energies

MDPI

Review

A Survey on Key Management and Authentication Approaches in Smart Metering Systems

Mohamed S. Abdalzaher [1,*], Mostafa M. Fouda [2], Ahmed Emran [3], Zubair Md Fadlullah [4,*] and Mohamed I. Ibrahem [5,6]

1 Department of Seismology, National Research Institute of Astronomy and Geophysics, Cairo 11421, Egypt
2 Department of Electrical and Computer Engineering, College of Science and Engineering, Idaho State University, Pocatello, ID 83209, USA
3 Department of Electrical Engineering, Al-Azhar University, Cairo 11651, Egypt
4 Department of Computer Science, Western University, London, ON N6A 5B7, Canada
5 Department of Cyber Security Engineering, George Mason University, Fairfax, VA 22030, USA
6 Department of Electrical Engineering, Faculty of Engineering at Shoubra, Benha University, Cairo 11672, Egypt
* Correspondence: msabdalzaher@nriag.sci.eg (M.S.A.); zfadlullah@ieee.org (Z.M.F.)

Abstract: The implementation of the smart grid (SG) and cyber-physical systems (CPS) greatly enhances the safety, reliability, and efficiency of energy production and distribution. Smart grids rely on smart meters (SMs) in converting the power grids (PGs) in a smart and reliable way. However, the proper operation of these systems needs to protect them against attack attempts and unauthorized entities. In this regard, key-management and authentication mechanisms can play a significant role. In this paper, we shed light on the importance of these mechanisms, clarifying the main efforts presented in the context of the literature. First, we address the main intelligent attacks affecting the SGs. Secondly, the main terms of cryptography are addressed. Thirdly, we summarize the common proposed key-management techniques with a suitable critique showing their pros and cons. Fourth, we introduce the effective paradigms of authentication in the state of the art. Fifth, the common two tools for verifying the security and integrity of protocols are presented. Sixth, the relevant research challenges are addressed to achieve trusted smart grids and protect their SMs against attack manipulations and unauthorized entities with a future vision. Accordingly, this survey can facilitate the efforts exerted by interested researchers in this regard.

Keywords: smart grid; key management; smart meter; advanced metering infrastructure; cyberphysical system

Citation: Abdalzaher, M.S.; Fouda, M.M.; Emran, A.; Fadlullah, Z.M.; Ibrahem, M.I. A Survey on Key Management and Authentication Approaches in Smart Metering Systems. *Energies* **2023**, *16*, 2355. https://doi.org/10.3390/en16052355

Academic Editor: Md Rasheduzzaman

Received: 6 February 2023
Revised: 25 February 2023
Accepted: 27 February 2023
Published: 1 March 2023

1. Introduction

Smart grids (SGs) are known as the new and upcoming systems that generate power in order to increase the flow of electronic communication. SGs can improve and alter the processing capacity using the current state of power grids (PGs) and smart cities [1]. It can also provide demand–response features for third parties and distributed intelligence [2], supplied renewable energy [3–7], and upgraded power grid (PG) elements to improve response time [8]. Generally speaking, SGs have three main components: power distribution, advanced metering, and microgrid systems [9]. In this regard, smart metering systems find their way to facilitate data observation and its transfer. Along with these types of contributions, SGs uphold three main security principles from the confidentiality, integrity, and availability triad. Accordingly, SGs can enforce confidentiality by preventing unauthorized access to the data flow within the current state of PGs. For integrity, SGs can restrict the modification of the grid circuitry within the current-state pwer grid (PG). Lastly, SGs can ensure that the data stored will be easily accessible for authorized end users [10].

Generally speaking, the SG is characterized by a two-way flow of information and electricity, and as this technology continues to advance and becomes more prevalent in day-to-day activity, security is of the utmost importance [8,11–14]. SG technology aims to make the PG much more efficient than ever before with solutions to bolster resiliency, improve distribution, and benefit the consumer, but with it there comes a number of security and privacy concerns [15–18]. In the advanced metering infrastructure (AMI), consumers have smart meters (SMs), which are intelligent, solid-state, programmable devices that can perform many functions [6,19,20]. Some of these include reporting electricity production or consumption back to the operators, and they serve to provide information on outages, bidirectional metering, and billing in a timely interval [17,21–23]. For many users, SMs are a major privacy concern because unlike in traditional meters where readings would be done manually and on a monthly basis, readings are automated and are transmitted via wireless links [24]. Indeed, the foundation of the SG's packet relaying is a two-way communication infrastructure, either wired or wireless. Wired networks, such as power line communication (PLC), are used to connect substations and control centers [25,26]. The risk here is that attackers may be able to intercept and access this information if it is not properly secured, so cryptographic means are utilized to encrypt these communications [16,27–30].

Due to the constant activity of SMs, active tampering detection or prevention must also be active in SMs to get precise notification when issues or vulnerabilities arise [31–35]. Moreover, smart metering and power optimization are among the main targets in SMs [36–39]. Different proposed schemes have been proposed to thwart these issues. Many of them focus on providing data integrity and protecting confidentiality because of their sensitivity in AMI networks [40]. It is worth mentioning that the high dependence on the exchange of information between the networks leaves SGs potentially open to threats and vulnerabilities due to the lack of security when information is being transmitted [8]. Different security methodologies have been effectively employed for privacy preservation in SGs such as machine learning (ML). ML has played a significant role in different research directions and research trends including the security front and preservation of human lives [41–50]. More particularly, ML has contributed to mitigating SM security issues. Moreover, the effective use of optimization techniques can contribute to prolonging the SM lifetime [51]. For the encryption of meter data, the authors in [52] suggested a localization-based key-management system. Data are encrypted by using a random key index, and the key is assigned to the meter's coordinate. A dependable third party controls and distributes the encryption keys. A technique based on received signal strength and the highest likelihood estimator is suggested for the localization of the meter. At the control center, the packets are decrypted by using a key that is mapped to the key index and coordinates for the meter.

Indeed, there must be a proper key-management system [53]. Traditional key-management schemes involve the generation, exchange, storage, update, and removal of keys and use either public key infrastructure (PKI) for the key establishment or symmetric key management and in order for components in the SG to communicate securely, proper session keys must be utilized [54]. In the PKI system, the public key certificate is gained from the trusted certificate authority's (CA) signature, which is associated with the device's identity and public key. The SM then can register its public key and ID with the CA. In PKI, the user can use the CA's public key to verify the signature and thus authenticate if the certificate is legitimate. In symmetric key schemes, the secret keys are either stored in secure locations or created by a trusted third party, and this key is shared to perform encryption and decryption functions. In most consumer settings, SMs communicate with each other and distributors over a home area network (HAN) to make decisions toward the grid and to report back to the operators, but these communications remain at risk of being exposed, so they must be encrypted [55–57]. Some of the biggest issues in key management include transporting keys in a secure manner (in a symmetric key configuration) as well as the excessive overhead involved, which makes many of these systems impractical. In addition, there is no single key-management infrastructure, and each scheme must be tailored to meet the network and security requirements of various systems [58].

Regarding authentication in SGs, SMs are an important entity because there is a need for reliability pertaining to data networking in SG security. For example, the memory systems within SMs have vulnerabilities against spoofing attacks and need to maintain power to transmit active tamper detection and prevention circuitry [8]. There are two solutions to fix this problem. First, a hardware-oriented authentication for AMI has been suggested by the ring oscillator physically unclonable functions (ROPUFs). The ROPUFs can protect the AMI systems from threats of data integrity and confidentiality by developing keys from the configuration of the integrated circuit or field programmable gate array (FPGA) chip within the SM [8]. The other solution is to implement a three-way factor authentication method that will improve the efficiency of renewable energy-based SGs.

One of the relevant research challenges that occurred with the hardware-oriented authentication scheme for AMI was suggesting the implementation of asymmetric key cryptography. The Diffie–Hellman Key Exchange was supposed to act as a minor method for authenticating a message through SMs with a shared session key, but the problem stemmed from the top-level overhead required in the certificate management [8]. Another relevant research challenge faced with the hardware-oriented authentication scheme for AMI was suggesting the implementation of a novel key-management scheme (KMS) for the AMI system. This type of key management will utilize the key graph and execute key management modes, such as unicast, broadcast, and multicast. The problem with this key management is that it will experience vulnerabilities to spoofing and modification attacks because of invasive memory [8]. The last relevant research challenge was a recommendation to merge physical key generation (PKG) and physically unclonable functions (PUFs) through a wireless channel to secure connection between end users and the original equipment manufacturer servers. The main problem is that there is no finding explaining the real-time demands in the subsystems when it comes to computation and secure communication [8]. Moreover, it is vulnerable to the risk of being affected by man-in-the-middle attacks [59]. In an attempt to mitigate man-in-the-middle attacks, a trusted anchor was proposed to assist in establishing a key between SMs and service providers.

