applied sciences

Review

Key Agreement and Authentication Protocols in the Internet of Things: A Survey

Sabina Szymoniak [1,*] and Shalini Kesar [2]

[1] Department of Computer Science, Częstochowa University of Technology, 42-200 Częstochowa, Poland
[2] Department of Computer Science & Information Systems, Southern Utah University, Cedar City, UT 84720, USA
* Correspondence: sabina.szymoniak@icis.pcz.pl

Abstract: The rapid development of Internet of things (IoT) technology has made the IoT applicable in many areas of life and has contributed to the IoT's improvement. IoT devices are equipped with various sensors that enable them to perform the tasks they were designed for. The use of such devices is associated with securing communication between devices and users. The key stages of communication are the processes of authentication and the process of agreeing on session keys because they are the basis of the subsequent communication phases. The specially designed security protocols are used to secure communication. These protocols define the course of communication and cryptographic techniques employed for securing. In this article, we have reviewed the latest communication protocols designed to secure authentication processes and agree on session keys in IoT environments. We analyzed the proposed protocols' security level, vulnerability, and computational and communication costs. We showed our observations, describing the requirements that a secure protocol should meet.

Keywords: Internet of things; security; security protocols

check for updates

Citation: Szymoniak, S.; Kesar, S. Key Agreement and Authentication Protocols in the Internet of Things: A Survey. *Appl. Sci.* **2023**, *13*, 404. https://doi.org/10.3390/app13010404

Academic Editors: Weidong Fang and Chunsheng Zhu

Received: 29 November 2022
Revised: 20 December 2022
Accepted: 25 December 2022
Published: 28 December 2022

1. Introduction

The rapid development of Internet of Things (IoT) technology has made the IoT applicable in many areas of life and contributed to its improvement [1]. We can find IoT devices in everyday life because we use intelligent washing machines, TV sets, and light bulbs. In combination with appropriate sensors, these devices intelligently control the lighting or water heating in a building. They can also protect our security with tracking devices [2–5]. In medical IoT, devices help to control the vital functions of chronically ill people, test blood glucose levels in people with diabetes, signal the patient's need for medications, and deliver them to the patient on time [6–8]. One of the typical applications of IoT in the industry to alert people about the possibility of an earthquake [9]. Athletes can also use IoT to control vital functions and performance to prevent life-threatening situations [10–12].

IoT devices are equipped with various sensors (for example, temperature, pressure, and velocity sensors) that enable them to perform the tasks for which they were designed. Sensors process signals from their work environment and then react to them appropriately. For example, if the room temperature is too high, the heating devices will be switched off to lower the temperature. IoT devices can also communicate with each other to convey relevant information [13–15]. Usually, the connected sensors form wireless sensor networks (WSNs), within which various operations and data exchanges are performed. Both networks, IoT and WSN, primarily use the standards IEEE 802.15.4 [16], NFC [17], 6LoWPAN [18], MQTT [19], and Bluetooth Low Energy [20] for communication.

Communication between IoT devices requires the use of various protocols that will define the purpose of the communication, the sequence of steps performed during it, and cryptographic techniques used to secure the transmitted information. The protocol's purpose may be to support communication between devices, but the protocol may also target aspects of communication security. Here, the protocol's goals can be the mutual authentication of the parties as well as the agreement of the session key. Usually, these protocols are described as security protocols. Securing communication is a necessary activity due to the possibility of various cyberattacks. Attacking users can try to intercept and modify transmitted messages, as well as steal confidential information [21–26]. In addition, the implementation of protocols in networks of interconnected IoT devices must take into account technical aspects such as the purpose of the network, the energy demand of the devices and the type of communication that will be carried out in it [27].

In the case of security protocols, it is essential to verify their correct operation, check whether they provide an appropriate level of security and whether they are not vulnerable to the latest methods of attacks. When verifying security protocols, we can use methods such as time automatics [28,29], BAN logic [30], GNY logic [31], real-or-random (ROR) [32], random Oracle model (ROM) [33], or Syverson-Van Oorschot (SVO) logic [34]. In addition, protocol verification is possible with such tools as Scyther [35,36], Tamarin [37,38], ProVerif [39–41], Avispa [42], or the tools mentioned in [22,43], or [44].

1.1. Motivations and Contributions

Technology surrounds us from almost every side. We use various intelligent devices that, above all, make our lives easier but also transfer large amounts of data. Often, the sent messages contain sensitive data related to users' devices. Thus, the need to secure data is an essential aspect of the operation of intelligent systems. Users require that the use of technological facilities is safe for them, both in protecting human health and life, as well as in data processing.

As a rule, the communication process consists of several stages. Specially designed protocols are used to secure each of these steps. These, in turn, are exposed to malicious users who look for security vulnerabilities to intercept and then use the data. The user authentication and key agreement stages deserve special attention here, as the security of subsequent communication phases depends on their safe course. We are aware that technological progress also entails the development of attack techniques. Therefore it is necessary to regularly review the level of security implemented by the protocols securing individual stages of communication. Properly selected and safe protocols will certainly increase IoT devices' security level. So, in this arithmetic, we provide an overview of how to secure the authentication processes and the reconciliation and agreement of keys using security protocols in WSNs.

We believe that studying the work of protocols that secure the authentication process and session key agreement in IoT can help readers understand the state of art in both theory and practice. We will explain what security problems and threats are exposed to IoT devices operating in such networks. In addition, we will discuss the security levels offered by the protocols used in IoT or WSNs. We will also highlight the challenges and requirements for the newly designed protocols.

1.2. Methodology

We collected articles that use various search engines (mainly Google Scholar and DBLP) during our research. Moreover, we analyzed references from found articles and citations to these papers. Our goal was to compose the most complete and up-to-date review of the security of authentication and session key agreement protocols operating in IoT systems.

1.3. Organization

The rest of this paper is organized as follows. Section 2 presents the characteristics of the IoT and WSNs. Next, we will discuss cryptographic techniques used in cryptographic protocols, the security requirements, and problems. Moreover, we will discuss typical cyberattacks in IoT systems. In Section 3, we provide an overview of the protocols used in IoT systems for the authentication process and session key agreement and distribution. In Section 4, we will summarize and conclude our analysis of the discussed protocols. We will focus on the security and technical aspects of these protocols. In addition, we will include our insights and research directions for the future. In the last section, we will present the conclusions of the entire article, findings from the research, and our plans for the future.

2. Materials and Methods

In this section, we will present theoretical aspects of the operation of the IoT and WSNs. We will discuss the types and classes of threats that await connected devices and their users. In addition, we will highlight the importance of using protocols that secure the authentication process and key agreement in IoT systems and WSNs.

2.1. Internet of Things and Wireless Sensor Networks

The Internet of things is a technology in which connected smart objects can directly or indirectly collect, process or exchange data via a computer network. Devices can communicate automatically and without human intervention by using the available network connections. The IoT concept is used in many aspects of human life (industry, city management, medicine, household, mobility). Depending on the application, the IoT can be divided into subcategories, such as the industrial IoT or medical IoT. Among IoT devices, we can indicate sports bands that can measure one's heart rate on an ongoing basis, count steps taken, or monitor sleep. Other intelligent devices are voice assistants, thanks to which, by using voice commands, we can receive the necessary information and control other devices connected to the network, such as smart bulbs, refrigerators, TVs, or ovens [2,3,45–48]. We put together IoT solutions and typical cyberattacks on IoT systems in Figure 1.

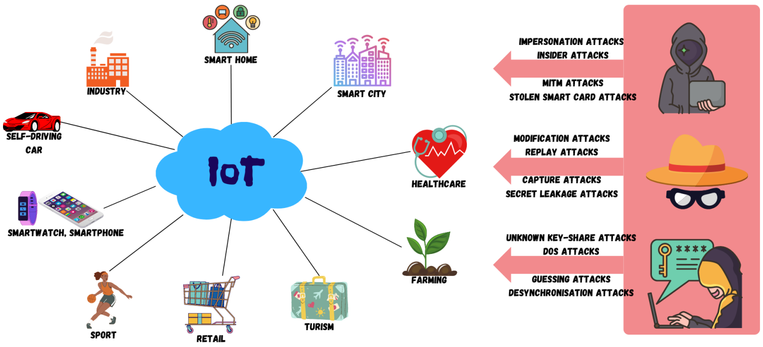

Figure 1. IoT solutions and typical cyberattacks on IoT systems.

IoT devices are often equipped with various types of sensors that detect and react to characteristic properties of the environment, such as speed, temperature, and altitude. Sensors can also collect and exchange data with other sensors, devices, end users, servers, or clouds. Hence, IoT networks often implement wireless sensor network (WSN) technology to collect and transmit data. WSNs are characterized by mobility, reliability, node heterogeneity, real-time data transmission, and reaction to sensor failures. WSN networks are also used to monitor a specific environment and react to changes occurring in it [45,46,49–51].

2.2. Cryptographic Methods

Cryptography is the science of creating the algorithms and protocols necessary to protect information. Information protection is related to such concepts as data encryption, electronic communication privacy protection, authentication, or key agreement [52–55]. The most characteristic process related to cryptography is the encryption process. It consists of transforming information from plaintext into a form that will be incomprehensible to outsiders.

Encryption is the process of transforming (encrypting) information (plaintext) into a form that is incomprehensible to outsiders. An encrypted message is called a ciphertext. The reverse of encryption is the decryption process, which recovers the original message, or plaintext, from the ciphertext. The security of cryptographic algorithms is often achieved by using an additional secret parameter known as a cryptographic key. Their use ensures that even if the intruder knows the algorithm used to encrypt the message, he will not be able to decrypt it unless he has the key. Thus, the ciphertext is safe as long as the secret key used in communication is [52–54,56,57].

Key encryption algorithms can be divided into symmetric and asymmetric [16]. In symmetric algorithms, also called secret-key algorithms, it is possible to obtain a decryption key from an encryption key. There are also situations in which the keys are identical. In the case of symmetric algorithms, a secret key must be agreed upon between the communicating parties before commencing communication using a secure method. This is related to the problem of key agreement. To have a safe, symmetrically encrypted feed, we need a secure communication channel to forward the key [54,58,59].

On the other hand, asymmetric algorithms use key pairs assigned to users. Such a pair are the public and private keys. Diffie and Hellman presented the concept of a public key in [60]. The public key is known to all users, and anyone possessing it can encrypt their messages. However, the ciphertexts obtained this way can only be deciphered with the corresponding private key. The user must be sure that his public key corresponds to his private key. Thus, the public key encrypts, and the private key decodes the message. However, there is a situation in which the roles of the keys are reversed. If the message is encrypted with the private key, the resulting ciphertext becomes the so-called electronic signature, i.e., protection against unauthorized modification. Decryption is then possible by using the public key [54,58,59].

When the data to be signed is large, it takes a long time to sign. Hash functions or hashes are used in these situations, and their operation is based on appropriately processing extensive data to a smaller size. Hash functions are primarily used to check and confirm the authenticity of data, ensuring that the data has not been tampered with in an unauthorized manner. The mentioned functions are unidirectional, so it is impossible to reconstruct the data based on the hash itself. This means that the whole message that has been signed [61,62] must be sent with the electronic signature.

