryption systems. Depending on the authentication factors, we distinguish between dual-factor schemes that require a smart card and password, and three-factor schemes that demand a smart card, key word, and digital fingerprint. The classification results in cryptographic algorithms and authentication factors are presented in Figs. 4 and 5, respectively. The analysis of Fig. 5 shows that a major part of the proposed schemes in the literature are two-factor-based schemes because the addition of the third factor increases partially the computational cost and the energy consumption. Furthermore, the correlation between the results presented in Fig. 2 which provides the login and identity verification estimated run time for each scheme, and the results shown in Fig. 4 indicate that hybrid authentication schemes require much more execution time than lightweight schemes. The thing that explains the wide deployment of lightweight schemes compared with others.

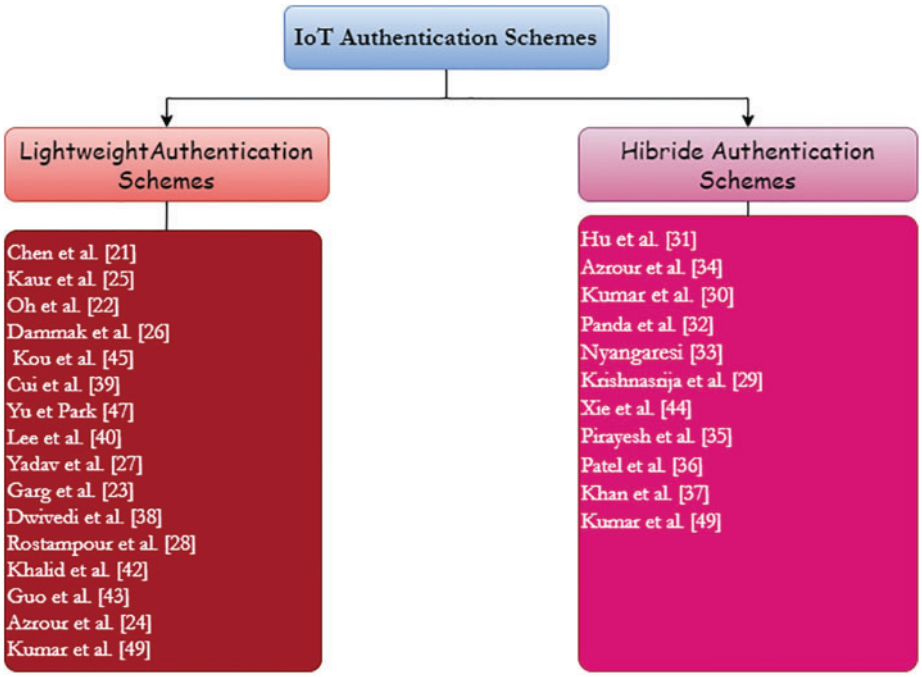

Figure 4: Classification results based on cryptographic technics

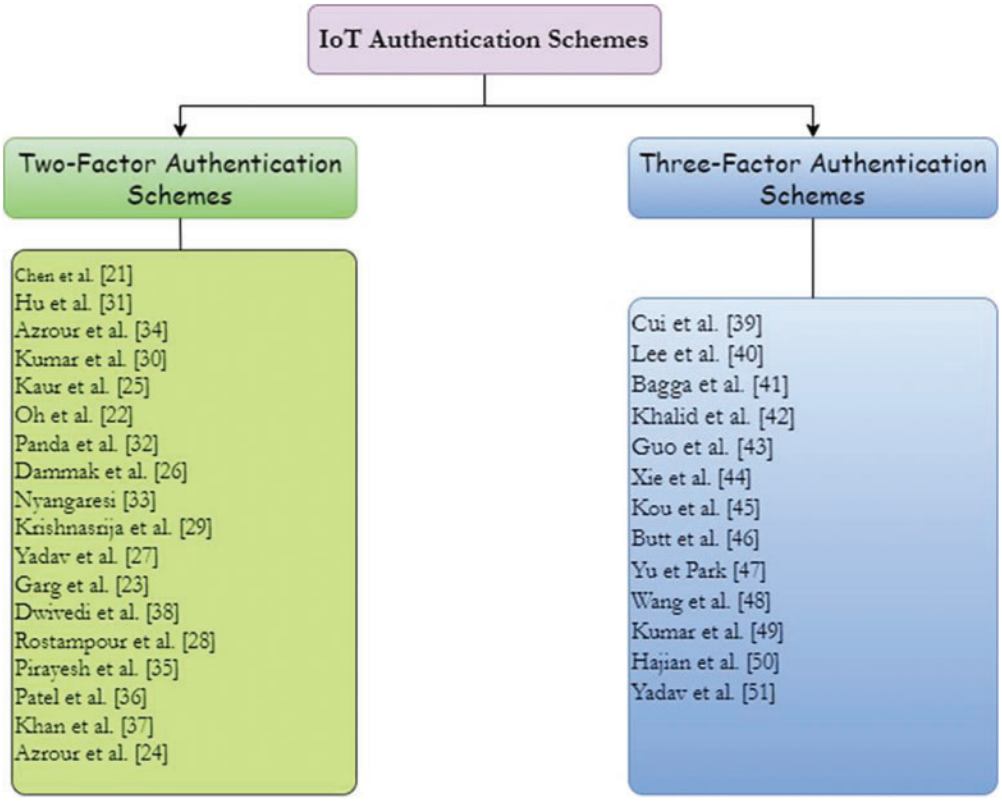

Figure 5: Classification results based on authentication factors

6 Future Research Directions

The comparison made in this paper illustrates that the reviewed schemes provide a high level of security, nonetheless, some attacks still require more interest such as node capture, DoS attack, stolen verifier, denning-ssaco attack, and GWN bypassing. Besides, the maturity of the authentication schemes is centralized, as a result, they cannot be efficient with decentralized infrastructures and networks. To overcome the gaps in the literature schemes this section offered some new directions for future research.

6.1 Blockchain-Based Authentication

Considering that a major part of the current IoT authentication schemes relies on centralized infrastructures, are inconsistent with distributed frameworks, and are vulnerable to several attacks, Blockchain-based authentication balances Blockchain technology with MFA to produce a trustworthy authentication mechanism. Using decentralized ledgers that protect critical credentials, Blockchain-based authentication offers an additional layer of protection. However, this kind of solution demands strong technical knowledge, accurate implementation, and realistic evaluation. More than that, it requires a high computational power. The whole potential of Blockchain-based authentication can be reached by decreasing complexity and costs and increasing flexibility and authenticity [121].