These schemes were tested to develop a method of key distribution for SGs so that SMs and service providers could have the ability to authenticate with one another through a session key and have secure communication. The problem is that this method is vulnerable to ephemeral secret leakage and privileged-insider attacks and gives weak confidentiality regarding end-user credentials in SMs [59]. Due to the fact that SMs can contribute to several applications [60–63], sufficient mitigation of the attack manipulations impacting the SMs, taking into consideration contemporary technology, can reduce the disastrous effects, whether on the level of human lives or the level of infrastructure [64–67].

The major contributions of the paper are as follows.

- We highlight the significance of the common key management and authentication approaches by outlining the primary initiatives discussed in the state of the art.
- We address the fundamental concepts of cryptography that are involved in SGs.
- We discuss the primary intelligent attacks affecting the operation and smooth functionality of the SGs.
- We provide an overview of the most frequently suggested key-management strategies together with a fair evaluation outlining their benefits and drawbacks.
- We introduce the most recent and efficient authentication models.
- The common two tools for confirming the security and integrity of protocols are highlighted.
- In an effort to create reliable SGs and safeguard their SMs from attack manipulations and unauthorized entities, pertinent research challenges are addressed to the main key-management and authentication methodologies with a vision for future work.
- In light of these points, this paper can aid motivated researchers' work in this area.

The rest of the paper is organized as follows. Section 2 clarifies the motivation of the present study. Section 3 focuses on the main definitions of cryptography that are involved in SGs. Then, the common SGs attacks are discussed in Section 4. Section 5 presents the com-

mon key-management techniques. Afterward, the authentication schemes are addressed in Section 6. The verification tools are then considered in Section 7. Finally, the paper is concluded with a vision for future work and open research challenges in Section 8.

2. Motivation

Cryptography has made significant contributions to the confidentiality, integrity, and authenticity of data in cyberphysical systems, such as control data and personally identifiable information. The integrity of any encryption system is dependent on the security of the cryptographic keys used to encrypt and decrypt data, so when a key becomes compromised, the entire system it was designed for is no longer secure. The key issue with SMs is that the recorded data is often highly detailed, including information on specific appliances and the time at which they were used. One major concern if this information becomes disclosed is that criminals would be able to plan a burglary given that they know what types of appliances a consumer has based on their electric signatures, and they may be able to learn their daily habits, including when no one will be home. Expanding on the last point, it is a violation of privacy if an outsider can observe your daily routine and habits, so it is crucial that this information is properly secured and only those meant to can view it.

In Ref. [68], the authors have only considered the logical key hierarchy mechanism (LKH) for group security in communication systems in their study, which is only a type of key-management mechanism. In Ref. [69], the authors addressed the importance of key-management systems from only the point of view of AMI for SGs. However, in creating a secure key-management system for cyberphysical systems, the schemes shall be both resilient and lightweight for the current infrastructure in the field because devices such as SMs have very limited resources and must be properly accounted for. It is also important to include common mitigation techniques for different types of attacks on symmetric and asymmetric key systems such as brute force attacks or cryptanalysis. The key-generation process must be complex enough to avoid being guessed, and the encryption algorithm should not contain a fundamental flaw in the mathematical theory the system is based upon because, with the proper resources, an attacker may be able to decrypt messages without the key or potentially not even know the algorithm. The primary criteria that must be considered is a system that is secure, fast, noncomputationally intensive, and scalable for a large number of devices in order to provide ample security while also being practical. In light of what was mentioned, it motivates us to bring attention to the importance of SG and SM security.

Unlike other studies, this study considers the common key-management and authentication mechanisms, taking into consideration intelligent SG attacks. Moreover, it also highlights the roles and functionality of the two commonly utilized verification tools of protocols utilized in this regard. Finally, the study shed light on relevant research problems addressed to the primary key-management and authentication approaches with a vision for future work to build trustworthy SGs and protect their SMs from attack manipulations and unauthorized entities.

3. Important Terms and Definitions in Cryptography

For secure communication between the involved entities in SGs, it is important to define several key terms that contribute to developing efficient security solutions.

3.1. Encryption

It is a process to convert information into a cipher with the use of keys to maintain the confidentiality of the information being encrypted. To have a good encryption algorithm, there are several criteria that the algorithm must fulfill.

- Efficiency: The operations used in encryption and decryption algorithms must be easy to implement on hardware and software.

- Resistance to Statistical Analysis: Encryption algorithms must destroy any statistical structure in the plain-text data
  - Diffusion: A change of a single bit in the plain-text string will cause a number of bits in the cipher text string to be changed.
  - Confusion: A change of a single bit in the encryption key will cause a number of bits in the cipher text string to be changed.
- Resistance to Brute Force Attacks: The algorithm must be able to prevent the attacker from computing and testing precomputed encryption keys.
- Resistance to Side Channel Attacks: This is where attacks exploit loopholes in the environment of the implementation. An example of this is a timing attack in which the attacker analyzes the computing time of certain operations that could help the attacker obtain useful information about the encryption key.

3.2. Symmetrical Algorithm

Symmetrical algorithm: In this key system, the same key is used for encryption as well as decryption. There are risks associated with the initial transfer of the key (such as it being intercepted), but it can be used to safely encrypt or decrypt data after it has been successfully transferred.

- AES: Advanced Encryption Standard is a form of a symmetric-key algorithm that is a block cipher, but its encryption and decryption are not symmetrical. To complete its operations, AES divides the plain-text string into 128-bit blocks and can use encryption keys of three different key lengths: 16-byte long (128 bit), 24-byte long (192 bit), or 32-byte long (256 bit). These three variants of AES all have the same encryption and decryption structures but differ only in the number of rounds, wherein each round uses a different round key. This algorithm takes the plain text and does a variety of operations such as substitute, shift, mix, add round key, and invert over multiple rounds and produces a cipher text able to resist differential cryptoanalysis and linear cryptoanalysis. For added security, use of a 128-bit key makes it resistant to brute force attacks and there have been no methods discovered that are efficient enough to be considered serious threats to AES.

3.3. Asymmetrical Algorithm

Asymmetric key encryption uses one key to encrypt and a different key to decrypt. The key pairs, known as the public and private keys, allow for risk-free key exchanges. Both systems share public keys but do not share private keys. The public key is used for encryption and generates cipher text; however, only the private key can decrypt the cipher text. This is not always the case, as the private key may also create cipher text depending on the scheme. If done this way, this allows for nonrepudiation, which entails that the sender cannot claim that they did not encode a message, and all recipients are aware that the message is genuine. This property is also known as a cryptographic signature.

- Diffie–Hellman: This is a public-key algorithm and its purpose is to allow two users to exchange a key in a secure manner that can then be used for subsequent symmetric encryption of messages. Its effectiveness depends on the difficulty of computing discrete logarithms because it is difficult to solve x from $y = a^x mod p$, $x < p$. The fundamental theory behind this is that given p, g, and $g^a mod p$, it is not feasible to compute private key a.

3.4. Hashing

Hash functions are functions that take a specific set of data and turn it into a representation of the data. For example, when a 500-MB file is hashed, rather than simply displaying the information of the file, a piece of "reference data" is used to show that the original information exists. When that file is referenced, instead of accessing the full 500-MB file, the stand-in reference point is used. The implementation of hash models makes systems

more secure by making it more difficult to access true data. It also makes systems faster, because when things are referenced, they are not actually being referenced as their whole true value of data but a smaller representation of that data.

Hashing utilizes a methodology for data transformation between entities, called a one-way function. The idea of a one-way function is the transformation of an input into a second input without any way to reverse the transition. These hash models not only make communication faster but increase the security of information transferred during communication. One-way hash models are utilized to make authentication functions and models that cannot be exploited by attacks like man-in-the-middle attacks.

To sum up, hashing is a technique by which to ensure the integrity of any arbitrary length data by converting it into a fixed-length string. To do this, a hashing function is used and returns values called hash values or simply hashes. There are several properties required for a hash function.

- It should be easy to calculate the hash value given the message m and be able to calculate $h(m)$.
- The function should only work one way where $h(m)$ is easily calculated with m, but it is difficult to calculate m with $h(m)$.
- It must be weakly collision resistant, meaning that an attacker, given m_1, cannot produce another message m_2 with $h(m_1) = h(m_2)$.
- Additionally, it must fulfill strong collision resistance in which it is not possible for the hashes of two messages to be identical to one other: $(h(x) = h(y))$.