2.3. Cyberattacks on IoT Systems

Communication in IoT environments is exposed to various attacks. The attacks' results also can be multiple, and everything depends on the attacker's knowledge, intentions, and imagination. For example, the attacks' effects may be data loss, interception, or modification. We can indicate many kinds of attacks in IoT. We summarised common attacks in IoT in Table 1.

Table 1. Typical attacks in IoT.

Attack	Description	References
Replay attack	The attacker intercepts traffic and sends correspondence to its original target, duplicate packets can be sent many times to the recipients.	[63,64]
Spoofing attack	The attacker tries to hide the communication or identity so that it appears to be associated with a trusted, authorized source.	[65]
Stolen (smart card, verifier) attack	The attacker can guess or steals the password; for example, when the smart card is lost, also he can use the stolen verifier directly to impersonate the authorized participant of the communication.	[66]
Man in the Middle attack (MITM)	The attacker disrupts communication between two nodes by injecting a malicious node between legitimate nodes.	[64,67]
Impersonation attack	The attacker uses the identity of another user (user, server, gateway, node, IoT device).	[68–70]
(Privileged)-insider attack.	The attacker, or insider, is authorized to access the system, then the insider can use his access to the data breach.	[64]
Known session-specific temporary information (KSSTI) attack	The attacker can calculate the session key based on temporary information.	[71]
(Offline password) guessing attack	The attacker tries iteratively to guess a password or other login details to impersonate the user.	[72]
Denial of Service (DoS) attack	The attacker floods the network with signals, which results in network closure.	[64,67,73]
Sinkhole attack	The attacker announces updates of routing information, thus attracting network traffic, and as a consequence, it may launch further attacks.	[64,67]
Desynchronisation attack	The attacker tries to destroy synchronization between the nodes.	[74]
(Sensor node, IoT device) capture attack, cloning attack	The attacker hijacks a sensor node or IoT device to take over the network, remove the node from the network, and redeploys it as a malicious node.	[64,75,76]
key compromise impersonation (KCI) attack	The attacker installs the client's certificate on the device and can then impersonate it.	[77]

An essential aspect of security that must be considered in IoT systems is the implementation of the CIA triad (confidentiality, integrity, availability). This is a model aimed at the steering of security policy. Confidentiality protects us from unauthorized attempts to access confidential information. Integrity ensures data consistency, accuracy, and reliability. Availability ensures that access to data will be easy for authorized parties [78]. The security protocols are one of the methods that implement mentioned rules. The protocols are short programs that describe the communications course and rules. They can secure communication and ensure security aspects like mutual authentication, user anonymity, perfect forward or backward secrecy, or untraceability [26,79].

The security protocols play a significant security function during the users' communication. They define a sequence of steps during which users execute activities like authentication, authorization, key agreement, and exchange. We can highlight that security protocols ensure secure authentication and authorization processes so that they can prevent unauthorized access by dishonest users. Moreover, they support key agreement and exchange processes, so the users should be sure that a secure channel provides their communication. Unfortunately, many protocols can be broken because they do not provide adequate security. Users' information can be stolen and used by attackers. The following section will overview existing security protocols for the IoT or WSNs. We will focus on protocols for authentication and agreement of the session key. In addition, we will discuss the security levels offered by these protocols.

3. Security Protocols for the Internet of Things

Communication in various IoT environments usually consists of several stages using specially designed security protocols. The stages of authentication and agreement of the session key are the most characteristic stages of communication. During authentication, the user or device confirms their identity. As a result of correct authentication, the user or device acquires certain rights and privileges depending on the system. Various mechanisms are used in authentication protocols to ensure an appropriate level of security (for example, using methods described in Section 2.2). An essential element of authentication protocols is the number of factors used in the authentication process. It is worth indicating three groups of factors that are used during the authentication process:

- Knowledge factor relates to something the user knows, e.g., username and password;
- Ownership factor refers to something the user has, e.g., a smart card or security token; and
- Inheritance factor refers to the user's biometric characteristics, i.e., something the user can be identified by, such as a fingerprint or an iris pattern.

An equally important stage of communication is distributing the session key. The keys are used to encrypt and decrypt messages. There are many different approaches to the problem of session key agreement. We can define a separate protocol for these purposes and extract a fragment of the authentication protocol that will be responsible for the agreement of the session key (e.g., [80]).

As mentioned earlier, the most desirable features of security protocols are connected with the implementation of the CIA triad (confidentiality, integrity, availability). Data confidentiality is critical in IoT environments. Any situation that threatens the security of such environments can contribute to the threat to users' privacy and their data. Data can be stolen and misused. Data confidentiality is essential in any situation, but it becomes crucial when communication concerns patients' health data. An excellent solution to secure data and thus ensure data confidentiality is the use of elliptic curve algorithms, which use the mathematics of elliptic curves. Usually, these algorithms are considered in the case of the Rivest–Shamir–Adleman algorithm as an alternative cryptographic method. Elliptic curve algorithms use a smaller key size than the Rivest–Shamir–Adleman algorithm.

The second security feature is data integrity, ensuring data consistency, accuracy, and reliability. Here, the characteristic technology has become blockchain technology. Blockchain can be defined as a register of decentralized data that is securely shared between users. The data is divided into shared blocks, linked to unique identifiers in the form of cryptographic hashes. The use of blockchain technology enables accessible collection, integration, and sharing of data.

The last security feature is availability, ensuring that access to data will be easy for authorized parties. We can use biometric techniques and physical unclonable functions to support data availability. Physical unclonable functions use randomness to give an object a unique "fingerprint". Thanks to this, only users or devices with defined permissions will gain access to data.

Below in this Section, we will present a comprehensive review of the latest authentication protocols, including authentication protocols with key agreement phases for IoT solutions. We will deliver them, dividing them according to their use (medicine and healthcare, edge, industry, vehicles, drones, and general IoT solutions). This review will support the summary of the characteristics and features of the protocols that occurred in the IoT or WSN environments.

Rasslan et al. in [81] have proposed identity-based strong designated verifier signature authentication protocols for medical IoT solutions. The proposed protocols can support the authentication process of the IoT device network, which consists of both typical devices designed to control the vital functions of patients and autonomous vehicles and drones. A characteristic feature of both solutions is their short signature size. Moreover, the authors showed that both schemes are characterized by low communication and computing costs compared to similar solutions. The authors confirmed that the proposed protocols meet the assumptions of the ROM and protect patient privacy, and ensure data integrity and authenticity.

Masud et al. in [82] have proposed an authentication protocol for medical IoT solutions. The proposed protocol is based on blockchain [83] and fog calculations, Ethereum-powered smart contracts [84], PUF, and biometrics. Blockchain and fog technology ensure nonrepudiation, transparency, low latency, and efficient bandwidth use. Other technologies are used to prevent replay, spoofing, and cloning attacks. The authors checked and confirmed the protocol's security by using the Scyther tool. Moreover, they compared their protocol with similar computation costs and performance solutions. The authors showed that the proposed protocol could be successfully used in healthcare networks that use devices with limited resources.

Chander et al. in [85] also addressed medical safety issues. The authors focused on solutions for telecare medicine information systems [86]. They proposed an authentication protocol that uses hash functions, random functions, radio frequency identification (RFID) technology [87], and bitwise logical operations [88]. They checked the correctness and security of the proposed protocol with the help of BAN and GNY logics and Avispa and Scyther tools. These studies have shown that the protocol is resistant to typical attacks occurring in IoT networks and meets the most crucial security properties. However, Soni et al. in [89] have reexamined the protocol apportioned by Chander et al. in [85]. The authors showed that despite the use of hashing functions that reduce computing costs of endpoint devices, storage and communication costs are higher.

Consequently, there may be delays in the transmission of medical data. Moreover, they have shown that this protocol is susceptible to impersonation, insider, stolen smart card, MITM, and modification attacks. Furthermore, the protocol does not include the possibility of changing the password, which significantly affects the security of data transmission.

Wang et al. in [90] proposed a protocol for medical IoT that protects patient data from illegal access by unauthorized servers. The authors created an encryption method for this protocol based on cyclic shift and XOR operation. Thanks to it, the protocol maintains the safety of users but does not burden devices. The authors demonstrated the security of the proposed protocol by using the BAN logic. Moreover, they have shown that the protocol is resistant to typical attacks in IoT environments. The authors also compared their protocol with similar solutions and obtained satisfactory results in achieving safety attributes and energy consumption during communication and calculations.

Prasanalakshmi et al. in [91] focused on IoT solutions in the healthcare field. The authors designed a protocol by using the AES [92] and blowfish [93] algorithms to encrypt medical data, the Koblitz method to choose the embedding points [94] curve, and hyperelliptic curve [95] for embedding medical data in a medical image. The embedded image prepared in this way is then compressed with a five-level discrete wavelet transform file to achieve a reasonable payload. The authors confirmed the proposed method's correctness, especially in medical image processing. Moreover, they suggested that the protocol could be used in real-time applications.

Chen et al. in [96] introduced the LAP-IoHT protocol, a three-factor authentication protocol designed for health-related IoT solutions. Authentication is based on using the smart card, passwords, and biometric features. The authors conducted a safety analysis of the proposed protocol based on the ROR model. Research has shown that the protocol is resistant to replay attacks, user impersonation attacks, server impersonation attacks, privileged-insider attacks, KSSTI attacks, and stolen smart card attacks. Moreover, the protocol ensures perfect forward secrecy. The authors also showed that the LAP-IoHT protocol is more computationally efficient than similar solutions and has low communication costs.

Agrahari et al. [97] focused on securing communication between doctor and patient. The authors proposed a two-factor authentication protocol by using hashing functions and bilinear pairing. Authentication is based on the smart card and password entered by the users. The authors checked the safety and correctness of the proposed scheme by using the Avispa tool and the BAN logic. The formal and informal analyses showed that the protocol meets the following security properties, mutual authentication, user anonymity, perfect forward secrecy, and untraceability, and is resistant to MITM, offline password guessing attacks, and privileged-insider attacks and replay attacks. The authors also compared their protocol with similar solutions and obtained satisfactory results in achieving security attributes and energy consumption during communication and calculations.

Tanveer et al. in [98] have proposed an authentication protocol targeting the telecare medical information system. This protocol uses lightweight cryptography-based authenticated encryption with associative data and the hash function of the Esch256 [99] hash. The authors showed that their protocol ensures the anonymity and privacy of users and is resistant to MITM attacks, replay attacks, impersonation attacks and DoS attacks. Moreover, the authors used the ROM model and Scyther tools to confirm the level of security provided by the proposed protocol. Compared to similar solutions, this protocol generates lower computational and communication costs.