6.2 Post-Quantum Cryptography

Currently, ECC is considered one of the most lightweight cryptographic techniques that can be used to build a robust authentication scheme, and it is the most suitable for IoT device's limitations. Unfortunately, this method is at risk of being ruptured by Quantum Computing attacks such as Shor's Algorithm, Grover's Algorithm, Side-Channel Attack, Multi-target Pre-image Search Attack, and so on. However, the existence of some computational problems resistant to quantum attacks such as quasi-cyclic syndrome decoding (QCSD) with parity problem, and ring learning with rounding (RLWR) problems have motivated researchers to construct secure post-quantum cryptography (PQC). In 2017, a standardization proceeding was started by the National Institute of Standards and Technology, which classify which classify post-quantum cryptography algorithms into five classes: Lattice-based Cryptography, Code-based Cryptography, Multivariate Polynomial Cryptography, Hash-based Signatures, and Isogeny-based Cryptosystem. After the 3rd round, seven schemes were announced. However, the standardization document is expected to be published in 2024 [122].

6.3 Machine Learning for Authentication

Machine learning (ML) is an artificial intelligence field that relies on data and algorithms to imitate the way human learning, progressively improving its accuracy. Recently, Machine learning techniques have been widely considered to assist in the authentication process for IoT networks. Generally, the use of ML in authentication can be either: Supervised learning which is useful against intrusion and DDoS attacks, unsupervised learning which is useful to identify irregularities and threats without any previous knowledge, and powerful for communication detection attacks such as Sybil attacks, or reinforcement learning used to determine an optimal set of actions that maximize the reward in a given environment. Even though ML provides robust solutions for IoT authentication resistance against attacks, it demands high computation power and energy requirements. Researchers have a strong interest in making these solutions effective considering the limited nature of IoT devices [123,124].