3.5. Elliptic Curve Cryptography

Elliptic curve cryptography (ECC) is a technique utilized to encrypt data and make it more secure. It is key-focused and is closely linked with the Rivest–Shamir–Adleman (RSA) cryptographic algorithm. ECC is an attempted improvement on RSA, attempting to make authentication more viable and guaranteed to be secure with fewer resources dedicated. This is an important aspect of security when it comes to devices that cannot handle a high level of overhead resource demand (such as phones, IoT devices, etc). ECC is utilized by cryptography functions in digital signatures and in pseudorandom number generators.

3.5.1. Elliptic Curve Discrete Log Problem

The original discrete log formula is $2^n \ mod \ a = b$, and the idea is for this equation to be complex and difficult to solve. This difficulty provides security to cryptographic functions that utilize it in its algorithms. However, as technology continues to improve, the problem becomes easier and easier to solve, destroying its security. In order to counteract this, cryptographic methods that implement it (like RSA) require a larger number of bits to continue to have the same level of security. This, as said before, increases the overhead of the systems that utilize it. The elliptic curve discrete log problem resolves this issue slightly, as the elliptic curve log problem equation is far more complex and thus requires fewer bits to utilize it to the fullest in a security context. This may only be a temporary solution to technological advancements causing cryptographic algorithms to become obsolete, as the speed at which processing power advances is not slowing down any time soon.

3.5.2. ECC Working Strategy

As its name suggests, ECC utilizes elliptic curves to create secure connections between pairs of keys in a public encryption function. Elliptic curves in math operate in a finite field and are based on the function $y^2 = x^3 + ax + b$ [70]. Elliptic curves have some characteristics that make them perfect for a cryptography function. One is horizontal symmetry, meaning that for any point found on the curve, it can be flipped over the x-axis and not change the curvature. A second interesting characteristic is that any line that is not vertical will only interact with the curve at three places at max. With that in mind, we consider the situation in which two points on a graph are "dotted" together (e.g., $A \cdot B = F$) to be given a third final point. In a cryptographic context, when given A and F the algorithm

must discover what B is, and this is difficult to accomplish, making it a functionally secure method [70].

3.5.3. ECC Desirability

As stated before, ECC looks to improve on the negatives of RSA that make it difficult to implement into devices, such as the the high demand for resources to make it viable and secure. For an RSA cryptographic function to be deemed secure, the bit length of the key should be 1024 bits. In comparison, in an elliptic curve function to achieve the same level of functional security would require a key length of only 160 bits. That is a drastically reduced number and greatly reduces the resources required to perform encryption securely. This reduced requirement in bits not only allows for less computationally capable devices like those linked with the Internet of things to perform the actions with little difficulty, but it also increases the speeds of the encryption transaction due to the algorithms being easier to handle with a smaller number of bits.

3.6. Bitwise Functions

Bitwise functions perform operations on binary strings, bit by bit. The result of a bitwise function will be one of two values. A 1 means true, and a 0 means false. Bitwise functions are used in low-level programming, in the transmission of messages, and more. It is worth mentioning that XOR bitwise functions are the main ones utilized for comparison. Moreover, hamming code is among the common codes employed in this regard.

3.6.1. XOR Bitwise Functions

Exclusive or (XOR) is a bitwise function. During logical operations, if two compared bits have a value of 1, then it returns a value of True. If there is no 1 present or both values return 1, the function will return False.

3.6.2. Hamming Code

Hamming code is a tool in telecommunications that handles miscommunication errors. In communication systems, hamming code is important, as it is expected for these systems to be error free or close to it [71]. High accuracy is a strict requirement in these systems and Hamming code makes that possible. As SMs deal with sensitive information, it is possibly dangerous if transmitted incorrectly, and it is pertinent that every piece of data that is transmitted and received be verified to be as accurate as possible. Hamming code is an algorithm that detects errors in binarily coded messages by using something referred to as "parity" bits. Parity bits are bits that are attached to the tail end of transmitted data and are used to verify the authenticity of the information received. The way the parity bits are dispersed in the data will reveal whether the data received is the expected relay sent out [72]. Hamming code detects these errors by comparing bit strings utilizing XOR bitwise functions (otherwise known as Modulo). Hamming code does increase the overhead requirements of a system [73]. Consequently, this can be a problem for systems that have a low amount of onboard RAM.

3.7. Merkle Trees

Merkle trees are data structures found in computer systems. Merkle trees utilize hash functions in order to accomplish some of its functionality. Merkle Trees increases the speed of the authentication of information, and this is beneficial when dealing with large data sets that need to be accessed.

Merkle Trees Desirability

It aimed to reduce the required strain on systems to carry out authentication and provide secure communication [8]. A Merkle hash tree takes all data and organizes it similarly to a literal tree with a trunk and branches stemming from it. Information on the branches originates from information at the trunk. For example, if there were three

branches (hash values $B1$, $B2$, and $B3$), the hash value of the trunk would be equal to $B1 + B2 + B3$. This method of information organization creates "redundancy" in data by reducing the amounts of steps and "new" data needed to access more information.

The implementation of asymmetric key cryptography into the hardware-oriented authentication scheme for AMI solved the issue regarding authentication but created another challenge. The number of resources necessary to carry out the asymmetric cryptography functions was too demanding for non-high-level systems. This led to the implementation of a new hashing technique that utilized the Merkle hash tree technique. This technology has proof of working and improving the security of authentication, as it has been utilized as a method of authentication in secure network transactions like cryptocurrency.

3.8. Hardware-Oriented Security

As technology continues to advance, the reliance on software security is becoming increasingly more dangerous. Prior to the increase in advancements, systems were not developed with specific cyber specifications in mind, thus making hardware a very easy access point into exploiting systems. A hardware-focused security approach aims to focus on decreasing the risk and attack vector of specific hardware components of a system. The implementation of software such as ROPUFs on a field programmable gate array (FPGA) allows for a more secure hardware status for manufactured devices.

3.8.1. Field Programmable Gate Arrays

FPGAs are hardware circuits that are manufactured with configuration in mind. They allow for specific customizations to be made to them [74]. They allow consumers or organizations that obtain them after creation to customize them for their desired outcomes. They are useful, as they come separate from the devices they will be operating in, so it is unknown at the time of production what exact settings and configuration would be desirable in order to achieve an attended goal with the final system the gate array will reside in. This postproduction configuration allows device manufacturers to be more flexible. Gate arrays are utilized during communication between devices due to their ability to make the process of understanding the algorithms that make the communication possible trivial [74]. In this regard, ring oscillators play a significant role.

3.8.2. Ring Oscillators

Ring oscillators are used to create a frequency signal in systems. They are groups of logic gates in circuits that are made up of NOT gates. The number of NOT gates must be an odd number. The output of the logic gates oscillates between values representing either true or false outcomes. The initial NOT logic gate in a chain receives one of its given inputs from the final NOT logic gate in the system. This process utilizes a concept called "time delay," in which inputs received to NOT gates are not all at a consistent rate of time with that rate constantly changing. Consequently, although there are a limited set of values that can be the final output of the oscillator, the time delay makes it so the output is difficult to predict. This increases security in a system when utilized.

4. Common Attacks in SG

This section presents the most common attacks affecting SGs that have been efficiently handled by key management and authentication methodologies.

4.1. Replay Attack

The proposed scheme protects against replay attacks by including timestamps with every message that is being sent during the login, authentication, and key agreement phases. Although the contents and variables of each message may differ, all include the variable T_i, which serves as the timestamp for that specific message [59].

4.2. Man-in-the-Middle Attack

Man-in-the-middle attacks are preventable by this scheme because even if an adversary was able to generate a new timestamp T_i' and a random nonce ru_i', they still do not know the secret credentials RID_i and signature s_i. Without the secret credentials, it is impossible for the adversary to impersonate another user or modify the contents of a message [59].

4.3. Privileged-Insider Attack

Privileged inside attacks can also be prevented with the proposed scheme. Suppose a privileged insider has access to the important registration information of a user. Without the biometric key σ_i of the user, the adversary cannot verify a guessed password in order to authenticate themselves as the user. Similarly, this proposed scheme can also prevent user impersonation attacks in a similar way [59].

4.4. Spoofing Attack

The main feature of the spoofing attack in SGs is to disrupt the network traffic measured by the distributed SMs. Moreover, this attack is versatile in its consequences, such as existing routing loops, extending or shortening the source route, and injecting errors in the transferred data. In the literature context, among the main efforts confronting this attack, we can find significant proposals, such as [75].

4.5. Invasive Attack

Invasive attacks are those on physical systems that permanently alter the chip's physical characteristics. The attack's goal is to record information that is kept in memory spaces of meters. These attacks are also employed to defeat blown fuse linkages, disable meters, and disconnect circuits. Interestingly, SMs are not the only targets of these attacks. From the state of the art, in [76,77], intelligent security models have been proposed for detection isolation and localization and anomaly-detection models to mitigate the attack manipulations of this kind of attack.