Pardeshi et al. in [100] highlighted the problems of adequately securing IoT devices in fog or edge processing. This problem arises with mass-produced IoT devices that ignore basic security requirements and make them vulnerable to attacks. Therefore, the authors proposed a hash–chain fog/edge zero-knowledge protocol, the task of which is to authenticate each other and agree on session keys in the fog/cloud processing environment for different devices. In the proposed protocol, the authentication process takes place by using a centralized server that manages the keys. The protocol consists of the phases: initialization, registration, authentication, communication, and revocation. The authors confirmed the performance and correctness of the protocol on various architectures and workstations, including interconnectivity. Moreover, they established the security of the protocol using the BAN logic. They also demonstrated the protocol's resistance to active and passive attacks, modification, sinkhole, monitoring, replay, location disclosure, and Sybil attacks.

Iqbal et al. in [101] proposed an authentication protocol with a key agreement for IoT and cloud computing environments. The authors used elliptic curve algorithms and symmetric encryption/decryption. The authors performed a formal protocol security analysis by using BAN logic and the Scyther tool. In turn, informal analyses showed the protocol's resistance to replay attacks, impersonation attacks, traceability attacks, message integrity attacks, and MITM attacks. Computational and communication cost studies have shown that the protocol proposed by Iqbal et al. in [101] is more efficient than similar solutions.

Wu et al. in [102,103] focused on IoT-related cloud computing solutions. In both years, they used Intel software guard extensions (SGX) [104] to improve the security of protocols used in cloud solutions. In Wu et al. [102], the authors proposed the SAKAP protocol for authentication and session key reconciliation. The authors use SGX to store a shared key. The authors performed formal (using the ROR model and the ProVerif tool) and informal protocol analysis. Research has shown that the protocol is resistant to replay attacks, MITM attacks, and impersonation attacks and provides security features such as anonymity and untraceability. In turn, in [103], the authors proposed the SQXAP protocol that can be used to authenticate intelligent vehicles in cloud systems. The authors also performed formal (using the ROR model) and informal analyses for this protocol. Research has shown that the protocol is resistant to replay attacks, insider attacks, and MITM attacks, and provides security properties such as mutual authentication, anonymity, and untraceability.

Zhao et al. in [105], Zhao et al. focused on industrial IoT (IIoT) security. The authors noticed that the low computing power of IIoT devices resulted in the low level of security implemented in such networks. The authors proposed a three-factor authentication and key-handshake protocol to solve such problems based on elliptic curve cryptography. The protocol can work on networks with one or more gateways. The authors confirmed the security of this protocol by using the ROM model and the Scyther tool. In turn, informal analyses confirmed that the protocol provides mutual authentication, session key agreement, forward and backward secrecy, user anonymity, and untraceability. Moreover, the protocol is resistant to stolen smart card attacks, replay attacks, privileged-insider attacks, desynchronization attacks, and impersonation attacks. The authors also compared their protocol and similar solutions for IIoT and obtained satisfactory results in achieving security attributes and energy consumption during communication and calculations.

Yi et al. in [106] also proposed an authentication protocol for IIoT. The proposed protocol uses the physically unclonable function (PUF) [107] chip and uses the Bloom [108] filter to preauthenticate and reduce computation and communication costs. The authors performed a formal safety analysis of the proposed protocol by using the Avispa tool and informal analysis. The research showed that the proposed protocol for ensuring the following security properties: mutual authentication, identity anonymity, and untraceability and forward and backward secrecy of session keys, and is also resistant to tampering attacks, replay attacks, simulation and forgery attacks, physical attacks, and desynchronization attacks. Moreover, the authors compared their protocol with other schemes regarding security and computational and communication costs with satisfactory results.

Panda et al. in [109] focused on industrial IoT solutions and proposed an authentication protocol for machine-to-machine communication. The authors tried to minimize the computational and communication load while increasing communication security. The authors used only XOR operations and hashing functions, and the shared symmetric key is only generated after two rounds of communication without human intervention. The authors carried out a formal (using BAN logic and the Avispa tool) and informal analysis of the protocol's security, showing that it is resistant to typical attacks occurring in IoT environments. In conclusion, the authors emphasized the advantages of a protocol that meets security properties with low computational and communication costs. Moreover, they noted that the protocol could be successfully implemented in other IoT domains.

Zhang et al. in [110] have developed an authentication protocol for the cross-domain IoT environment. The protocol uses the elliptic curve digital signature algorithm, blockchain technology, and a specially designed cryptocurrency token to build trust between entities. The authors analyzed the safety of the proposed protocol. They showed that it is resistant to MITM attacks, replay attacks, revealing identity attacks, authority abuse attacks, and DoS attacks. In addition, they demonstrated its computing and communication performance. In turn, Wang et al. in [111] confirmed this protocol's computing and communication advantages. However, they showed that it only allows one-way authentication and adds to the burden of certificate storage.

Li et al. in [112] have proposed a mutual authentication protocol with key handshaking based on blockchain, elliptic curves, and bilinear pairs. The authors replaced the centralized CA with the registration authority to avoid single-node failure and some attacks. In addition, the key recovery and key update scheme use the Lagrange interpolation method [113]. The authors formally confirmed the safety of the proposed protocol by using the ProVerif tool and the ECK model [114]. Informal security analyses have shown that the proposed protocol is resistant to typical IoT attacks. Moreover, the authors noted that this protocol's computational and communication overhead is negligible. However, Ryu et al. in [115] pointed out that the protocol barred by Li et al. in [112] user anonymity is prone to insider attacks.

Hajian et al. in [116] proposed a two-way, mutual authentication and key agreement protocol. The protocol involves four phases: initialization, registration and generation of secret keys of long duration, key authentication and reconciliation, and updating public and private keys. The authors, using the ROR model, BAN logic and the Scyther tool, confirmed the correctness and safety of the proposed protocol. Additionally, the informal analysis showed resistance to this protocol to replay attacks, MITM attacks, device capture attacks, privilege-insider attacks, KCI attacks, known specific temporary information attacks, impersonation attacks, and known-key attacks. In addition, these analyses showed that the protocol provides anonymity and untraceability and perfect forward/backward secrecy. The authors also assessed their protocol in terms of communication, calculation costs, and energy consumption, and they obtained satisfactory results in comparison with similar solutions.

Gong et al. in [117] proposed a lightweight protocol for authenticating and negotiating session keys. The proposed protocol uses shared secret and elliptic curve public key technology and is based on the CoAP framework [118]. The techniques used to ensure the security and anonymity of devices and users. The authors verified the performance and safety of the proposed protocol by using the Dolev–Yao adversary model [119] and the CPN Tools tool [120]. The analysis showed that the protocol provides the following security properties: confidentiality, data integrity, mutual authentication, perfect forward and backward secrecy, device anonymity, and unlinkability. The protocol is resistant to impersonation attacks, MITM attacks, privileged-insider attacks, replay attacks, KCI attacks, desynchronization attacks, and DoSs attacks. Moreover, the authors compared their protocol with other schemes regarding security and computational and communication costs with satisfactory results.

Chen et al. in [121] proposed another two-factor authentication and key agreement protocol for IoT environments. The proposed protocol consists of the predeployment phase, the IoT device registration phase, and the login and authentication phase. The authors distinguished two roles: IoT devices and a server. The IoT device must register on the server. Further communication between these devices takes place by using a session key generated by the server. The authors tested the security of the proposed protocol by using the ROR model and the BAN logic. Studies have shown that the protocol is resistant to privileged-insider attacks, known temporary information disclosure attacks, stolen verification attacks, IoT device simulation attacks, and physical IoT device capture attacks. In addition, the protocol provides the perfect forward secrecy property. Moreover, the authors compared the proposed protocol with similar security and computational and communication cost solutions, obtaining satisfactory results.

Another mutual authentication protocol was proposed by Safkhani et al. in [122]. The authors focused on the use of RFID technology in the IoT environment. The authors created a new message authentication code function for the proposed protocol by analyzing the existing protocols and their problems and possible attacks. The authors formally informally verified their protocol's security (using BAN logic and the Scyther tool). The protocol is resistant to replay attacks, secret disclosure attacks, impersonation attacks, and desynchronization attacks. Moreover, the authors showed that their proposed protocol is characterized by low computing and communication costs, and therefore it can be implemented in environments with low resources and computing power.

Khorasgani et al. in [123] proposed three lightweight protocols called LRSAS+, LRARP, and LRARP+ for use in IoT solutions. The authors chose the operations performed during the protocol to be safe and computationally light, i.e., they do not burden the communicating devices. The authors confirmed the protocol's security by using GNY logic and the Scyther tool. The protocol is resistant to tag-tracking attacks, replay and reader impersonation attacks, desynchronization attacks, and DoSs attacks. In addition, the protocol meets forward–backward secrecy. The study of the efficiency of the proposed protocols also confirmed the authors' initial assumptions regarding not overloading communicating devices.

Alam et al. [124] have proposed a new authentication protocol for use in IoT environments. The authors used the elliptic curve discrete logarithm problem [125] properties, hash functions, and XOR operations to ensure robust and secure authentication. The authors tested their protocol by using the BAN logic and the Avispa tool and demonstrated its resistance to forging, guessing, masquerading, DoSs and MITM attacks. Moreover, the protocol complies with security properties such as user anonymity and untraceability or perfect forward secrecy. Furthermore, the authors compared the proposed protocol with other schemes in terms of security and computational and communication costs, obtaining satisfactory results. The authors concluded that the proposed protocol can be implemented for various applications of IoT devices and that it can be successfully extended with other techniques of securing the authentication process.

Mirsaraei et al. in [126] proposed a three-factor authentication protocol for IoT environments. The protocol uses blockchain technology, hashing functions, XOR, and the concept of a fuzzy extractor. The cryptographic techniques ensure an appropriate level of security, protect data against manipulation and increase the transparency of the recorded information on smart cards. The authors used the BAN logic, the ROR model and the Avispa tool for formal analysis. Research has shown the security of mutual authentication implemented by the proposed protocol.

Conversely, an informal analysis showed that the protocol provides data confidentiality, mutual authentication, data integrity, forward security, anonymity, authorization, three-factor secrecy, and secured password updating. Moreover, the proposed protocol is resistant to replay attacks, password-guessing attacks, DoS attacks, server impersonation attacks, privileged-insider attacks, KSSTI attacks, user impersonation attacks, stolen smart card attacks, MITM attacks, and brute force attacks. The authors concluded that their protocol is superior in computation cost, communication cost, security requirements, and attack resistance compared to similar solutions.

Saqib et al. in [127] proposed a three-factor authentication protocol for mission-critical IoT-based applications. The protocol is based on the publish–subscribe model and uses elliptical curve cryptography (ECC) and computationally low hash chains. Authentication is done through an identity, password, and digital signature. The authentication process also generates a dynamic session key based on the value of the nonce. Dynamic key changes make the protocol resistant to attacks on session keys. An informal protocol security analysis showed its resistance to MITM attacks, smart card stolen attacks, publisher, subscriber, or broker impersonation attacks, known session key attacks, offline password guessing attacks, replay attacks, and privileged-insider attacks. In addition, the protocol provides confidentiality, mutual authentication and perfect forward secrecy. The formal safety analysis was performed by using the Scyther tool. The authors also showed that, compared to similar protocols, the proposed protocol saves bandwidth and communication energy while reducing resource-constrained sensor nodes' computation and communication costs.