7 Conclusion

This paper presents a deep comparative study of recent IoT authentication schemes regarding the importance of authentication in the Internet of Things as the first line of defense counter to security threats in such an environment. Firstly, we presented a simple taxonomy of authentication mechanisms in IoT. Then we offered the result of our detailed comparison. Our comparison was based on four criteria: The cryptographic mechanisms and simulators used, the provided security features, the resistance against most popular attacks, and the computational and communication cost. The result of our comparison shows that the authentication schemes in the literature may be based on several cryptography technics including Hash function, ECC, Encryption and decryption, Chaotic map, and Random numbers. Each one of the listed technologies has some features which may help provide authenticity and confidentiality. The requirement of the authentication scheme in terms of computational and communication costs differs according to the technology used. Accordingly, the analysis of the advantages and weaknesses of the studied schemes determines the attacks and the security services that need more interest to overcome the gaps in recent schemes namely node capture, DoS attack, stolen verifier, denning-ssaco attack, GWN bypassing, unlinkability, key secrecy, and perfect forward. Finally, we provided some future research directions that may enhance the IoT authentication schemes. As a result, the wide deployment and scalability of the IoT networks.

Acknowledgement: Researchers would like to thank the Deanship of Scientific Research, Qassim University for funding publication of this project.

Funding Statement: The authors received no specific funding for this study.

Author Contributions: The authors confirm contribution to the paper as follows: Study conception and design: Mourade Azrour and Ahmad El Allaoui; data collection: Souhayla Dargaoui; analysis and interpretation of results: Azidine Guezzaz and Abdulatif Alabdulatif; draft manuscript preparation: Abdullah Alnajim. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The used data are available once the readers want by contacting mo.azrour@umi.ac.ma.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] M. U. Farooq, M. Waseem, S. Mazhar, A. Khairi, and T. Kamal, "A review on internet of things (IoT)," *Int. J. Comput. Appl.*, vol. 113, no. 1, pp. 1–7, 2015. doi: 10.5120/19787-1571.

[2] S. Dargaoui, M. Azrour, A. El Allaoui, A. Guezzaz, and S. Benkirane, "Authentication in internet of things: State of art," in *Proc. 6th Int. Conf. Netw. Intell. Sys. Secur.*, 2023, pp. 1–6.

[3] IUT-T, Présentation générale de l'Internet des objets, secteur de la normalisation des télécommunications de l'UIT, 06-2012, 2012. Accessed: Feb. 03, 2023. [Online]. Available: https://www.itu.int

[4] G. D. Elizabeth, "Architecting a connected future," ISO, 2019. 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, pp. 1821, 2021. doi: 10.3390/su13041821.

[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," *Sens.*, vol. 20, no. 9, pp. 2495, 2020. doi: 10.3390/s20092495.

[7] D. Kandris, C. Nakas, D. Vomvas, and G. Koulouras, "Applications of wireless sensor networks: An up-to-date survey," *Appl. Syst. Innov.*, vol. 3, no. 1, pp. 14, 2020. doi: 10.3390/asi3010014.

[8] A. M. Ghosh and K. Grolinger, "Edge-cloud computing for internet of things data analytics: Embedding intelligence in the edge with deep learning," *IEEE Trans. Ind. Inform.*, vol. 17, no. 3, pp. 2191–2200, 2020. doi: 10.1109/TII.2020.3008711.

[9] M. M. Sadeeq, N. M. Abdulkareem, S. R. Zeebaree, D. M. Ahmed, A. S. Sami and R. R. Zebari, "IoT and cloud computing issues, challenges and opportunities: A review," *Qubahan Acad. J.*, vol. 1, no. 2, pp. 1–7, 2021. doi: 10.48161/qaj.v1n2a36.

[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*, Cham: Springer International Publishing, 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," *Int. J. Cloud Comput.*, vol. 10, no. 5–6, pp. 633–644, 2021. doi: 10.1504/IJCC.2021.120399.

[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 J. Mabrouki, A. Mourade, A. Irshad, S. A. Chaudhry (Eds.), *Advanced Technology for Smart Environment and Energy*, Cham: Springer International Publishing, 2023, pp. 151–160. 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 Int. Conf. Smart Comput. (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. doi: 10.1109/ACCESS.2019.2942846.

[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 Intell. Syst.*, vol. 8, no. 5, pp. 3805–3815, 2022. doi: 10.1007/s40747-021-00582-9.

[17] M. Azrour, J. Mabrouki, A. Guezzaz, and A. Kanwal, "Internet of things security: Challenges and key issues," *Secur. Commun. Netw.*, vol. 2021, no. 3, pp. 1–11, 2021. doi: 10.1155/2021/5533843.