4.6. Denial of Service (DoS) Attacks

DoS attacks usually work by flooding targeted SMs with requests until traditional traffic is not able to be processed, which denies service to additional entities. Moreover, the DoS attacks are able to disrupt the data integrity and authentication between SMs in the SGs. Several efforts have been proposed in the literature targeting the different DoS attacks, such as [78].

4.7. Brute Force Attack

The brute force attack focuses on the security and confidentiality of observed SMs measures in SGs. Accordingly, catastrophic situations may occur due to the sensitivity of SMs and the vulnerability of physical quantities measured in SGs. Many research efforts have been exerted to resolve such intelligent attacks, such as in [78,79].

4.8. Offline and Online Attacks

First, the online attack can access the encrypted data or a password hash. Then, the attacker can experiment with key combinations without worrying about being discovered or interfered with. Secondly, the attacker in the online attack must communicate with the target system he is seeking to access. In Refs. [78,79], the proposed model can mitigate both kinds of attacks.

5. Key-Management Methodologies

This section addresses the methodologies of key management for SGs. In the literature context, many research efforts have been proposed in this regard. Here, we discuss the main nine techniques and algorithms as follows.

5.1. Diffie–Hellman

The Diffie-Hellman key exchange is a key part of secure communication protocols. It is a component in a communication protocol that enables the ability for them to have a secure connection [80]. It makes it possible for a secure environment to be established and for two unknown users to establish a key they can use simultaneously to communicate. A secure environment when making keys is important because if keys are intercepted it makes communication between users insecure and dangerous. If someone has access to the key but has no authority to view it, they can now access all messages exchanged between users using said key. The Diffie–Helman Key Exchange establishes this secure environment by having both users indirectly discover the secret key they wish to use. Figure 1 shows the general structure of Diffie–Helman.

The way the exchange works is that two people looking to communicate start off with their own parts of a key, let us say *A* & *B*. Neither knows the other's part, and both users agree on a likewise third addition. In Ref. [80], the authors add together the piece they know and the agreed-upon piece together. They then exchange that combination, and once again add their known part to it. They now have a like-key that is the same without ever exposing what their own original keys were. This works functionally with keys, as they are usually represented by long, complex strings of bits rather than just single alphanumerical letters, making it extremely difficult for a bad actor that retrieves a piece of the key during the exchange to decipher it.

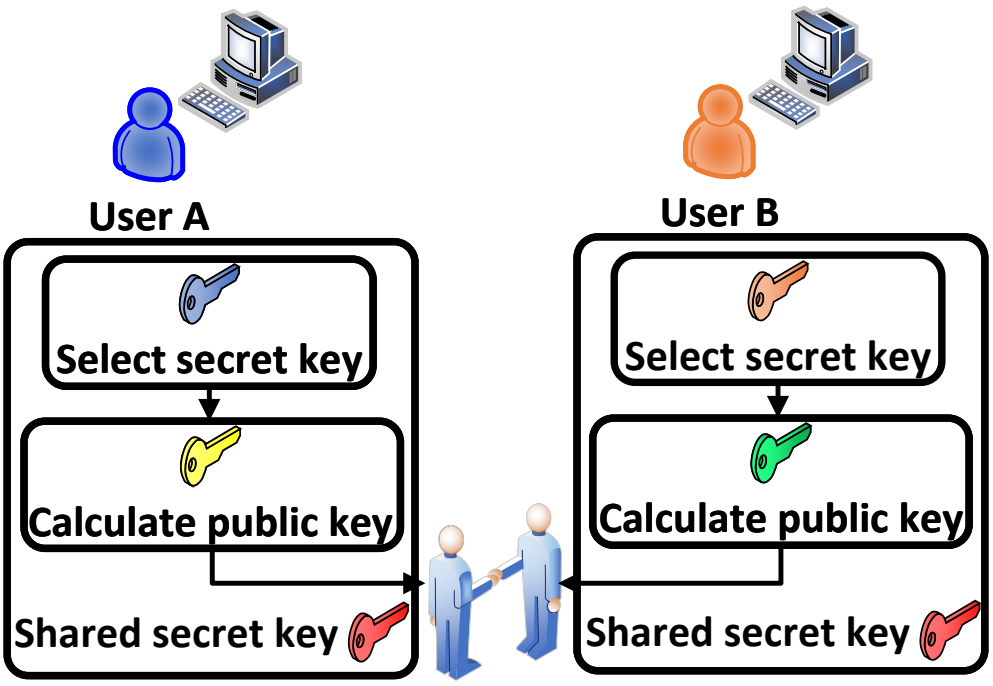

Figure 1. General structure of Diffie–Hellman.

5.2. Scalable Key Management (SKM)

Figure 2 shows the general structure of an SKM scheme that was proposed by [81]. The system structure is illustrated as follows. A HAN network, links smart appliances, distributed energy resources, the HAN gateway, and other control devices to the SM. A wide area network (WAN) facilitates utility companies and customers to communicate in both directions. Power line communication systems, cellular networks, or IP-based networks can all be used to create wide-area communication infrastructure, depending on the real requirements [82]. Moreover, a database system called the meter data management system (MDMS) is employed to store, manage, and analyze metering data to improve customer services [81].

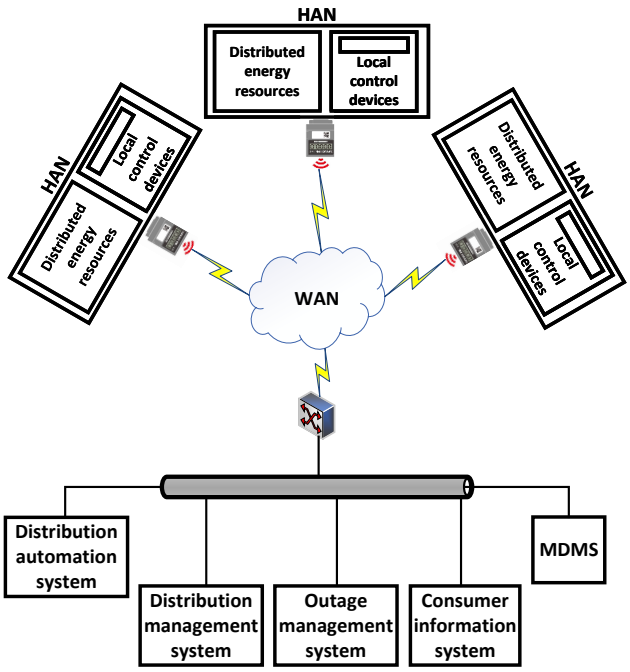

Figure 2. General structure of SKM.

5.3. Logical Key Hierarchy

The LKH, which uses a key tree for each demand response (DR) project, addresses the scalability issue. Each LKH member maintains a copy of the secret keys to its leaf and all other nodes along the path leading from its leaf to the root. Figure 3 illustrates the process of the LKH. The authors in [83] showed that scalability is guaranteed for big SGs with dynamic demand response projects using their suggested LKH. Additionally, a multigroup key graph structure is suggested in this work to lower key-management storage and communication costs. A fresh set of keys can be shared by several DR projects by using the suggested key graph technique.

When compared to the communication costs brought on by using a separate LKH tree, the joining or departure of a user in a DR project has no impact on the cost of rekeying operations. In this study, a two-level graph is used to simulate the multigroup key graph structure. The lower level designates a user set that has subscribed to the same first DR project. The leaf node of the tree represents a user's key at the lower level, and the tree's root represents the group key for the DR project. The root key combinations for concurrent users subscribing to various DR projects are shown in the upper-level graph.

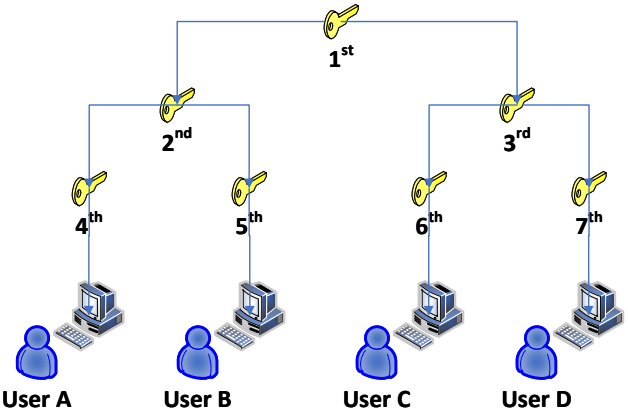

Figure 3. General architecture of LKH.