Hu et al. in [128] focused on the weaknesses of existing IoT authentication protocols. The authors opposed a two-factor authentication protocol by using ECC, passwords, and smart cards. The authors conducted formal (using the ProVerif tool) and informal verification of their protocol. Based on analyses, they showed that the protocol is resistant to impersonation attacks, offline password guessing attacks, replay attacks, and sensor node captured attacks. In addition, they found the proposed protocol to be secure, meeting user and session key security requirements. In addition, it achieves satisfactory results in terms of computational costs.

Haseeb-ur-rehman et al. in [129] introduced a two-factor authentication protocol based on a symmetric key, by using biometrics and a password. The proposed protocol consists of six phases: the initialization, the smart device enrollment, the gateway node enrollment, the user enrollment, the login and authentication and the password and biometric update. The authors conducted formal (using the Avispa tool) and informal analyses of the safety of the proposed protocol. Research has shown that the protocol ensures security properties such as session key freshness property, perfect forward secrecy, user anonymity, and untraceability. In addition, it is resistant to replay attacks, impersonation attacks, and MITM attacks. The authors also showed that their protocol has lower computational costs than similar protocols.

Kumar et al. in [130] focused on IoT solutions for vehicles. The authors proposed an authentication protocol based on RFID and PUF technologies. The protocol assumes the presence of three roles: a tag, a reader, and a cloud server, and each of the components can operate independently. The tag is responsible for initiating communication with the reader, and the reader must validate the message sent by the tag and send it to the server. The server is responsible for tag and reader authentication. The authors tested the safety of the proposed protocol by using the ROR model and informal analyses. Research has shown that the protocol is resistant to ephemeral secret leakage attacks, MITM attacks, insider attacks, replay attacks, impersonation attacks, offline password-guessing attacks, and desynchronization attacks. Moreover, the proposed protocol maintains the following security properties: location privacy, mutual authentication and session key agreement, forward secrecy, and message authentication. Furthermore, the authors compared their protocol with other schemes regarding security and computational and communication costs with satisfactory results.

Gupta et al. in [131] proposed an authentication protocol for IoT solutions for vehicles. The authors based the security of their protocol on identity-based cryptography [132] and lattice cryptography [133]. The authors verified the correctness and security of their protocol by using the ROM model. Research has shown that the protocol is resistant to MITM attacks, Unknown key-share attacks, and known-key security attacks and provides perfect forward secrecy. In addition, the authors compared the protocol with similar solutions in terms of reference and communication costs. The authors concluded that the proposed protocol is computationally efficient and can be implemented in real IoT solutions for vehicles.

Zhang et al. in [134] observed that the development of IoT systems for vehicles, on the one hand, contributed to easing the traffic load and improving travel efficiency. On the other hand, these systems are exposed to security threats in many respects. Therefore, the authors proposed an authentication protocol for such solutions. The proposed protocol uses blockchain technology and a chaotic mapping algorithm. It allows vehicles and roadside units to register to obtain a public identity, which they then use to authenticate and negotiate the key. The authors confirmed the security of their protocol with the Scyther tool. Moreover, they showed that the proposed protocol has lower computation and communication costs than the existing schemes.

Bera et al. in [135] focused on IoT solutions that use drones in agriculture. The authors proposed an authentication and key management protocol based on blockchain technology. The authors examined their protocol for its susceptibility to attacks occurring in IoT environments. They showed that the protocol is resistant to MITM attacks, replay attacks, impersonation attacks, privileged-insider attacks, physical IoT smart device and drone capture attacks, and ephemeral capture attacks, secret leakage attacks. In addition, the authors performed a formal protocol analysis by using the ROR model and the Avispa tool. In conclusion, the authors concluded that the protocol has low computational and communication costs.

Tanveer et al. suggested two protocols for IoT drone solutions: a protocol for the authentication process in [136], and a protocol for the key agreement process in [137,138]. These protocols use AES-CBC-256, ECC, SHA-256 hash functions, and XOR operations. The authors have demonstrated the resistance of these protocols to common attacks occurring in IoT environments, for example, replay attacks and MITM attacks. The authors used the ROM model and the Scyther tool for formal analysis of the protocols. The authors used both proposed protocols in the [139] framework for drones because both are efficient in terms of communication, storage and computing costs compared to similar solutions.

Javed et al. in [140] have abandoned the blockchain-based authentication protocol and the hyperelliptic curve cryptography for IoT drones. In this approach, the blockchain is used as a certification authority, and transactions are defined as certificates. Such action is designed to reduce maintenance costs while ensuring a high level of communication security. The authors concluded that the proposed protocol is resistant to common attacks in drone IoT networks and is also cost-effective in terms of computation and communication compared to similar solutions.

4. Discussion

Many different protocols are available for use in IoT environments, with different characteristics, purposes and applications. As mentioned in this manuscript, we focused on protocols that fulfill the purposes of authentication, agreement, and agreement of the session key. The protocols may pursue one or more of these objectives during their operation. The overviewed protocols use cryptographic techniques to achieve their goals and secure communication. These protocols have been validated with various tools and methods for vulnerability to attacks and providing essential security features.

In Table 2, we summarized the revised protocols in terms of the purpose they pursue. We have designated three types of protocols based on the analyzes performed. Here we can observe the need to create protocols primarily for user authentication. An essential aspect of communication is the reconciliation and agreement of session keys; hence, developing and applying this protocol is also key to securing communication.

Table 2. The summary of protocol types.

Protocol Type	References
Authentication protocol	[81,82,85,90,91,96–98,103,106,110,122–124,126,128–131,134,136,140]
Authentication & key agreement protocol	[100–102,105,109,112,116,117,121,127,135]
Key agreement protocol	[137,138]

Table 3 provides a summary of the protocols discussed in terms of their uses and interoperability. We considered protocols targeted at specific solutions such as those intended for medicine and health, fog, edge, or cloud computing, and vehicular, drone, or industrial purposes. However, protocols that can be used in different resolutions (multidomain protocols) also play an essential role. In addition to multidomain solutions, many security protocols have been developed for solutions related to direct human safety, be it physical or environmental. First and foremost, it is about securing communications in medical environments where, on the one hand, we need to ensure patients 'data and privacy and, on the other hand, safeguard their health and life, as IoT devices are used to control patients' vital functions. Another important aspect will be the protocols for industrial solutions that also relate to securing people environmentally and physically. As in the case of medical solutions, we must secure both data sent in industrial networks and protect against attacks that could contribute to the incorrect operation of industrial devices and thus threaten the health and life of employees.

Table 3. The summary of protocol solutions.

IoT Solution	References
Medicine & health	[81,82,85,90,91,96–98]
Fog, edge, or cloud computing	[100–103]
Vehicular	[130,131,134]
Drones	[135,136,140]
Industrial	[105,106,109,137,138]
Multidomain	[110,112,116,117,121–124,126–129]

Table 4 shows the attacks against which the described protocols for IoT are resistant. The table contains only those protocols for which the authors conducted formal and informal security evidence and indicated which attacks their proposed protocol is resistant to. In some papers (such as [81,82,91,134,136] or [137,137,137,137]) lists of attacks emerged. On the other hand, in other papers (such as [90,109] or [112]), the authors only suggested that their protocols are resistant to typical attacks in IoT environments. The table contains a list of attacks and an annotation regarding the resistance of the tested protocol to attack. We only included those attacks that appear in a few papers. These attacks seemed once (e.g., Sybil attack or sinkhole attack) are included in the Others column. The flag + indicates that the authors have demonstrated that their proposed protocol is immune to attack. The flag - means that the protocol has not been verified to be vulnerable to attack.

We have observed that the most frequently tested vulnerabilities in IoT environments are impersonation attacks, MITM attacks, and replay attacks. Most reviewed papers reported studies of proposed protocols for these attacks, indicating that they are among the most dangerous vulnerabilities. These attacks can lead to the loss of a significant amount of information, necessitating protection against them in IoT environments. The attacker can combine different techniques when carrying out an attack. An attacker can listen to and intercept network traffic and then retransmit it to convince the recipient to perform specific actions. The attack results depend on the attacker's knowledge, skills and imagination and the vulnerability and specificity of the attacked environment. One of the most dangerous outcomes of an attacker may be the loss of confidential information. Protection against this type of attacker activity should consider using message timestamps and one-time session keys during communication.

Table 4. The summary of attacks upon the protocols.

Paper	Impersonation	Insider	Stolen Smart Card	MITM	Modification	Replay	Capture	Secret Leakage	Unknown Key-Share	Known-Key Security	Guessing	Desynchronisation	KSSTI	DoS	Others
[85]	+	+	+	+	+	-	-	-	-	-	-	-	-	-	-
[96]	+	+	+	-	-	+	-	-	-	-	-	-	+	-	-
[97]	-	+	-	+	-	+	-	-	-	-	+	-	-	-	-
[98]	+	-	-	+	-	+	-	-	-	-	-	-	-	+	-
[100]	-	-	-	-	+	+	-	-	-	-	-	-	-	-	+
[101]	+	-	-	+	-	+	-	-	-	-	-	-	-	-	-
[102]	+	-	-	+	-	+	-	-	-	-	-	-	-	-	-
[103]	-	+	-	+	-	+	-	-	-	-	-	-	-	-	-
[105]	+	+	+	-	-	+	-	-	-	-	-	+	-	-	+
[106]	-	-	-	-	-	+	-	-	-	-	-	+	-	-	+
[110]	-	-	-	+	-	+	-	-	-	-	-	-	-	+	+
[116]	+	+	-	+	-	+	+	-	-	+	-	-	+	-	+
[117]	+	+	-	+	-	+	-	-	-	-	-	+	-	+	+
[121]	-	+	+	-	-	-	-	-	-	-	-	-	+	-	+
[122]	+	-	-	-	-	+	-	-	-	-	-	+	-	-	+
[123]	+	-	-	-	-	-	-	-	-	-	-	+	-	+	+
[124]	-	-	-	+	-	-	-	-	-	-	+	-	-	+	+
[126]	+	-	+	+	-	+	-	-	-	-	+	-	+	+	+
[127]	+	+	+	+	-	+	-	-	-	+	-	-	-	-	-
[128]	+	-	-	-	-	+	+	-	-	-	+	-	-	-	-
[129]	+	-	-	+	-	+	-	-	-	-	-	-	-	-	-
[130]	+	+	-	+	-	+	-	+	-	-	+	+	-	-	-
[131]	-	-	-	+	-	-	-	-	+	+	-	-	-	-	-
[135]	+	+	-	+	-	+	+	+	-	-	-	-	-	-	-

Table 5 summarizes the security aspects of the analyzed protocols. Moreover, in this table, we have included only those protocols for which the authors conducted formal and informal proofs of security and indicated the security aspects that their protocols provide. In some papers (e.g., [90,91,100,101]), the authors did not include the list of aspects. In this table, we have included a list of aspects with an annotation of whether the protocol meets the property (designation +). The designation - means that there is no information about the assurance of ownership by the investigated protocol. The analysis showed forward security is the most desirable security property, a specific feature of the session key agreement protocols.

Table 5. The summary of security aspects.