[18] M. Mohy-eddine, A. Guezzaz, S. Benkirane, and M. Azrour, "An effective intrusion detection approach based on ensemble learning for IIoT edge computing," *J. Comput. Virol. Hack. Tech.*, vol. 19, no. 4, pp. 1–13, 2022. doi: 10.1007/s11416-022-00456-9.

[19] M. Douiba, S. Benkirane, A. Guezzaz, and M. Azrour, "An improved anomaly detection model for IoT security using decision tree and gradient boosting," *J. Supercomput.*, vol. 79, pp. 1–20, 2022. doi: 10.1007/s11227-022-04783-y.

[20] C. Hazman, A. Guezzaz, S. Benkirane, and M. Azrour, "lIDS-SIoEL: Intrusion detection framework for IoT-based smart environments security using ensemble learning," *Clust. Comput.*, vol. 26, pp. 1–15, 2022. doi: 10.1007/s10586-022-03810-0.

[21] W. H. Hassan, "Current research on internet of things (IoT) security: A survey," *Comput. Netw.*, vol. 148, no. 5, pp. 283–294, 2019. doi: 10.1016/j.comnet.2018.11.025.

[22] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: A review," in *2012 Int. Conf. Comput. Sci. Electron. Eng.*, 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," *J. Netw. Comput. Appl.*, vol. 204, no. 4, pp. 103414, 2022. doi: 10.1016/j.jnca.2022.103414.

[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," *Sens.*, vol. 22, no. 4, pp. 1361, 2022. doi: 10.3390/s22041361.

[25] M. Saqib and A. H. Moon, "A systematic security assessment and review of internet of things in the context of authentication," *Comput. Secur.*, vol. 125, pp. 103053, 2022. doi: 10.1016/j.cose.2022.103053.

[26] A. N. Bahache, N. Chikouche, and F. Mezrag, "Authentication schemes for healthcare applications using wireless medical sensor networks: A survey," *SN Comput. Sci.*, vol. 3, no. 5, pp. 382, 2022. doi: 10.1007/s42979-022-01300-z.

[27] W. K. Ahmed and R. S. Mohammed, "Lightweight authentication methods in IoT: Survey," in *2022 Int. Conf. Comput. Sci. Softw. Eng. (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," *Meas. Sens.*, vol. 25, pp. 100591, 2022. doi: 10.1016/j.measen.2022.100591.

[29] A. H. Mohsin *et al.*, "Blockchain authentication of network applications: Taxonomy, classification, capabilities, open challenges, motivations, recommendations and future directions," *Comput. Stand. Interfaces*, vol. 64, pp. 41–60, 2019. doi: 10.1016/j.csi.2018.12.002.

[30] A. H. Sodhro, A. I. Awad, J. van de Beek, and G. Nikolakopoulos, "Intelligent authentication of 5G healthcare devices: A survey," *Internet Things*, vol. 20, no. 4, pp. 100610, 2022. doi: 10.1016/j.iot.2022.100610.

[31] J. R. Jiang, "Short survey on physical layer authentication by machine-learning for 5G-based internet of things," in *2020 3rd IEEE Int. Conf. Knowl. Innov. Invent. (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. doi: 10.1109/ACCESS.2020.3047895.

[33] M. A. Ferrag, L. Maglaras, and A. Derhab, "Authentication and authorization for mobile IoT devices using biofeatures: Recent advances and future trends," *Secur. Commun. Netw.*, vol. 2019, no. 1, pp. 1–20, 2019. doi: 10.1155/2019/5452870.

[34] W. Yang, S. Wang, N. M. Sahri, N. M. Karie, M. Ahmed and C. Valli, "Biometrics for internet-of-things security: A review," *Sens.*, vol. 21, no. 18, pp. 6163, 2021. doi: 10.3390/s21186163.

[35] M. El-Hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, "A survey of internet of things (IoT) authentication schemes," *Sens.*, vol. 19, no. 5, pp. 1141, 2019. doi: 10.3390/s19051141.

[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," *Comput. Netw.*, vol. 217, no. 4, pp. 109335, 2022. doi: 10.1016/j.comnet.2022.109335.

[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 Symp. Comput. Commun. (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 Int. Conf. Consum. Electron. (ICCE)*, IEEE, 2022, pp. 1–4.