5.4. Information Centric Networking (ICN)

In order to guarantee secrecy, integrity, and authentication, the authors of [84] propose a key-management scheme for several SMs as well as ICN in AMI systems. The plan's goals were to provide security, manage network traffic, and facilitate mobility. Energy data in the AMI system must be kept a secret because it can reveal personal information about daily routines and habits. Utilizing ICN ensures data integrity in addition to authenticity and confidentiality. Because it is dependent on the safety of the data itself, it differs from the protection offered by end-to-end transmission. Here, the unicast, broadcast, and multicast secure message exchange is guaranteed. Figure 4 shows the architecture of the ICN.

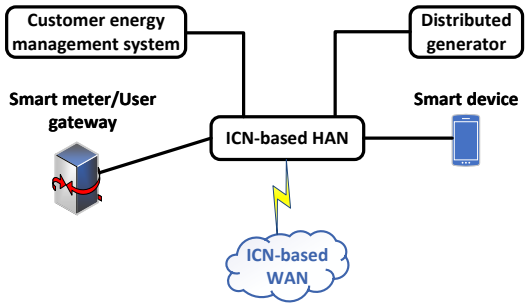

Figure 4. General structure of ICN.

5.5. Resilient End-to-End Message Protection (REMP)

Figure 5 illustrates the REMP paradigm. The authors in [85] addressed the challenges and limitations of conventional message protection and key-management schemes. The approach that they offered is known as REMP for short. REMP is introduced as an alternative to improve end-to-end security, "privacy, integrity, message source authentication, and key exposure resilience". It is a publish-subscriber group security scheme that improves the heavy computational load in using public keys. It also preserves the scalability and extensibility of the publish-subscriber group communications key-management schemes. REMP possesses four characteristics that make it a drastic improvement, compared to known message-protection schemes.

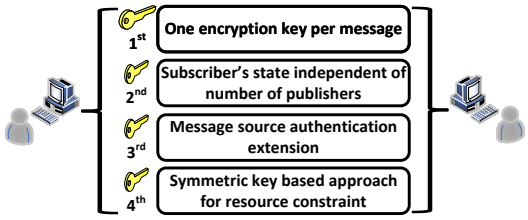

Figure 5. General structure of REMP.

The first characteristic is "one encryption key per message". The publisher will encrypt the message that they want to send by applying a separate session key. There is one session key per message that the publisher sends and uses for encryption. This characteristic increases the key security and privacy between multiple publishers within a group. This prevents other publishers from updating the publish key by either a new publisher entering the group or a publisher leaving the group, leaving the shared public key exposed to malicious exploitation. By having a session key per publisher and per message, other publishers leaving or entering the group cannot access this key because it is unique. It also prevents attackers from exploiting a shared session key, thus collecting and replaying cipher texts.

The second characteristic is the "subscriber's state independent of the number of publishers". An advantage that REMP possesses is that the subscriber can compute a one-time decryption key once a message is received, through the use of a long-term master key. This can prevent the subscriber to keep the security state set by the publisher and

avoid any extreme overloading if any failures or restarts occur with the subscriber. This REMP characteristic displays scalability in the situation of a multipublisher group.

The third characteristic is "message source authentication extension", which addresses the problem of message source authentication. REMP exploits end-to-end authenticators and message brokers that multicast messages from the publishers in a group. Once a message is sent, the end-to-end authenticator has the sender's or publisher's identity and a ciphered message authentication code of the message. An example of this is shown in a solution that was proposed by Badra et al. [86] who mention the use of REMP to help improve end-to-end message confidentiality and integrity, as well as prevent replay attacks. This scheme that is created, is split into two phases—the application phase, and the handshake phase. In the application phase, every time a client application sends a request message to trusted third parties, the following are attached: the client's certificate URL, random number, and server address. When the trusted third party reviews the message received, they verify the client signature before using the server public key to authenticate the client into the server. With the server's public key, the trusted third party can generate a ticket for the authenticated client, which contains a message called the "response", which consists of encrypted fields. With this, the client can detect replay attacks by comparing and signing the client's random number through a trusted third party. The handshake phase verifies that both random numbers of the trusted third party and the client match in order to generate symmetric keys for encryption and message authentication. In [87], the solution proposed still has issues with end-to-end security between the WAP terminal and application server due to the client and trusted third parties not having WTLSCert and X.509 certificates. This solution then ties into the final characteristic of REMP.

The final characteristic of REMP is the symmetric key-based approach for resource constraints. In a cyberphysical system (CPS), communications devices communicate with servers in an administrative domain. A preshared key, or PSK, per device and symmetric ciphers like AES or 3DES can work with the cyberphysical system. In REMP extensions, symmetric-key operations are predominant because it protects confidentiality and integrity. With symmetric keys, REMP can use ECC to support a secure multicast to a massive number of subscribers and maintain symmetric-key operations, and secure data collection from a massive number of publishers.

These four characteristics lay out the foundation for REMP as an alternative tool for the key-management and message-protection scheme, whose system architecture and solution will be discussed in the later section.

5.6. NIKE and NIKE+

The authors in [87] contributed to this topic by proposing their own protocol for key establishment. Two versions of this protocol have been made for this paper—one called novel identity-based key establishment (NIKE) and the other called NIKE+. Their protocol is based on ECC. This protocol works by first having the grid owner take inputs to set as parameters, which are then forwarded to a trusted authority (TA). The TA will then use these parameters in combination with a master key to send the SM and the AHE private keys. Once this is done, a session key can be established between an SM and AHE. Figure 6 denotes the architecture of the NIKE process.

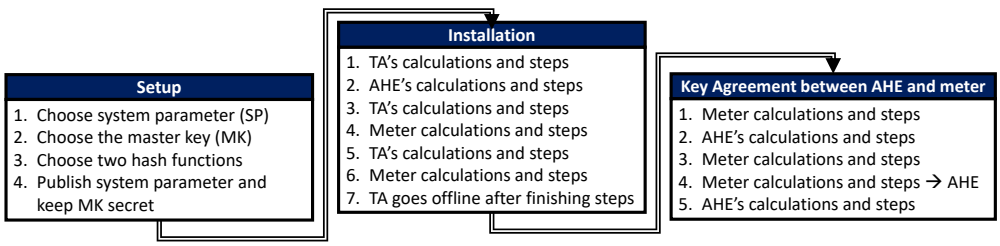

Figure 6. Algorithm of NIKE.

The difference between their two proposed methods (NIKE and NIKE+) is that NIKE+ has more of the calculations performed on the AHE compared to NIKE. This is because the resources on the SM are very limited. By moving the calculations to AHE, which is less resource restricted, the protocol can do calculations much faster. When comparing NIKE and NIKE+ calculation times, NIKE was shown to take 4.91 s while NIKE+ only took 2.46 s in total. NIKE+ proved to be much faster when compared to protocols that were mentioned earlier. The protocols proposed by Wan et al. [81] (SKM and SKM+) both took over 7 s, the protocol proposed by [88] took a total of about 45 s, and the protocol proposed by [89] took 4.91 s. Compared to these NIKE+ performed much better. NIKE and NIKE+ have also proven to be secure when using the AVISPA tool to check for any vulnerabilities.

NIKE performs its key establishment scheme by using a three-step process: setup, installation, and key agreement. The scheme in the proposed paper [87] uses three components communicating with each other in order to ensure creation of a secure environment for establishing keys. NIKE and NIKE+ both use an SM for the consumer side, an AHE for the SG operations center, and a TA in order to help secure the initial connection between the SM and the AHE. Figure 7 illustrates the architecture of the NIKE+ process.

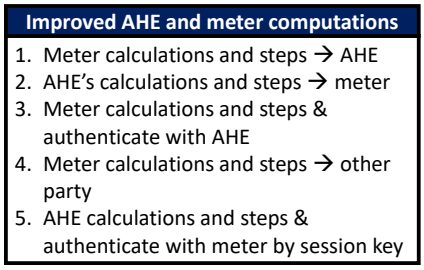

Figure 7. Algorithm of NIKE+.

For the first step, the setup occurs on the TA. This step is meant to create some of the preliminary parameters to be used for the secure key establishment. One variable, k, is first received by the TA. This value k will be used to generate the parameters to be used in the key exchange. With k, the TA decides upon a prime number, q, that will be used in the calculations. The prime number q consists of k amount of bits, so carefully choosing a k value will help provide better security because it influences other parameters. With the q value having been created, the TA then uses this value in order to generate the values F_q, E/F_q, G_q, and P. Two hash functions, H_1 and H_2, a master key, x, and a public key, P_{pub}, will also be generated by the TA. These values will all be sent to the SM and the AHE as parameters for the key establishment.