Paper	Privacy	Data Integrity	Authenticity	Forward Secrecy	Backward Secrecy	Mutual Authentication	User Anonymity	Untraceability	Session Key Agreement	Confidentiality
[81]	+	+	+	-	-	-	-	-	-	-
[96]	-	-	-	+	-	-	-	-	-	-
[97]	-	-	-	+	-	+	+	+	-	-
[98]	+	-	-	-	-	-	+	-	-	-
[102]	-	-	-	-	-	-	+	+	-	-
[103]	-	-	-	-	-	+	+	+	-	-
[105]	-	-	-	+	+	+	+	+	+	-
[106]	-	-	+	+	+	+	+	+	-	-
[116]	-	-	-	+	+	-	+	+	-	-
[117]	-	+	-	+	+	+	+	-	-	+
[121]	-	-	-	+	-	-	-	-	-	-
[123]	-	-	-	+	+	-	-	-	-	-
[124]	-	-	-	+	-	-	+	+	-	-
[126]	-	+	-	+	-	+	+	-	-	+
[127]	-	-	-	+	-	+	-	-	-	+
[129]	-	-	-	+	-	-	+	+	-	-
[130]	+	-	-	+	-	+	-	-	+	-
[131]	-	-	-	+	-	-	-	-	-	-

The authors of all overviewed papers have also conducted performance studies of their protocols. The authors compared their proposals with similar solutions in terms of communication and calculation costs and energy consumption. The authors found that the proposed protocols achieve better performance in all studies than comparable solutions.

To summarize the overviewed protocols, the authentication process is the essential communication element in IoT environments. The process consists of confirming the identity of the communicating parties. One or more factors may be used during authentication; the more factors, the greater the safety of the entire process. If only passwords are used for authentication, this can be a weak and vulnerable security. An attacker can intercept, guess or crack passwords. Hence, a better solution is to use biometrics as it will avoid spoofing or impersonating attacks.

Authentication is vulnerable to rogue users. Attackers can launch attacks to obtain private user information, block the operation of selected system components, or cause the system to malfunction. The most dangerous attacks are MITM attacks, replay attacks, and the impersonation mentioned above because they can lead to the loss of user data and the compromise of essential security properties. The desynchronization attack can be equally dangerous because, in many IoT environments (for example, medical), proper data synchronization is crucial to the entire system's operation.

An essential element of securing communication is using session keys, which are used to encrypt it. To protect communication against a replay attack or MITM attack, it is worth using one-time session keys, and messages should be timestamped. Thanks to this, the system will unequivocally determine whether a legitimate network node generated the processed message or whether it was intercepted by the attacker and resent by him.

In addition to the security aspects, we should also bear in mind the issues related to the scalability of protocols in the IoT environment. Devices used in IoT environments, or WSN sensors, have limited computing power. For this reason, calculations performed on individual devices while the protocol is running should not drain its energy. For this reason, when designing authentication or key agreement protocols, it is worth using lightweight cryptographic algorithms that will ensure an appropriate level of data security but will not burden system resources. In turn, data storage should be left to centralized units with more computing and hardware resources than individual nodes of the IoT or WSN environment.

Newly proposed protocols should be adequately screened for vulnerability to attacks and their essential security features. There are many different methods and tools for this (mentioned in Section 1). In addition, implemented and operational protocols should also be systematically checked for this, as the methods used by attackers constantly evolve.

5. Conclusions

In this manuscript, we surveyed papers that proposed key agreement and authentication protocols for the Internet of things and wireless sensors networks. We collected papers focusing on problems with security, especially in IoT that offer new protocols aimed at correcting vulnerabilities in existing protocols. We discussed the theoretical aspects of IoT environments, cryptographic methods that can be used to secure communication, and cyberattacks that can compromise the security in the environments under consideration.

We highlighted the key agreement, distribution process, and authenticating users or devices on such networks in this manuscript. These processes provide critical communication steps as they prevent unauthorised access to session keys and unauthorised access by unauthorised users or devices. Data transferred between network nodes can be of different natures and importance, and they need to be appropriately secured during communication. All communications are exposed to dishonest users called attackers. Attackers' activity may involve attacks on various aspects of the network, such as passwords, keys, biometric data or devices, and eavesdropping and retransmitting the same messages.

We looked at various solutions related to authentication and matching of session keys. The authors of the protocols under consideration focused on essential security properties such as untraceability and anonymity, and the solutions' authors focused on crucial security features. The authors also validated their protocols with formal and informal methods that considered the vulnerability of these protocols. Various techniques (e.g., BAN logic or GNY) and automatic tools (e.g., Scyther, ProVerif) were used for verification. Thanks to the methods and tools used, the authors showed what level of security is provided by the protocol they propose.

The selected protocols' analysis showed that the most dangerous attacks for IoT are impersonation attacks, MITM attacks, and replay attacks because the susceptibility to these attacks was most often checked and verified by the authors of the selected works. During impersonation attacks, the attacker identifies himself with another user on the network and tries to convince other users of his identity. The replay attack involves duplicating packets and sending them multiple times. At any time during this attack, the attacker can also use a MITM attack to intercept transmitted messages. A successfully conducted attack may result in the loss of confidential data, which may cause further problems for the user. The essential protection principle against attacks is using timestamps in messages and one-time session keys. Timestamps will allow us to verify the time when a message was generated.

On the other hand, disposable session keys will prevent the repeated sending of a message encrypted with an outdated key. Other types of attacks cannot be underestimated. Attacks during which the attacker tries to guess the password (guessing attacks) and the loss of data or devices that verify the user (stolen attacks) are equally dangerous. Such situations may contribute to the fact that an unauthorized user can log in with the correct credentials of an honest user and thus impersonate him.

After analyzing the current state of knowledge in the security protocols for IoT and WSN environments, we set out to indicate further research directions in this area. Here we can indicate the three most important aspects that should pay attention to constructing secure protocols for IoT.

The first is security. Protocols should provide an appropriate level of security for users and data sending because the methods of breaking security are constantly evolving. Therefore, research goals in security protocols for IoT and WSN environments should focus on technologies and solutions that provide increasingly better security. The elliptic curve algorithms are particularly noteworthy here, because they offer security comparable to the Rivest–Shamir–Adleman algorithm when using shorter encryption keys. Authentication and verification of users' identities are also essential elements of security. These processes should take place, taking into account at least two factors. Authentication using only the user's password does not provide an adequate level of security, especially in situations in which the user uses the same password when logging into many services or applications. The best solution worth developing is using biometric methods during these two processes. Biometric methods allow us to identify and confirm the user's identity.

The second aspect of security protocols for IoT and WSN environments is performance. The computing load of IoT devices during communication should be as low as possible so that devices and their users can work efficiently without delays. Blockchain is an interesting technology in this regard, because it ensures nonrepudiation and data transparency. On the other hand, considering calculations in clouds or fog is conducive to achieving low transmission delays and efficient bandwidth use.

The last aspect to consider is cross-platform. Protocols for IoT should be cross-platform. Some of the protocols reviewed in this manuscript are application-specific (e.g., in medicine). When designing a security protocol for IoT, it is worth considering a broader spectrum of applications so that one authentication or key agreement and distribution protocol can be implemented in many solutions.

After analyzing the current state of knowledge in the field of protocols for the IoT and WSNs environments, we set ourselves further research goals. In our next work, we will focus on designing and creating a secure communication framework to be implemented in IoT. We will include a newly designed and secure communication protocol, thanks to which it will be possible to agree on and distribute the session key and user authentication. When designing and creating the framework and protocol, we will consider the security features to ensure the safety of users. We will also include one-time verification credentials, keys, and timestamps to protect the environment from attacks.

Author Contributions: Conceptualization, S.S. and S.K.; methodology, S.S.; validation, S.S. and S.K.; formal analysis, S.K.; investigation, S.S.; writing—original draft preparation, S.S. and S.K.; writing—review and editing, S.S. and S.K.; visualization, S.S.; supervision, S.S. and S.K.; project administration, S.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The project financed under the program of the Polish Minister of Science and Higher Education under the name "Regional Initiative of Excellence" in the years 2019–2023 project number 020/RID/2018/19 the amount of financing PLN 12,000,000.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

AES(-CBC-256)	Advanced Encryption Standard Cipher Algorithm in Cipher Block Chaining Mode (256 bits keys)
BAN logic	Burrows–Abadi–Needham logic
CA	Certification Authority
CIA triad	Confidentiality, Integrity, Availability triad
CoAP	Constrained Application Protocol
CPN	Coloured Petri Nets
DoS	Denial of Service attack
ECC	Elliptical Curve Cryptography
ECK model	Extended Canetti-Krawczyk model
Esch256	Esch256 (Efficient, Sponge-based, and Cheap Hashing (256 bits hashes)
GNY logic	Gong-Needham-Yahalom logic
(I)IoT	(Industrial) Internet of Things
LAP-IoHT	Lightweight Authentication Protocol for the Internet of Health Things
KCI	Key Compromise Impersonation attack
KSSTI	Known Session-Specific Temporary Information attack
MITM	Man in the Middle attack
MQTT	MQ Telemetry Transport
NFC	Near Field Communication
PUF	Physically Unclonable Function
RFID	Radio Frequency Identification
ROM	Random Oracle Mode
ROR	Real-Or-Random
SGX	Intel Software Guard Extensions
SHA-256	Secure Hash Algorithm (256 bits hashes)
SQXAP	SGX-Based Authentication Protocol
SVO logic	Syverson-Van Oorschot logic
WSN	Wireless Sensor Networks
XOR	Exclusive Or
6LoWPAN	IPv6 over Low-Power Wireless Personal Area Networks

References

1. Kumar, A.; Saha, R.; Conti, M.; Kumar, G.; Buchanan, W.J.; Kim, T.H. A comprehensive survey of authentication methods in Internet-of-Things and its conjunctions. *J. Netw. Comput. Appl.* **2022**, *204*, 103414. [CrossRef]
2. Kim, J.; Colabianchi, N.; Wensman, J.; Gates, D.H. Wearable Sensors Quantify Mobility in People With Lower Limb Amputation During Daily Life. *IEEE Trans. Neural Syst. Rehabil. Eng.* **2020**, *28*, 1282–1291. [CrossRef] [PubMed]
3. Steinmetzer, T.; Wilberg, S.; Bönninger, I.; Travieso, C.M. Analyzing gait symmetry with automatically synchronized wearable sensors in daily life. *Microprocess. Microsystems* **2020**, *77*, 103118. [CrossRef]
4. Khan, F.; Xu, Z.; Sun, J.; Khan, F.M.; Ahmed, A.; Zhao, Y. Recent Advances in Sensors for Fire Detection. *Sensors* **2022**, *22*, 3310. [CrossRef]
5. Alsaeed, N.; Nadeem, F. Authentication in the Internet of Medical Things: Taxonomy, Review, and Open Issues. *Appl. Sci.* **2022**, *12*, 7487. [CrossRef]
6. Wu, H.; Dyson, M.; Nazarpour, K. Arduino-Based Myoelectric Control: Towards Longitudinal Study of Prosthesis Use. *Sensors* **2021**, *21*, 763. [CrossRef]
7. Chen, A.; Zhang, J.; Zhao, L.; Rhoades, R.D.; Kim, D.Y.; Wu, N.; Liang, J.; Chae, J. Machine-learning enabled wireless wearable sensors to study individuality of respiratory behaviors. *Biosens. Bioelectron.* **2020**, *173*, 112799. [CrossRef]
8. Singh, S.; Nandan, A.S.; Sikka, G.; Malik, A.; Vidyarthi, A. A secure energy-efficient routing protocol for disease data transmission using IoMT. *Comput. Electr. Eng.* **2022**, *101*, 108113. . [CrossRef]
9. Sivakumar, P.; Sandhya Devi, R.; Ashwin, M.; Rajan Singaravel, M.; Buvanesswaran, A. Protocol Design for Earthquake Alert and Evacuation in Smart Buildings. In *IoT and WSN based Smart Cities: A Machine Learning Perspective*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 1–14.
10. Zhou, H.; Wang, Z.; Zhao, W.; Tong, X.; Jin, X.; Zhang, X.; Yu, Y.; Liu, H.; Ma, Y.; Li, S.; et al. Robust and sensitive pressure/strain sensors from solution processable composite hydrogels enhanced by hollow-structured conducting polymers. *Chem. Eng. J.* **2021**, *403*, 126307. [CrossRef]