[39] X. Jia *et al.*, "IRBA: An identity-based cross-domain authentication scheme for the internet of things," *Electron.*, vol. 9, no. 4, pp. 634, 2020. doi: 10.3390/electronics9040634.

[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," *Sustain. Cities Soc.*, vol. 41, no. 4, pp. 878–885, 2018. doi: 10.1016/j.scs.2018.06.004.

[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 Annu. Conf. IEEE Ind. Electron. Soc.*, 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," *Digit. Commun. Netw.*, vol. 25, no. 2, pp. 514, 2022. doi: 10.1016/j.dcan.2022.10.006.

[43] A. E. M. Eljialy, M. Y. Uddin, and S. Ahmad, "Novel framework for an intrusion detection system using multiple feature selection methods based on deep learning," *Tsinghua Sci. Technol.*, vol. 29, no. 4, pp. 948–958, 2024. doi: 10.26599/TST.2023.9010032.

[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 Things J.*, vol. 7, no. 9, pp. 9128–9143, 2020. doi: 10.1109/JIOT.2020.3004077.

[45] V. Kumar and S. Ray, "Continuous behavioral authentication system for IoT enabled applications," in *Int. Conf. Netw. Secur. Blockchain Technol.*, 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 Recognit. Lett.*, vol. 144, no. 5, pp. 35–41, 2021. doi: 10.1016/j.patrec.2021.01.019.

[47] S. Duraibi, "Voice biometric identity authentication model for IoT devices," *Int. J. Secur. Priv. Trust Manag. (IJSPTM)*, vol. 9, no. 2, pp. 1–10, 2020. doi: 10.5121/ijsptm.2020.9201.

[48] N. Ghosh, S. Chandra, V. Sachidananda, and Y. Elovici, "SoftAuthZ: A context-aware, behavior-based authorization framework for home IoT," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10773–10785, 2019. doi: 10.1109/JIOT.2019.2941767.

[49] D. Li, W. Peng, W. Deng, and F. Gai, "A blockchain-based authentication and security mechanism for IoT," in *2018 27th Int. Conf. Comput. Commun. Netw. (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," *Clust. Comput.*, vol. 23, no. 3, pp. 2067–2087, 2020. doi: 10.1007/s10586-020-03058-6.

[51] S. Guo, X. Hu, S. Guo, X. Qiu, and F. Qi, "Blockchain meets edge computing: A distributed and trusted authentication system," *IEEE Trans. Ind. Inform.*, vol. 16, no. 3, pp. 1972–1983, 2019. doi: 10.1109/TII.2019.2938001.

[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. doi: 10.1109/ACCESS.2020.3011137.

[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 Conf. (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 J. Biomed. Health Inform.*, vol. 24, no. 8, pp. 2146–2156, 2020. doi: 10.1109/JBHI.2020.2969648.

[55] D. Díaz-Sánchez, A. Marín-Lopez, F. A. Mendoza, and P. A. Cabarcos, "DNS/DANE collision-based distributed and dynamic authentication for microservices in IoT," *Sens.*, vol. 19, no. 15, pp. 3292, 2019. doi: 10.3390/s19153292.

[56] P. Sudhakaran, "Energy efficient distributed lightweight authentication and encryption technique for IoT security," *Int. J. Commun. Syst.*, vol. 35, no. 2, pp. e4198, 2022. doi: 10.1002/dac.4198.

[57] G. Pathak, J. Gutierrez, A. Ghobakhlou, and S. U. Rehman, "LPWAN key exchange: A centralised lightweight approach," *Sens.*, vol. 22, no. 13, pp. 5065, 2022. doi: 10.3390/s22135065.

[58] U. Verma and D. Bhardwaj, "CMAKM-FIoT: Centralised mutual authentication and key management scheme for fog computing-enabled IoT network," *Int. J. Electron. Bus.*, vol. 17, no. 4, pp. 407–427, 2022. doi: 10.1504/IJEB.2022.126265.

[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," *Int. J. Distrib. Sens. Netw.*, vol. 18, no. 6, pp. 15501329221104332, 2022. doi: 10.1177/15501329221104332.

[60] S. Farooq and P. Chawla, "A novel approach of mutual authentication in fog computing," in *Proc. 1st Int. Conf. Comput. Electron. Wireless Commun.*, 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," *J. Inf. Secur. Appl.*, vol. 68, no. 4, pp. 103259, 2022. doi: 10.1016/j.jisa.2022.103259.