The second step, installation, then has the SM and AHE communicating with the TA. This step has the AHE calculate R_{AHE} by using a random number r and calculating rP. This value is sent to the TA, in which the TA responds back with y_{AHE}, which is the value generated by hashing together R_{AHE} and the ID of the AHE that it is trying to communicate. Following that process, the SM performs a similar procedure, and the TA responds back with y_i, which is the value generated by hashing the SM ID and also the y_{AHE}, which was produced with the AHE.

The third step, the key agreement, is then performed by having the AHE and SM communicate back and forth with each other. The SM begins this by generating a random number to be used to calculate T_M. This value is then sent alongside the ID of the SM, ID_M, and R_M, toward the AHE. The AHE then uses the values given by the SM to generate k_{AHE}, which is used for session key generation. AHE responds to this by sending back its ID_{AHE}, M_1 which was generated by calculating the hash H_1 (0, $k_{\mathrm{AHE},\,M}$), and T_{AHE}, which was calculated similarly to T_M. The SM is able to authenticate the AHE by also calculating the hash M_1 by itself and comparing it to the one sent by the AHE. The SM then calculates M_2 and performs a similar process in order to authenticate itself to the AHE. Once both the SM and the AHE have authenticated each other, they are both able to create the key that they will be communicating by using hashing and concatenating the IDs with secrets

they both have. In the case of the SM, it has less computational power compared to the AHE. What NIKE+ changes from NIKE is the computational load required by the SM and the AHE. Shifting some of the computations from the SM over to the AHE allows the key establishment to be accomplished much faster.

5.7. Anonymous Key Distribution

Figure 8 indicates the architecture of the anonymous key distribution process. The authors in [90] applied an "identify-based" signature and identity-based encryption to propose an anonymous key distribution scheme for SGs. This would require SMs and service providers to mutually authenticate with each other than establish session keys between them to communicate securely. However, this scheme was insecure against ephemeral secret leakage attacks and failed to provide strong privacy credentials for SMs. This scheme was also vulnerable to privileged insider attacks and offline password-guessing attacks [90].

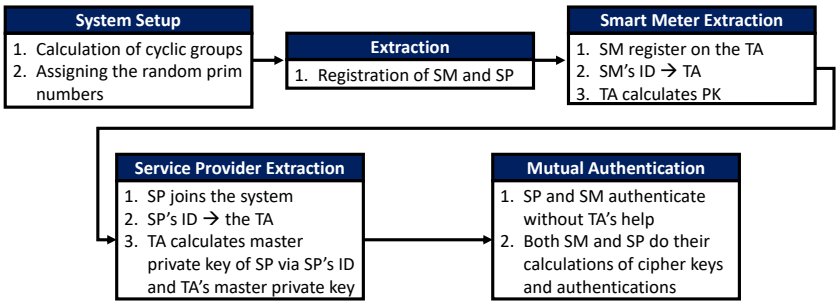

Figure 8. General architecture of anonymous key distribution.

5.8. Key Management System

The authors in [91] proposed a novel key-management system framework of AMI systems based on the key graph as shown in Figure 9. The key graph includes key management for unicast, multicast, and broadcast modes. The main issue around this scheme is "it is based on nonvolatile memory technologies which are vulnerable to spoofing and invasive attacks" [8].

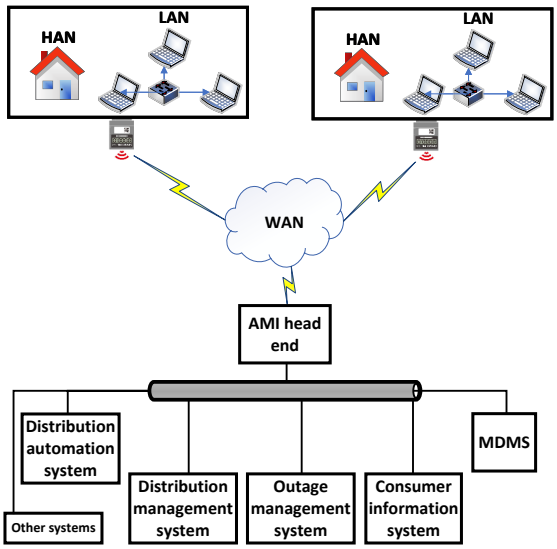

Figure 9. General architecture of KMS.

5.9. Needham-Schroeder-Based Symmetric Key

In Ref. [92], the authors proposed a novel key-management scheme that combines symmetric-key techniques with elliptical curve public key techniques. The proposed

scheme presented strong security along with great scalability and accessibility. However, the scheme is still vulnerable to man-in-the-middle attacks [59].

Although different schemes have been presented to address issues with SG communication, most of these schemes fail to provide functionality and security features, such as perfect secrecy, secret key security, protection against offline password-guessing attacks, strong SM credential privacy, dynamic SM addiction, and update phases [59]. The authors of this article try to address these issues and present their own scheme for a three-factor user-authentication scheme for renewable-energy-based SG environments (TUAS-RESG). To sum up, Table 1 identifies the pros and cons of the addressed key-management mechanisms.

Table 1. Common types of key-management schemes.

Type	Advantages	Disadvantages
Diffie–Hellman [80]	Can effectively deal with key management	Vulnerable to man-in-the-middle attack
SKM [81,82]	End-to-end encryption, the ability of key generation, key freshness, support forward and backward secrecy, support integrity, support confidentiality, support authentication	High computational time
LKH [83]	Suitable for large SGs with dynamic demand response projects, allow multiple demand response projects to share new key sets, solve the scalability issue, less storage and communication cost are needed	In case of compromise, the rekey of a multicast group requires to balance the number of transmissions and storage
ICN [84]	Suitable for a large number of SMs, control network congestion, support mobility	Establishing an experiment environment via ICN is challenging, ICN relies on name-based routing, implementation is not easy, high memory usage leading to performance degradation
REMP [85,86]	Improve end-to-end security, privacy, integrity, message source authentication, and key exposure resilience, less computational process	Faces some end-to-end security issues between the application server and WAP terminal when the client and trusted third parties not having WTLSCert and X.509 certificate [86,93,94]
NIKE&NIKE+ [81,87–89]	It is not based on pairing, very low overhead	Keys between the corrupted user and benevolent ones not leaked immediately [94]
Anonymous key distribution [90]	Utilize identify-based signature and identity-based encryption	Insecure against ephemeral secret leakage attacks and failed to provide strong privacy credentials for SMs [90]
KMS [8,91]	Suitable for unicast, multicast, and broadcast modes	Relies on nonvolatile memory technologies which are vulnerable to spoofing and invasive attacks
Needham–Schroeder-based symmetric key [59,92]	High scalability and accessibility, efficient protection against offline password guessing attacks	Vulnerable to man-in-the-middle attacks

6. Authentication Schemes

This section introduces the main authentication schemes in the literature. More particularly, six mechanisms have been considered, namely, PUFs, lightweight message and attribute-based authentications, Merkle-tree-based authentication, mutual authentication for unicast and multicast communications, TUAS-RESG, Markov chain, and game theory.

6.1. Physical Unclonable Functions

In Ref. [95], the authors proposed a scheme that combines PUFs and a PKG technique wirelessly to provide secure communication. PUFs are a hardware implementation of security for devices. In other words, PUFs are a hardware solution to authentication problems that plague hardware-authentication schemes. They also address the need to store cryptographic keys on a system without requiring additional hardware installation.

In authentication, there is an issue with devices being replicated. Once replicated, bad actors can pretend to be using the original device that was created. This can give them unintended access to systems that were given to the original, real device. Accordingly, by utilizing randomness, PUFs give devices a unique signature that cannot be replicated. This is done by using the hardware of a specific device to generate unreplicable data. This scheme has strong encryption and authentication. However, "no information about real-time requirements of computation and secure communication subsystems is provided". Along with those issues, the precise cost of such a protocol has yet to be identified or established. It should be noted that even if the same hardware specifications were present in multiple instances of a device, each of them would still continue to output a unique piece of data.

In this regard, in Ref. [96], the authors tried to address some of the major security issues, scalability, and efficient communication between SMs and utilities with AMIs. Their proposed scheme was based on a combination of PUFs and ID-based authentication that combines the best of symmetric cryptography with identity-based cryptosystems. Moreover, the proposed scheme provided security at the application layer, handled ID-based keys, and eliminates the risk of key compromise on the hardware level. It is also able to thwart DoS attacks and reduce the average packet latency by 8–14×. In that work, the authors have not identified any limitations revolving around this proposed framework. However, the implementation of such a framework could be difficult due to the combination of different security systems. That model has relied on Hamming code, which provided better security while sending less information back to the utility company, therefore reducing overhead [8].