11. Bag, A.; Lee, N.E. Recent Advancements in Development of Wearable Gas Sensors. *Adv. Mater. Technol.* **2021**, *6*, 2000883. [CrossRef]
12. Nait Aicha, A.; Englebienne, G.; Van Schooten, K.S.; Pijnappels, M.; Kröse, B. Deep Learning to Predict Falls in Older Adults Based on Daily-Life Trunk Accelerometry. *Sensors* **2018**, *18*, 1654. [CrossRef] [PubMed]
13. Kubanek, M.; Bobulski, J. Device for Acoustic Support of Orientation in the Surroundings for Blind People. *Sensors* **2018**, *18*, 4309. [CrossRef] [PubMed]
14. Kamil, I.A.; Ogundoyin, S.O. A lightweight mutual authentication and key agreement protocol for remote surgery application in Tactile Internet environment. *Comput. Commun.* **2021**, *170*, 1–18. [CrossRef]
15. Mena, A.R.; Ceballos, H.G.; Alvarado-Uribe, J. Measuring Indoor Occupancy through Environmental Sensors: A Systematic Review on Sensor Deployment. *Sensors* **2022**, *22*, 3770. [CrossRef] [PubMed]
16. Alshammari, M.R.; Elleithy, K.M. Efficient and Secure Key Distribution Protocol for Wireless Sensor Networks. *Sensors* **2018**, *18*, 3569. [CrossRef]
17. Ye, H.; Lee, C.J.; Wu, T.Y.; Yang, X.D.; Chen, B.Y.; Liang, R.H. Body-Centric NFC: Body-Centric Interaction with NFC Devices through Near-Field Enabled Clothing. In Proceedings of the Designing Interactive Systems Conference, Online, 13–17 June 2022; pp. 1626–1639.
18. Al-Amiedy, T.A.; Anbar, M.; Belaton, B.; Kabla, A.H.H.; Hasbullah, I.H.; Alashhab, Z.R. A Systematic Literature Review on Machine and Deep Learning Approaches for Detecting Attacks in RPL-Based 6LoWPAN of Internet of Things. *Sensors* **2022**, *22*, 3400. [CrossRef]
19. Stanforda-Clarka, A.; Nipper, A. MQTT: The Standard for IoT Messaging. 2021. Available online: https://mqtt.org/ (accessed on 10 November 2022).
20. Lacava, A.; Zottola, V.; Bonaldo, A.; Cuomo, F.; Basagni, S. Securing Bluetooth Low Energy networking: An overview of security procedures and threats. *Comput. Netw.* **2022**, *211*, 108953. [CrossRef]
21. Upadhyay, D.; Manero, J.; Zaman, M.; Sampalli, S. Intrusion Detection in SCADA Based Power Grids: Recursive Feature Elimination Model With Majority Vote Ensemble Algorithm. *IEEE Trans. Netw. Sci. Eng.* **2021**, *8*, 2559–2574. [CrossRef]
22. Szymoniak, S. Security protocols analysis including various time parameters. *Math. Biosci. Eng.* **2021**, *18*, 1136–1153. [CrossRef]
23. Szymoniak, S.; Siedlecka-Lamch, O.; Zbrzezny, A.M.; Zbrzezny, A.; Kurkowski, M. SAT and SMT-Based Verification of Security Protocols Including Time Aspects. *Sensors* **2021**, *21*, 3055. [CrossRef]
24. Galinec, D.; Steingartner, W.; Zebic, V. Cyber Rapid Response Team: An Option within Hybrid Threats. In Proceedings of the 2019 IEEE 15th International Scientific Conference on Informatics, Poprad, Slovakia, 20–22 November 2019; pp. 43–49.
25. Steingartner, W.; Galinec, D.; Kozina, A. Threat Defense: Cyber Deception Approach and Education for Resilience in Hybrid Threats Model. *Symmetry* **2021**, *13*, 597. [CrossRef]
26. Szymoniak, S. Amelia—A new security protocol for protection against false links. *Comput. Commun.* **2021**, *179*, 73–81. [CrossRef]
27. Roggenbach, M.; Shaikh, S.A.; Nguyen, H.N. Formal Verification of Security Protocols. *Formal Methods for Software Engineering: Languages, Methods, Application Domains*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 395–451.
28. Zbrzezny, A.M.; Szymoniak, S.; Kurkowski, M. Practical Approach in Verification of Security Systems Using Satisfiability Modulo Theories. *Log. J. IGPL* **2020**, *30*, 289–300. [CrossRef]
29. Arcile, J.; André, E. Timed Automata as a Formalism for Expressing Security: A Survey on Theory and Practice. *ACM Comput. Surv.* **2022**, *55*, 127. [CrossRef]
30. Burrows, M.; Abadi, M.; Needham, R.M. A logic of authentication. *Proc. R. Soc. Lond. A. Math. Phys. Sci.* **1989**, *426*, 233–271.
31. Gong, L.; Needham, R.M.; Yahalom, R. Reasoning about Belief in Cryptographic Protocols. In Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, USA, 7–9 May 1990; Volume 1990, pp. 234–248.
32. Abdalla, M.; Fouque, P.A.; Pointcheval, D. Password-based authenticated key exchange in the three-party setting. In Proceedings of the International Workshop on Public Key Cryptography, Les Diablerets, Switzerland, 23–26 January 2005; Springer: Berlin/Heidelberg, Germany, 2005; pp. 65–84.
33. Xue, K.; Meng, W.; Li, S.; Wei, D.S.; Zhou, H.; Yu, N. A secure and efficient access and handover authentication protocol for Internet of Things in space information networks. *IEEE Internet Things J.* **2019**, *6*, 5485–5499. [CrossRef]
34. Syverson, P.F.; Van Oorschot, P.C. On unifying some cryptographic protocol logics. In Proceedings of the 1994 IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, CA, USA, 16–18 May 1994; pp. 14–28.
35. Barbosa, M.; Barthe, G.; Bhargavan, K.; Blanchet, B.; Cremers, C.; Liao, K.; Parno, B. SoK: Computer-Aided Cryptography. In Proceedings of the 2021 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 24–27 May 2021; pp. 777–795. [CrossRef]
36. Cremers, C.; Fontaine, C.; Jacomme, C. A Logic and an Interactive Prover for the Computational Post-Quantum Security of Protocols. In Proceedings of the S&P 2022—43rd IEEE Symposium on Security and Privacy, San Francisco, CA, USA, 23–25 May 2022.