[62] A. B. Amor, S. Jebri, M. Abid, and A. Meddeb, "A secure lightweight mutual authentication scheme in social industrial IoT environment," *The Journal of Supercomputing*, vol. 79, no. 12, pp. 13578–13600, 2022.

[63] I. Alshawish and A. Al-Haj, "An efficient mutual authentication scheme for IoT systems," *J. Supercomput.*, vol. 78, no. 14, pp. 1–32, 2022. doi: 10.1007/s11227-022-04520-5.

[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," *Concurr. Comput. Pract. Exp.*, vol. 35, no. 1, pp. e7428, 2023. doi: 10.1002/cpe.7428.

[65] H. Park, M. Kim, and J. Seo, "IoT multi-phase authentication system using token based blockchain," *KIPS Trans. Comput. Commun. Syst.*, 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," *Ilk Online*, vol. 20, no. 4, pp. 2401–2406, 2021. doi: 10.17051/ilkonline.2021.04.275.

[67] B. B. Rao and A. A. Waoo, "Advanced system to identify users and devices in IoT using token-based authentication," *Int. J. Innov. Sci. Res. Technol.*, vol. 6, no. 10, pp. 996–999, 2021.

[68] L. Sasirega, and C. Shanthi, "Lightweight ECC and token based authentication mechanism for WSN-IoT," *Sci. Tech. J. Inf. Technol. Mech. Opt.*, vol. 22, no. 2, pp. 332–338, 2022. doi: 10.17586/2226-1494-2022-22-2-332-338.

[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 Trans. Ind. Inform.*, vol. 18, no. 10, pp. 7118–7127, 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," *Web.*, vol. 18, no. 2, pp. 199–211, 2021. doi: 10.14704/WEB/V18I2/WEB18316.

[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," *Innov. Technol. Sci. Solut. Ind.*, vol. 4, no. 18, pp. 31–39, 2021. doi: 10.30837/ITSSI.2021.18.031.

[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. doi: 10.1109/ACCESS.2021.3103889.

[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 Things J.*, vol. 9, no. 11, pp. 8205–8228, 2022. doi: 10.1109/JIOT.2022.3142084.

[74] A. Braeken, "PUF-based authentication and key exchange for internet of things," *IoT Secur. Adv. Authentication*, pp. 185–204, 2020. doi: 10.1002/9781119527978.ch10.

[75] K. Lounis and M. Zulkernine, "Lessons learned: Analysis of PUF-based authentication protocols for IoT," *Digit. Threats Res. Pract.*, vol. 4, no. 2, pp. 1–33, 2021. doi: 10.1145/3487060.

[76] A. Shamsoshoara, A. Korenda, F. Afghah, and S. Zeadally, "A survey on physical unclonable function (PUF)-based security solutions for internet of things," *Comput. Netw.*, vol. 183, no. 1, pp. 107593, 2020. doi: 10.1016/j.comnet.2020.107593.

[77] C. Wang, D. Wang, G. Xu, and D. He, "Efficient privacy-preserving user authentication scheme with forward secrecy for Industry 4. 0," *Sci. China Inf. Sci.*, vol. 65, no. 1, pp. 1–15, 2022. doi: 10.1007/s11432-020-2975-6.

[78] M. Mumtaz, J. Akram, and L. Ping, "An RSA based authentication system for smart IoT environment," in *2019 IEEE 21st Int. Conf. High Perform. Comput. Commun.; IEEE 17th Int. Conf. Smart City; IEEE 5th Int. Conf. Data Sci. Sys. (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," *Appl. Sci.*, vol. 10, no. 6, pp. 1962, 2020. doi: 10.3390/app10061962.

[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," *Comput. Mater. Contin.*, vol. 67, no. 3, pp. 3349–3361, 2021. doi: 10.32604/cmc.2021.012454.

[81] A. Tewari and B. B. Gupta, "A novel ECC-based lightweight authentication protocol for internet of things devices," *Int. J. High Perform. Comput. Netw.*, vol. 15, no. 1–2, pp. 106–120, 2019. doi: 10.1504/IJHPCN.2019.103548.

[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. doi: 10.1109/ACCESS.2020.2980739.

[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 Syst. J.*, vol. 15, no. 3, pp. 4431–4438, 2021. doi: 10.1109/JSYST.2021.3057047.