The effort has been extended by [8], in which the authors tried to address the issues presented above by proposing a novel authentication and secret key storage scheme for AMI systems by using the ROPUFs on FGPA without the requirement of a secure volatile memory system or additional costly hardware in SMs. This scheme would eliminate the need to store secret keys in SMs and instead derive such keys from the FGPA chips themselves. More particularly, ROPUFs adapt the functionality of ring oscillators and PUFs in order to provide hardware security. ROPUFs combine ring oscillators, PUFs, and multiplexers in a logic circuit. ROPUFs get their output values by comparing the frequency of oscillation between the ring oscillators that are included in the system. The output bit value is dependent on the speed of the paths of the ring oscillators in the circuit. These paths of oscillators will always run at different speeds and create unpredictability within outputs. This unpredictability increases the authenticity of systems [97], preventing signals from being replicated and giving devices a unique signature.

6.2. Blockchain-Based Authentication

Recently, blockchain has played a significant role for authentication and authorization in many sensitive applications such as SGs. In Ref. [98], an edge computing-based SG system protocol for mutual authentication and key management. Without the need for additional complicated cryptographic primitives, the protocol may offer effective conditional anonymity and key management by utilizing blockchain. The model stops a user's identity from being revealed to the edge server. In addition, because of identity-based registration, the entry and exit of new end users would not have an impact on those of the already-existing end users.

6.3. A Lightweight Message and Attribute-Based Authentications

The authors of this paper present a "lightweight message authentication scheme for connecting the SMs distributed at various hierarchical networks" [8]. However, this scheme results in a high level of overhead in certificate management due to the use of traditional public-key cryptography. This is implemented by using the Diffie–Hellman exchange protocol to establish shared session keys [99].

In Ref. [100], the authors proposed a privacy-preserving authentication scheme for SG environments that utilizes a two-step protocol for authentication between SMs and data collection units, and AMIs. However, some functionalities and security features are missing in this proposed scheme. Their proposed scheme is susceptible to availability attacks such as DoS attacks.

The authors in [101] presented an attribute-based authentication and authorization scheme for SGs that protect against both outsider and insider threats in SGs by "verifying the user authorization and performing user authentication together". This proposed scheme has been tested by BAN-Logic and protocol verifier (ProVerif) showing strong durability with very little computational overhead to improve performance.

6.4. Merkle-Tree-Based Authentication

The authors in [102] addressed the vulnerability that SGs face, such as message injection attacks and replay attacks, which could degrade the performance of SGs. To prevent such an issue, the authors proposed an authentication scheme that considers SGs with computation-constrained resources and employs the Merkle hash tree technique. This proposed scheme helps to reduce computational overhead and prevents replay, message injection, and message analysis attacks. However, its resiliency toward DoS attacks is still untested and could prove to be critical.

6.5. Mutual Authentication for Unicast and Multicast Communications

In this scheme, the authors proposed a scheme for mutual authentication between SG utility networks and HAN SMs [89]. This method also provided "a novel key management protocol for data communication between the utility servers and customer SMs". This proposed scheme prevented brute force, replay, denial-of-service, and man-in-the-middle attacks and improved network overhead caused by security key-management packets. However, the proposed scheme does not address authentication between SMs and appliances.

6.6. TUAS-RESG and Two-Factor Authentications

With the emergence of the Internet of things, devices can exchange information with each other in order to increase efficiency and use. With this growth happening in the technological field, SGs are emerging, providing a more stable and efficient power to end users via three-factor user authentication [59]. IoT devices and SGs work hand-in-hand, exchanging and interpreting information by utilizing TUAS-RESG [59]. To facilitate this two-way communication between end users and SGs, SMs, sensing devices, and control systems are put in place. That model has relied on a well-known signature scheme called El-Gammal. However, the proposed scheme did not support the password and biometric update phase and dynamic SM addition phase.

For two-factor authentication, the authors in [103] addressed current issues with SG security by identifying the overlooked significance that the SG is a cyber-physical system, meaning more consideration of its cyber and physical domains needs to be addressed. Overlooking this issue has resulted in substitution and man-in-the-middle attacks. The authors presented a combination of a contextual factor based on physical connectivity in the PG with the conventional authentication factor in the challenge–response protocol to create a two-factor cyber-physical device authentication protocol to defend against coordinated cyber-physical attacks on SGs.

6.7. Markov Chain and Game Theory for Authentication

The authors in [104], proposed a dynamic and distributed "trust model based on a Markov chain to formalize the trust metric variation and its stability". This scheme allowed vehicles to act as their monitor and update the trust metric of their neighbors depending on the behavior of the network. Its flexibility allowed it to adapt the model according to the application's context. This scheme's strength is shown by its resistance and robustness during testing. While the proposed scheme is very strong, its performance evaluation of the trust model in the real context of VANETs needs improvements and enhancements.

To decide on a just cost allocation for the noise that is added to a system, parties might work together under the guidance of game theory. Therefore, a complex branch of intelligent optimization is game theory. The game theory model shows a competition between teams of players who might decide to cooperate or compete against one another to advance their results or payouts through the employed strategy or strategies carried out by the progressive player actions. The definitions of the key game parameters from the cited references [105–107].

In the field of security, game theory can be used to spot rogue nodes, lessen the impact of outside incursions, and find nodes that act egotistically and overburden the entire network. Nash equilibrium (NE) has become a realistic concept for wireless networks, and more specifically for the security of wireless nodes. NE is an intelligent solution to social concerns.

The authors in [108] investigated how to use game theory to shield wireless nodes from egotistical or malicious nodes. That study examined several game-theoretic protection tactics for wireless nodes and provided a classification of game-theory strategies based on the nature of the attacks. The significance of evolutionary games for the security of wireless nodes facing clever attacks was then recognized in a trust model employing game theory for decision-making. Finally, several game theory perspectives were put forth to encourage the cooperation and validity of data among various wireless nodes. A Stackelberg game was developed to fight external assault manipulations utilizing the energy defense budget versus the corresponding attack budget, as suggested in [109], in order to avoid disrupting the reported data in clustered sensor networks. The proposed work may successfully address the hardware issue that arises in the presence of the attack impact in sensor network-based cognitive radio, as stated in [110]. The suggested model also effectively manages energy use. In order to create a security model for sensor network-based cognitive radio to defend against the data falsification attack, ref. [106] presented a Stackelberg game. This strategy was created for two distinct attack–defense situations. Based on the threshold level for calculating the interference power, two scenarios were offered.

An efficient Stackelberg game was suggested in [111] in order to attain data trustworthiness in PGN. This attack scenario frequently manipulates groups of the PGN's deployed nodes, which cannot be controlled by the method just mentioned. The attack scenario, which is more serious than that considered in previous studies, was addressed by the presented model. A game-theoretic protection strategy was put forth for clustered wireless sensor networks based on a repeated game in the article [112]. The suggested method was developed to identify rogue nodes that discard HPPs in order to improve the dependability of high-priority data (HPT). The results of this study demonstrate that, in comparison to a noncooperative defensive mechanism, the suggested protection model's HPT is improved, resulting in the Pareto ideal HPT. A game-theoretic strategy based on non-zero-sum games is proposed in [113] to provide a strong trust model against sophisticated threats faced by IoT applications. The collected results demonstrate improved performance in identifying malicious nodes and a simple model.

7. Versification Tools of Protocols

This section highlights the main tools utilized for verifying the tools of key management [114]. Specifically, we concentrate on the automated validation of Internet se-

curity protocols and applications (AVISPA) tool [87], and the recent version of ProVerif (Version 2) [115].

7.1. AVISPA

In Ref. [87], the researchers utilized the AVISPA tool to verify the security integrity of the NIKE key-management scheme that was developed. AVISPA is an applications tool providing a suite of applications and modules that are used to build and analyze the security of Internet protocols and applications [116,117]. Figure 10 shows the process of the AVISPA tool.

There are three layers to the AVISPA tool as you can see in Figure 10 [117]. The top layer is the high-level protocol specification language in which the designer of the protocol interacts with the tool to implement their security protocol along with a security property into the tool to be tested [116]. The middle layer is where the input is then converted to an intermediate format (IF) code with the use of a translator [117]. The IF code is analyzed with the bottom layer, the backend analyzers. These four analyzers are the on-the-fly model checker (OFMC), CL-based attack searcher (CL-AtSe), SAT-based model checker (SATMC), and tree automata-based protocol analyzer (TA4SP).

- OFMC uses a demand-driven method to perform protocol falsification and bounded verification by exploring the transition system described in the IF specification [116]. It allows the specification of algebraic properties of cryptographic and typed and untyped protocols [116].
- CL-AtSe utilizes simplification heuristics and redundancy elimination techniques to apply constraint solving to the Internet protocol [116].
- SATMC employs the IF, the initial state, and the set of states as parameters to represent a violation of the security protocol defined to build a propositional formula for said protocol [116].
- The TA4SP module approximates attackers' or intruders' knowledge of the inner workings of the protocol with the use of regular tree languages and rewriting. It can show if the protocol is flawed by underapproximating or whether it's safe for any number of sessions by overapproximating [116].