37. Cortier, V.; Delaune, S.; Dreier, J. Automatic generation of sources lemmas in Tamarin: Towards automatic proofs of security protocols. In *Proceedings of the ESORICS 2020—25th European Symposium on Research in Computer Security*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2020; Volume 12309, pp. 3–22. [CrossRef]
38. Dreier, J.; Hirschi, L.; Radomirović, S.; Sasse, R. Verification of Stateful Cryptographic Protocols with Exclusive OR. *J. Comput. Secur.* **2020**, *28*, 1–34. [CrossRef]
39. Blanchet, B.; Cheval, V.; Cortier, V. ProVerif with lemmas, induction, fast subsumption, and much more. In Proceedings of the IEEE Symposium on Security and Privacy (S&P'22), San Francisco, CA, USA, 22–26 May 2022; pp. 205–222.
40. Blanchet, B.; Smyth, B. Automated reasoning for equivalences in the applied pi calculus with barriers. *J. Comput. Secur.* **2018**, *26*, 367–422. [CrossRef]
41. Yao, J.; Xu, C.; Li, D.; Lin, S.; Cao, X. Formal Verification of Security Protocols: ProVerif and Extensions. In *Proceedings of the International Conference on Artificial Intelligence and Security*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 500–512.
42. Alegria, J.A.H.; Bastarrica, M.C.; Bergel, A. Avispa: A tool for analyzing software process models. *J. Softw. Evol. Process.* **2014**, *26*, 434–450. [CrossRef]
43. Siedlecka-Lamch, O.; Szymoniak, S.; Kurkowski, M. A Fast Method for Security Protocols Verification. In *Proceedings of the IFIP International Conference on Computer Information Systems and Industrial Management*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 523–534.
44. Piatkowski, J. The Conditional Multiway Mapped Tree: Modeling and Analysis of Hierarchical Data Dependencies. *IEEE Access* **2020**, *8*, 74083–74092. [CrossRef]
45. Kandris, D.; Nakas, C.; Vomvas, D.; Koulouras, G. Applications of Wireless Sensor Networks: An Up-to-Date Survey. *Appl. Syst. Innov.* **2020**, *3*, 14. [CrossRef]
46. Dalal, B.; Kukarni, S. Wireless Sensor Networks: Applications. In *Wireless Sensor Networks*; Yellampalli, S.S., Ed.; IntechOpen: Rijeka, Croatia, 2021; Chapter 1. [CrossRef]
47. Luo, Q.; Liu, C.; Yan, X.; Shao, Y.; Yang, K.; Wang, C.; Zhou, Z. A Distributed Localization Method for Wireless Sensor Networks Based on Anchor Node Optimal Selection and Particle Filter. *Sensors* **2022**, *22*, 1003. [CrossRef] [PubMed]
48. Shahzad, K.; Zia, T.; Qazi, E.-U.-H. A Review of Functional Encryption in IoT Applications. *Sensors* **2022**, *22*, 7567. [CrossRef] [PubMed]
49. Yang, W.; Liu, L.; Liu, Y.; Fan, L.; Lu, W. Secure and efficient multi-dimensional range query algorithm over TMWSNs. *Ad Hoc Netw.* **2022**, *130*, 102820. [CrossRef]
50. Alshudukhi, J.; Yadav, K. Survivability development of wireless sensor networks using neuro fuzzy-clonal selection optimization. *Theor. Comput. Sci.* **2022**, *922*, 25–36. [CrossRef]
51. Rizzardi, A.; Sicari, S.; Coen-Porisini, A. Analysis on functionalities and security features of Internet of Things related protocols. *Wirel. Netw.* **2022**, *28*, 2857–2887. [CrossRef]
52. Thakor, V.A.; Razzaque, M.A.; Khandaker, M.R.A. Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities. *IEEE Access* **2021**, *9*, 28177–28193. [CrossRef]
53. Rao, V.; Prema, K.V. A review on lightweight cryptography for Internet-of-Things based applications. *J. Ambient Intell. Humaniz. Comput.* **2021**, *12*, 8835–8857. [CrossRef]
54. Abusukhon, A.; AlZu'bi, S. New Direction of Cryptography: A Review on Text-to-Image Encryption Algorithms Based on RGB Color Value. In Proceedings of the 2020 Seventh International Conference on Software Defined Systems, SDS 2020, Paris, France, 20–23 April 2020; pp. 235–239. [CrossRef]
55. Christensen, C. Review of History of Cryptography and Cryptanalysis by John Dooley. *Cryptologia* **2019**, *43*, 536–538. [CrossRef]
56. Simmons, G.J. Symmetric and Asymmetric Encryption. *ACM Comput. Surv.* **1979**, *11*, 305–330. [CrossRef]
57. Lempel, A. Cryptology in Transition. *ACM Comput. Surv.* **1979**, *11*, 285–303. [CrossRef]
58. Jimale, M.A.; Z'aba, M.R.; Kiah, M.L.M.; Idris, M.Y.I.B.; Jamil, N.; Mohamad, M.S.; Rohmad, M.S. Authenticated Encryption Schemes: A Systematic Review. *IEEE Access* **2022**, *10*, 14739–14766. [CrossRef]
59. Alenezi, M.N.; Alabdulrazzaq, H.K.; Mohammad, N.Q. Symmetric Encryption Algorithms: Review and Evaluation Study. *Int. J. Commun. Netw. Inf. Secur.* **2020**, *12*. [CrossRef]
60. Diffie, W.; Hellman, M. New Directions in Cryptography. *IEEE Trans. Inf. Theor.* **2006**, *22*, 644–654. [CrossRef]
61. Fleischhacker, N.; Larsen, K.G.; Simkin, M. Property-Preserving Hash Functions from Standard Assumptions. Cryptology ePrint Archive, Report 2021/793. 2021. Available online: https://ia.cr/2021/793 (accessed on: 18 October 2022).
62. Kim, H.; Kim, D.; Yi, O.; Kim, J. Cryptanalysis of hash functions based on blockciphers suitable for IoT service platform security. *Multim. Tools Appl.* **2019**, *78*, 3107–3130. [CrossRef]
63. Rao, P.M.; Deebak, B. Security and privacy issues in smart cities/industries: Technologies, applications, and challenges. *J. Ambient. Intell. Humaniz. Comput.* **2022**. [CrossRef]
64. Attkan, A.; Ranga, V. Cyber-physical security for IoT networks: A comprehensive review on traditional, blockchain and artificial intelligence based key-security. *Complex Intell. Syst.* **2022**, *8*, 3559–3591. [CrossRef]
65. Hoang, T.M.; Van Chien, T.; Van Luong, T.; Chatzinotas, S.; Ottersten, B.; Hanzo, L. Detection of Spoofing Attacks in Aeronautical Ad-Hoc Networks Using Deep Autoencoders. *IEEE Trans. Inf. Forensics Secur.* **2022**, *17*, 1010–1023. [CrossRef]
66. Kumari, A.; Kumar, V.; Abbasi, M.Y.; Kumari, S.; Chaudhary, P.; Chen, C.M. CSEF: Cloud-Based Secure and Efficient Framework for Smart Medical System Using ECC. *IEEE Access* **2020**, *8*, 107838–107852. [CrossRef]

67. Sivasankari, N.; Kamalakkannan, S. Detection and prevention of man-in-the-middle attack in iot network using regression modeling. *Adv. Eng. Softw.* **2022**, *169*, 103126. [CrossRef]
68. Vinoth, R.; Deborah, L.J. An efficient key agreement and authentication protocol for secure communication in industrial IoT applications. *J. Ambient. Intell. Humaniz. Comput.* **2021**. [CrossRef]
69. Vinoth, R.; Deborah, L.J.; Vijayakumar, P.; Kumar, N. Secure Multifactor Authenticated Key Agreement Scheme for Industrial IoT. *IEEE Internet Things J.* **2021**, *8*, 3801–3811. [CrossRef]
70. Nyangaresi, V.O.; Rodrigues, A.J.; Abeka, S.O. Secure Algorithm for IoT Devices Authentication. In *Industry 4.0 Challenges in Smart Cities*; Springer: Berlin/Heidelberg, Germany, 2023; pp. 1–22.
71. Far, H.A.N.; Bayat, M.; Das, A.K.; Fotouhi, M.; Pournaghi, S.M.; Doostari, M. LAPTAS: Lightweight anonymous privacy-preserving three-factor authentication scheme for WSN-based IIoT. *Wirel. Netw.* **2021**, *27*, 1389–1412. [CrossRef]
72. Guan, A.; Chen, C.M. A Novel Verification Scheme to Resist Online Password Guessing Attacks. *IEEE Trans. Dependable Secur. Comput.* **2022**, *19*, 4285–4293. [CrossRef]
73. Pushpa, S.X.; Raja, S. Elliptic curve cryptography based authentication protocol enabled with optimized neural network based DoS mitigation. *Wirel. Pers. Commun.* **2022**, *124*, 1–25. [CrossRef]
74. Nashwan, S. Analysis of the Desynchronization Attack Impact on the E2EA Scheme. *Comput. Syst. Sci. Eng.* **2022**, *41*, 625–644. [CrossRef]
75. Liu, J.; Liu, L.; Liu, Z.; Lai, Y.; Qin, H.; Luo, S. WSN node access authentication protocol based on trusted computing. *Simul. Model. Pract. Theory* **2022**, *117*, 102522. [CrossRef]
76. Hameed, K.; Garg, S.; Amin, M.B.; Kang, B.; Khan, A. A context-aware information-based clone node attack detection scheme in Internet of Things. *J. Netw. Comput. Appl.* **2022**, *197*, 103271. [CrossRef]
77. ul haq, I.; Wang, J.; Zhu, Y.; Maqbool, S. An efficient hash-based authenticated key agreement scheme for multi-server architecture resilient to key compromise impersonation. *Digit. Commun. Netw.* **2021**, *7*, 140–150. . [CrossRef]
78. Kayalvizhi, M.; Ramamoorthy, S. Review of Security Gaps in Optimal Path Selection in Unmanned Aerial Vehicles Communication. In *Proceedings of the Sustainable Advanced Computing*; Aurelia, S., Hiremath, S.S., Subramanian, K., Biswas, S.K., Eds.; Springer: Singapore, 2022; pp. 439–451.
79. Szymoniak, S. Using A Security Protocol To Protect Against False Links. In *Proceedings of the Moving Technology Ethics at the Forefront of Society, Organisations and Governments*; Universidad de La Rioja: La Rioja, Spain, 2021; pp. 513–525.
80. Chen, Y.; Chen, J. Anonymous and provably secure authentication protocol using self-certified cryptography for wireless sensor networks. *Multimed. Tools Appl.* **2021**, *80*, 15291–15313. [CrossRef]
81. Rasslan, M.; Nasreldin, M.M.; Aslan, H.K. Ibn Sina: A patient privacy-preserving authentication protocol in medical internet of things. *Comput. Secur.* **2022**, *119*, 102753. [CrossRef]
82. Masud, M.; Gaba, G.S.; Kumar, P.; Gurtov, A. A user-centric privacy-preserving authentication protocol for IoT-AmI environments. *Comput. Commun.* **2022**, *196*, 45–54. [CrossRef]
83. Rejeb, A.; Rejeb, K.; Simske, S.J.; Keogh, J.G. Blockchain technology in the smart city: A bibliometric review. *Qual. Quant.* **2022**, *56*, 2875–2906. [CrossRef] [PubMed]
84. Aljofey, A.; Rasool, A.; Jiang, Q.; Qu, Q. A Feature-Based Robust Method for Abnormal Contracts Detection in Ethereum Blockchain. *Electronics* **2022**, *11*, 2937. [CrossRef]
85. Chander, B.; Gopalakrishnan, K. A secured and lightweight RFID-tag based authentication protocol with privacy-preserving in Telecare medicine information system. *Comput. Commun.* **2022**, *191*, 425–437. [CrossRef]
86. Dewan, C.; Ganesh Kumar, T.; Gupta, S. Comparative Study of Various Authentication Schemes in Tele Medical Information System. In *Applications of Computational Methods in Manufacturing and Product Design*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 557–564.
87. Zuo, J.; Feng, J.; Gameiro, M.G.; Tian, Y.; Liang, J.; Wang, Y.; Ding, J.; He, Q. RFID-based sensing in smart packaging for food applications: A Review. *Future Foods* **2022**, *2022*, 100198. [CrossRef]
88. Gulafshan, G.; Amara, S.; Kumar, R.; Khan, D.; Fariborzi, H.; Massoud, Y. Bitwise Logical Operations in VCMA-MRAM. *Electronics* **2022**, *11*, 2805. [CrossRef]
89. Soni, M.; Singh, D.K. Privacy-preserving secure and low-cost medical data communication scheme for smart healthcare. *Comput. Commun.* **2022**, *194*, 292–300. [CrossRef]
90. Wang, X.; Fan, K.; Yang, K.; Cheng, X.; Dong, Q.; Li, H.; Yang, Y. A new RFID ultra-lightweight authentication protocol for medical privacy protection in smart living. *Comput. Commun.* **2022**, *186*, 121–132. [CrossRef]
91. Prasanalakshmi, B.; Murugan, K.; Srinivasan, K.; Shridevi, S.; Shamsudheen, S.; Hu, Y.C. Improved authentication and computation of medical data transmission in the secure IoT using hyperelliptic curve cryptography. *J. Supercomput.* **2022**, *78*, 361–378. [CrossRef]
92. Priya, S.; Karthigaikumar, P.; Teja, N.R. FPGA implementation of AES algorithm for high speed applications. *Analog Integr. Circuits Signal Process.* **2022**, *112*, 115–125. [CrossRef]
93. Palka, P.; Perez, R.A.; Fang, T.; Saniie, J. Design Flow of Blowfish Symmetric-Key Block Cipher on FPGA. In Proceedings of the 2022 IEEE International Conference on Electro Information Technology (eIT), Mankato, MN, USA, 19–21 May 2022; pp. 193–197.
94. Koblitz, N. Hyperelliptic cryptosystems. *J. Cryptol.* **1989**, *1*, 139–150. [CrossRef]