[84] A. Lohachab, "ECC based inter-device authentication and authorization scheme using MQTT for IoT networks," *J. Inf. Secur. Appl.*, vol. 46, no. 2, pp. 1–12, 2019. doi: 10.1016/j.jisa.2019.02.005.

[85] S. Rostampour, M. Safkhani, Y. Bendavid, and N. Bagheri, "ECCbAP: A secure ECC-based authentication protocol for IoT edge devices," *Pervasive Mob. Comput.*, vol. 67, no. 2018, pp. 101194, 2020. doi: 10.1016/j.pmcj.2020.101194.

[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. doi: 10.1109/ACCESS.2021.3112554.

[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. doi: 10.1109/ACCESS.2019.2912998.

[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. doi: 10.1109/ACCESS.2020.3034447.

[89] P. K. Dhillon and S. Kalra, "Secure and efficient ECC based SIP authentication scheme for VoIP communications in internet of things," *Multimed. Tools Appl.*, vol. 78, no. 16, pp. 22199–22222, 2019. doi: 10.1007/s11042-019-7466-y.

[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, pp. e0234631, 2020. doi: 10.1371/journal.pone.0234631.

[91] B. Hu, W. Tang, and Q. Xie, "A two-factor security authentication scheme for wireless sensor networks in IoT environments," *Neurocomputing*, vol. 500, pp. 741–749, 2022.

[92] M. Azrour, J. Mabrouki, A. Guezzaz, and Y. Farhaoui, "New enhanced authentication protocol for internet of things," *Big Data Min. Anal.*, vol. 4, no. 1, pp. 1–9, 2021. doi: 10.26599/BDMA.2020.9020010.

[93] D. Kumar, S. Chand, and B. Kumar, "Cryptanalysis and improvement of a user authentication scheme for wireless sensor networks using chaotic maps," *IET Netw.*, vol. 9, no. 6, pp. 315–325, 2020. doi: 10.1049/iet-net.2019.0009.

[94] D. Kaur, D. Kumar, K. K. Saini, and H. S. Grover, "An improved user authentication protocol for wireless sensor networks," *Trans. Emerg. Telecommun. Technol.*, vol. 30, no. 10, pp. e3745, 2019. doi: 10.1002/ett.3745.

[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," *Sens.*, vol. 21, no. 4, pp. 1488, 2021. doi: 10.3390/s21041488.

[96] P. K. Panda and S. Chattopadhyay, "A secure mutual authentication protocol for IoT environment," *J. Reliab. Intell. Environ.*, vol. 6, no. 2, pp. 79–94, 2020. doi: 10.1007/s40860-020-00098-y.

[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 Annu. Consum Commun. Network. Conf. (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," *Secur. Commun. Netw.*, vol. 2021, pp. 1–12, 2021. doi: 10.1155/2021/4799223.

[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," *Comput. Mater. Contin.*, vol. 58, no. 2, pp. 545–565, 2019. doi: 10.1016/j.jksuci.2021.07.023.

[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, no. 2, pp. 1877–1898, 2021.

[101] V. O. Nyangaresi, "Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography," *J. Syst. Archit.*, vol. 133, no. 2, pp. 102763, 2022. doi: 10.1016/j.sysarc.2022.102763.

[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 Netw.*, vol. 138, no. 10, pp. 102997, 2023. doi: 10.1016/j.adhoc.2022.102997.

[103] S. Yu and K. Park, "ISG-SLAS: Secure and lightweight authentication and key agreement scheme for industrial smart grid using fuzzy extractor," *J. Syst. Archit.*, vol. 131, pp. 102698, 2022. doi: 10.1016/j.sysarc.2022.102698.

[104] R. Krishnasrija, A. K. Mandal, and A. Cortesi, "A lightweight mutual and transitive authentication mechanism for IoT network," *Ad Hoc Netw.*, vol. 138, no. 2, pp. 103003, 2023. doi: 10.1016/j.adhoc.2022.103003.

[105] J. Lee *et al.*, "PUFTAP-IoT: PUF-based three-factor authentication protocol in IoT environment focused on sensing devices," *Sens.*, vol. 22, no. 18, pp. 7075, 2022. doi: 10.3390/s22187075.

[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, pp. 2394, 2022. doi: 10.3390/sym14112394.