95. Nourozi, V.; Rahmati, F.; Tafazolian, S. The a-number of certain hyperelliptic curves. *Iran. J. Sci. Technol. Trans. Sci.* **2022**, *46*, 1235–1239. [CrossRef]
96. Chen, C.M.; Chen, Z.; Kumari, S.; Lin, M.C. LAP-IoHT: A Lightweight Authentication Protocol for the Internet of Health Things. *Sensors* **2022**, *22*, 5401. [CrossRef]
97. Agrahari, A.K.; Varma, S.; Venkatesan, S. Two factor authentication protocol for IoT based healthcare monitoring system. *J. Ambient. Intell. Humaniz. Comput.* **2022**. [CrossRef]
98. Tanveer, M.; Alkhayyat, A.; Chaudhry, S.A.; Zikria, Y.B.; Kim, S.W. REAS-TMIS: Resource-Efficient Authentication Scheme for Telecare Medical Information System. *IEEE Access* **2022**, *10*, 23008–23021. [CrossRef]
99. Beierle, C.; Biryukov, A.; dos Santos, L.C.; Großschädl, J.; Perrin, L.; Udovenko, A.; Velichkov, V.; Wang, Q. Lightweight AEAD and hashing using the sparkle permutation family. *IACR Trans. Symmetric Cryptol.* **2020**, *2020*, 208–261. [CrossRef]
100. Pardeshi, M.S.; Sheu, R.K.; Yuan, S.M. Hash-Chain Fog/Edge: A Mode-Based Hash-Chain for Secured Mutual Authentication Protocol Using Zero-Knowledge Proofs in Fog/Edge. *Sensors* **2022**, *22*, 607. [CrossRef]
101. Iqbal, U.; Tandon, A.; Gupta, S.; Yadav, A.R.; Neware, R.; Gelana, F.W. A Novel Secure Authentication Protocol for IoT and Cloud Servers. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 1–17. [CrossRef]
102. Wu, T.Y.; Wang, L.; Guo, X.; Chen, Y.C.; Chu, S.C. SAKAP: SGX-Based Authentication Key Agreement Protocol in IoT-Enabled Cloud Computing. *Sustainability* **2022**, *14*, 11054. [CrossRef]
103. Wu, T.Y.; Guo, X.; Chen, Y.C.; Kumari, S.; Chen, C.M. SGXAP: SGX-Based Authentication Protocol in IoV-Enabled Fog Computing. *Symmetry* **2022**, *14*, 1393. [CrossRef]
104. Costan, V.; Devadas, S. Intel SGX Explained. *IACR Cryptol. ePrint Arch.* **2016**, *2016*, 86.
105. Zhao, X.; Li, D.; Li, H. Practical Three-Factor Authentication Protocol Based on Elliptic Curve Cryptography for Industrial Internet of Things. *Sensors* **2022**, *22*, 7510. [CrossRef] [PubMed]
106. Yi, F.; Zhang, L.; Xu, L.; Yang, S.; Lu, Y.; Zhao, D. WSNEAP: An Efficient Authentication Protocol for IIoT-Oriented Wireless Sensor Networks. *Sensors* **2022**, *22*, 7413. [CrossRef] [PubMed]
107. Maes, R.; Verbauwhede, I. Physically unclonable functions: A study on the state of the art and future research directions. In *Towards Hardware-Intrinsic Security: Foundations and Practice*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 3–37.
108. Luo, L.; Guo, D.; Ma, R.T.; Rottenstreich, O.; Luo, X. Optimizing bloom filter: Challenges, solutions, and comparisons. *IEEE Commun. Surv. Tutor.* **2018**, *21*, 1912–1949. [CrossRef]
109. Panda, S.; Mondal, S.; Kumar, N. SLAP: A Secure and Lightweight Authentication Protocol for machine-to-machine communication in industry 4.0. *Comput. Electr. Eng.* **2022**, *98*, 107669. [CrossRef]
110. Zhang, Y.; Luo, Y.; Chen, X.; Tong, F.; Xu, Y.; Tao, J.; Cheng, G. A Lightweight Authentication Scheme Based on Consortium Blockchain for Cross-Domain IoT. *Secur. Commun. Netw.* **2022**, *2022*, 9686049. [CrossRef]
111. Wang, X.; Gu, C.; Wei, F.; Lu, S.; Li, Z. A Certificateless-Based Authentication and Key Agreement Scheme for IIoT Cross-Domain. *Secur. Commun. Netw.* **2022**, *2022*, 3693748. [CrossRef]
112. Li, Y.; Xu, M.; Xu, G. Blockchain-based mutual authentication protocol without CA. *J. Supercomput.* **2022**, *78*, 17261–17283. [CrossRef]
113. Wan, C.; Zhang, J. Identity-based key management for wireless sensor networks using lagrange interpolation. *Secur. Commun. Netw.* **2016**, *9*, 3713–3723. [CrossRef]
114. LaMacchia, B.; Lauter, K.; Mityagin, A. Stronger security of authenticated key exchange. In Proceedings of the International Conference on Provable Security, Wollongong, Australia, 1–2 November 2007; Springer: Berlin/Heidelberg, Germany, 2007; pp. 1–16.
115. Ryu, J.; Son, S.; Lee, J.; Park, Y.; Park, Y. Design of Secure Mutual Authentication Scheme for Metaverse Environments Using Blockchain. *IEEE Access* **2022**, *10*, 98944–98958. [CrossRef]
116. Hajian, R.; Haghighat, A.; Erfani, S.H. A Secure Anonymous D2D Mutual Authentication and Key Agreement Protocol for IoT. *Internet Things* **2022**, *18*, 100493. [CrossRef]
117. Gong, X.; Feng, T. Lightweight Anonymous Authentication and Key Agreement Protocol Based on CoAP of Internet of Things. *Sensors* **2022**, *22*, 7191. [CrossRef] [PubMed]
118. Islam, M.; Khan, Z.; Alsaawy, Y. A framework for harmonizing internet of things (IoT) in cloud: Analyses and implementation. *Wirel. Netw.* **2021**, *27*, 4331–4342. [CrossRef]
119. Nyangaresi, V.O. ECC based authentication scheme for smart homes. In Proceedings of the 2021 International Symposium ELMAR, Zadar, Croatia, 13–15 September 2021; pp. 5–10.
120. CPN Tools. Available online: http://www.cpntools.org/ (accessed on 10 October 2022).
121. Chen, C.M.; Li, X.; Liu, S.; Wu, M.E.; Kumari, S. Enhanced authentication protocol for the Internet of Things environment. *Secur. Commun. Netw.* **2022**, *2022*, 8543894. [CrossRef]
122. Safkhani, M.; Rostampour, S.; Bendavid, Y.; Sadeghi, S.; Bagheri, N. Improving RFID/IoT-based generalized ultra-lightweight mutual authentication protocols. *J. Inf. Secur. Appl.* **2022**, *67*, 103194. [CrossRef]
123. Khorasgani, A.A.; Sajadieh, M.; Yazdani, M.R. Novel lightweight RFID authentication protocols for inexpensive tags. *J. Inf. Secur. Appl.* **2022**, *67*, 103191. [CrossRef]
124. Alam, I.; Kumar, M. A novel protocol for efficient authentication in cloud-based IoT devices. *Multimed. Tools Appl.* **2022**, *81*, 13823–13843. [CrossRef]

125. Sakkari, D.S.; ulla, M.M. Review on Insight into Elliptic Curve Cryptography. In *Modern Approaches in Machine Learning & Cognitive Science: A Walkthrough*; Springer: Cham, Switzerland, 2022; pp. 81–93.
126. Mirsaraei, A.G.; Barati, A.; Barati, H. A secure three-factor authentication scheme for IoT environments. *J. Parallel Distrib. Comput.* **2022**, *169*, 87–105. [CrossRef]
127. Saqib, M.; Jasra, B.; Moon, A.H. A lightweight three factor authentication framework for IoT based critical applications. *J. King Saud Univ.-Comput. Inf. Sci.* **2022**, *34*, 6925–6937. [CrossRef]
128. Hu, B.; Tang, W.; Xie, Q. A two-factor security authentication scheme for wireless sensor networks in IoT environments. *Neurocomputing* **2022**, *500*, 741–749. [CrossRef]
129. Haseeb-ur Rehman, R.M.A.; Liaqat, M.; Aman, A.H.M.; Almazroi, A.A.; Hasan, M.K.; Ali, Z.; Ali, R.L. LR-AKAP: A Lightweight and Robust Security Protocol for Smart Home Environments. *Sensors* **2022**, *22*, 6902. [CrossRef] [PubMed]
130. Kumar, V.; Kumar, R.; Jangirala, S.; Kumari, S.; Kumar, S.; Chen, C.M. An enhanced RFID-based authentication protocol using PUF for vehicular cloud computing. *Secur. Commun. Netw.* **2022**, *2022*, 8998339. [CrossRef]
131. Gupta, D.S.; Ray, S.; Singh, T.; Kumari, M. Post-quantum lightweight identity-based two-party authenticated key exchange protocol for Internet of Vehicles with probable security. *Comput. Commun.* **2022**, *181*, 69–79. [CrossRef]
132. Garg, S.; Nayak, S.; Bavani Sankar, A.; Maity, S. Applications of Identity-Based Cryptography in Smart Home and Healthcare: A Recent Review. In *Cyber Security in Intelligent Computing and Communications*; Springer: Singapore, 2022; pp. 227–241.
133. Zheng, Z. Lattice-Based Cryptography. In *Modern Cryptography Volume 1*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 253–351.
134. Zhang, G.; Zhao, X.; Chen, M.; Ma, S. Efficient privacy protection authentication protocol for vehicle network in 5G. *Concurr. Comput. Pract. Exp.* **2022**, e7247. [CrossRef]
135. Bera, B.; Vangala, A.; Das, A.K.; Lorenz, P.; Khan, M.K. Private blockchain-envisioned drones-assisted authentication scheme in IoT-enabled agricultural environment. *Comput. Stand. Interfaces* **2022**, *80*, 103567. [CrossRef]
136. Tanveer, M.; Alkhayyat, A.; Naushad, A.; Kumar, N.; Alharbi, A.G. RUAM-IoD: A Robust User Authentication Mechanism for the Internet of Drones. *IEEE Access* **2022**, *10*, 19836–19851. [CrossRef]
137. Tanveer, M.; Shah, H.; Chaudhry, S.A.; Naushad, A. PASKE-IoD: Privacy-protecting authenticated key establishment for Internet of Drones. *IEEE Access* **2021**, *9*, 145683–145698. [CrossRef]
138. Tanveer, M.; Khan, A.U.; Kumar, N.; Hassan, M.M. RAMP-IoD: A robust authenticated key management protocol for the Internet of Drones. *IEEE Internet Things J.* **2021**, *9*, 1339–1353. [CrossRef]
139. Tanveer, M.; Nguyen, T.; Ahmad, M.; Abdei-Latif, A. Towards A Secure and Computational Framework for Internet of Drones Enabled Aerial Computing. *IEEE Trans. Netw. Sci. Eng.* **2022**. [CrossRef]
140. Javed, S.; Khan, M.A.; Abdullah, A.M.; Alsirhani, A.; Alomari, A.; Noor, F.; Ullah, I. An Efficient Authentication Scheme Using Blockchain as a Certificate Authority for the Internet of Drones. *Drones* **2022**, *6*, 264. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.