[107] A. K. Yadav, M. Misra, P. K. Pandey, and M. Liyanage, "An EAP-based mutual authentication protocol for WLAN connected IoT devices," *IEEE Trans. Ind. Inform.*, vol. 19, no. 2, pp. 1343–1355, 2022. doi: 10.1109/TII.2022.3194956.

[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," *Comput. Commun.*, vol. 195, no. 4, pp. 27–39, 2022. doi: 10.1016/j.comcom.2022.08.003.

[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," *Digit. Commun. Netw.*, vol. 9, no. 5, pp. 1080–1089, 2022. doi: 10.1016/j.dcan.2022.04.009.

[110] S. K. Dwivedi, R. Amin, and S. Vollala, "Design of secured blockchain based decentralized authentication protocol for sensor networks with auditing and accountability," *Comput. Commun.*, vol. 197, no. 1, pp. 124–140, 2023. doi: 10.1016/j.comcom.2022.10.016.

[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 Things J.*, vol. 9, no. 21, pp. 21493–21504, 2022. doi: 10.1109/JIOT.2022.3184293.

[112] R. Kumar, S. Singh, and P. K. Singh, "A secure and efficient computation based multi-factor authentication scheme for Intelligent IoT-enabled WSNs," *Comput. Electr. Eng.*, vol. 105, no. 3, pp. 108495, 2023. doi: 10.1016/j.compeleceng.2022.108495.

[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," *Microprocess. Microsyst.*, vol. 96, pp. 104722, 2023. doi: 10.1016/j.micpro.2022.104722.

[114] J. Pirayesh, A. Giaretta, M. Conti, and P. Keshavarzi, "A PLS-HECC-based device authentication and key agreement scheme for smart home networks," *Comput. Netw.*, vol. 216, no. 1, pp. 109077, 2022. doi: 10.1016/j.comnet.2022.109077.

[115] R. Hajian, A. Haghighat, and S. H. Erfani, "A secure anonymous D2D mutual authentication and key agreement protocol for IoT," *Internet Things*, vol. 18, no. 3, pp. 100493, 2022. doi: 10.1016/j.iot.2021.100493.

[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," *Digit. Commun. Netw.*, vol. 9, no. 2, pp. 358–366, 2022. doi: 10.1016/j.dcan.2022.11.001.

[117] Y. Guo, Z. Zhang, and Y. Guo, "SecFHome: Secure remote authentication in fog-enabled smart home environment," *Comput. Netw.*, vol. 207, no. 6, pp. 108818, 2022. doi: 10.1016/j.comnet.2022.108818.

[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 Eng.*, vol. 250, no. 1, pp. 110894, 2022. doi: 10.1016/j.oceaneng.2022.110894.

[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," in *GLOBECOM 2022–2022 IEEE Glob. Commun. Conf.*, Dec. 2022, pp. 516–521. doi: 10.1109/GLOBECOM48099.2022.10001345.

[120] M. Azrour, J. Mabrouki, and R. Chaganti, "New efficient and secured authentication protocol for remote healthcare systems in cloud-IoT," *Secur. Commun. Netw.*, vol. 2021, no. 4, pp. 1–12, 2021. doi: 10.1155/2021/5546334.

[121] M. S. Almadani, S. Alotaibi, H. Alsobhi, O. K. Hussain, and F. K. Hussain, "Blockchain-based multi-factor authentication: A systematic literature review," *Internet Things*, vol. 23, no. 2, pp. 100844, 2023. doi: 10.1016/j.iot.2023.100844.

[122] A. Kumar, C. Ottaviani, S. S. Gill, and R. Buyya, "Securing the future internet of things with post-quantum cryptography," *Secur. Priv.*, vol. 5, no. 2, pp. e200, 2022. doi: 10.1002/spy2.200.

[123] I. Cvitić, D. Peraković, M. Periša, and B. Gupta, "Ensemble machine learning approach for classification of IoT devices in smart home," *Int. J. Mach. Learn. Cybern.*, vol. 12, no. 11, pp. 3179–3202, 2021. doi: 10.1007/s13042-020-01241-0.

[124] S. Khanam, S. Tanweer, and S. S. Khalid, "Future of internet of things: Enhancing cloud-based IoT using artificial intelligence," *Int. J. Cloud Appl. Comput. (IJCAC)*, vol. 12, no. 1, pp. 1–23, 2022. doi: 10.4018/IJCAC.