Upon completing its analysis, the AVISPA Tool will output the result of the analysis of the defined security protocol and will state whether the input problem was solved either positively or negatively, the available resources that were exhausted, and whether the problem cannot be solved for a particular reason [116].

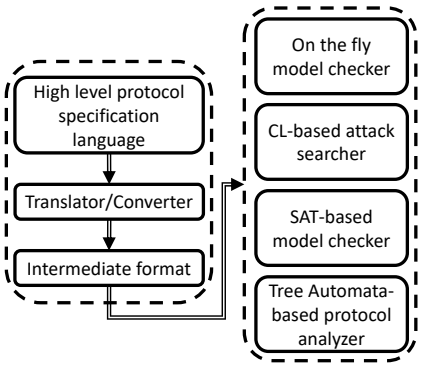

Figure 10. General structure of AVISPA.

7.2. ProVerif

This model, created by [114] depicts protocols using Horn clauses and employs over-approximation to evaluate an infinite number of sessions. Horn clauses and a portion of the pi calculus are the two types of input files that ProVerif accepts. The tool performs unbounded verification for a class of protocols by using an abstraction of fresh nonce generation. It can manage an infinite number of protocol sessions as well as a wide variety

of cryptographic primitives (shared and public-key cryptography, hash functions, etc.). Any equational theory can be modeled in ProVerif; however, the tool might not finish. Although this is true for XOR or Diffie–Hellman exponentiation, ProVerif does support the commutativity of the exponentiation alone [118]. Figure 11 shows the process of the AVISPA tool.

Several studies have focused on the efficient utilization of the ProVerif tool [119,120]. Figure 11 depicts the process of verifying the key-management protocol. Abbreviations shows the main acronyms throughout the paper.

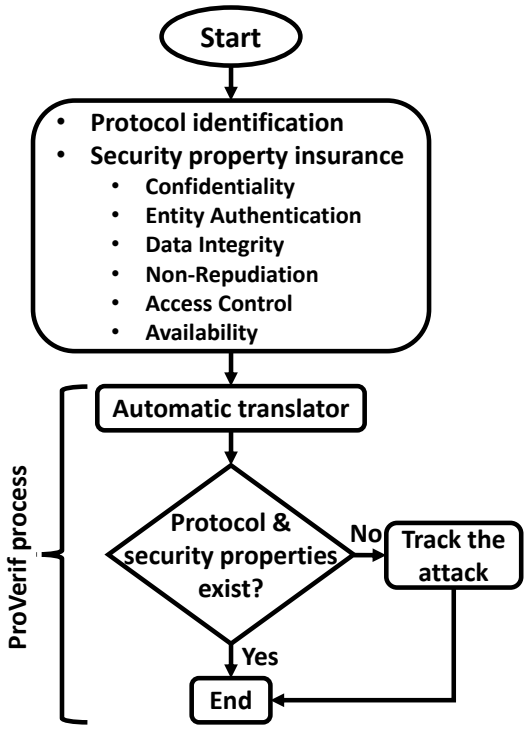

Figure 11. General structure of ProVerif.

8. Conclusions, Challenges, and Future Vision

The main takeaway from this survey is involved in the key-management and authentication mechanisms for SGs. The pros and cons of the most recent key-management techniques are addressed. Among the presented techniques, REMP and NIKE are considered the most effective ones with some drawbacks. REMP does not need subscribers in a group to directly communicate with publishers in a group, and as a result, outperforms many other point-to-point schemes. On the contrary, REMP is that conventional security schemes are insufficient to meet the security requirements of SG as a large-scale CPS. Moreover, REMP was unable to find a balance between end-to-end security strength and scalability and thinness requirements, along with computing capability. NIKE proposed a three-part key scheme involving setup, installation, and key agreement, but the greatest contribution was to shift the computational load onto the AMI head-end because it is less resource-restricted and will be able to complete calculations much faster. However, it has a high computational load and is susceptible to man-in-the-middle and desynchronization attacks. From the authentication point of view, the ROPUFs can be frequently used among the other ones. It can store cryptographic keys instead of nonvolatile memory systems or hardware encryptions. This makes the system easy to integrate because no additional hardware is needed and meters can have a unique ID that can identify them. ROPUFs can also be reconfigured with the AES encryption scheme, making the system easily deployable. The authentication occurs as the ROPUFS offers five levels of security to ensure the communication between the SM and utility company is secure before it is allowed to

connect to the Internet. However, systems authenticated by ROPUFs can be attacked by sending spoofing messages causing reconfiguration.

The future of SMs will continue to grow with the advancement in technology. As we have seen, key management and authentication are big problems that are needed in smart metering systems because they may threaten the PG stability. With the development of the existing authentication schemes, we will continue to address problems until we reach practical, lightweight, privacy-preserving, and robust key-management and authentication schemes to advance the security of communication and authentication in smart metering systems. Because this survey study focuses on the existing key-management and authentication schemes that were implemented in smart metering systems, in the future, however, key-management and authentication approaches that are used in other cyber-physical systems, such as vehicular networks, e-health, transportation systems, etc., can be considered because each environment has its own challenges and goals. Moreover, we showed that there is not yet a solution that fulfills all the proposed objectives and that there is still much work to be done in key management and authentication. For example, one can observe that the majority of the ROPUFs are suffering from the rising temperature on PUF-embedded devices which results in performance degradation. Hence, this limitation could potentially be focused on in future designs of PUF-based approaches. We have concluded that the approaches presented in this paper have security flaws. In the future, we will propose a new lightweight, authenticated key-agreement protocol that is based on a decentralized elliptic curve cryptosystem. Furthermore, we will verify and analyze the security claims of the newly proposed protocol.

Author Contributions: Conceptualization, M.S.A., M.M.F., A.E., Z.M.F. and M.I.I.; methodology, M.S.A., M.M.F. and M.I.I.; investigation, M.S.A., M.M.F., A.E., Z.M.F. and M.I.I.; writing—original draft preparation, M.I.I. and M.M.F.; writing—review and editing, M.S.A. and A.E.; supervision, M.I.I.; resources, M.S.A., M.I.I., M.M.F. and Z.M.F.; data curation, M.S.A., M.I.I. and M.M.F.; visualization, M.S.A. and M.I.I. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

Notation	Description
SG	Smart grid
PG	Power grid
PLC	Power Line Communication
AMI	Advanced metering infrastructure
SM	Smart meter
PKI	Public key infrastructure
ML	Machine learning
CA	Certificate authority
HAN	Home area network
PUFs	Physically unclonable functions
ROPUFs	Ring oscillator physically unclonable functions
FPGA	Field programmable gate array
KMS	Key management scheme
PKG	Physical key generation
LKH	Logical key hierarchy mechanism
$h(m)$	Hash value given the message m
ECC	Elliptic curve cryptography
RSA	Rivest–Shamir–Adleman cryptographic algorithm
DoS	Denial of service attack

SKM	Scalable key management
WAN	Wide area network
MDMS	Meter data management system
DR	Demand response
ICN	Information centric networking
REMP	Resilient end-to-end message Protection
CPS	Cyber-physical system
NIKE	Novel identity-based key establishment
TA	Trusted authority
NE	Nash equilibrium
HPT	High-priority data
AVISPA	Automated validation of internet security protocols and applications tool

References

1. Abdalzaher, M.S.; Elsayed, H.A.; Fouda, M.M.; Salim, M.M. Employing Machine Learning and IoT for Earthquake Early Warning System in Smart Cities. *Energies* **2023**, *16*, 495. [CrossRef]
2. Wang, W.; Lu, Z. Cyber security in the Smart Grid: Survey and challenges. *Comput. Netw.* **2013**, *57*, 1344–1371. [CrossRef]
3. Badr, M.M.; Ibrahem, M.I.; Baza, M.; Mahmoud, M.; Alasmary, W. Detecting Electricity Fraud in the Net-Metering System Using Deep Learning. In Proceedings of the 2021 IEEE International Symposium on Networks, Computers and Communications (ISNCC'21), Dubai, United Arab Emirates, 31 October–2 November 2021.
4. Badr, M.M.; Ibrahem, M.I.; Mahmoud, M.; Fouda, M.M.; Alsolami, F.; Alasmary, W. Detection of False-Reading Attacks in Smart Grid Net-Metering System. *IEEE Internet Things J.* **2022**, *9*, 1386–1401. [CrossRef]
5. Badr, M.M.; Ibrahem, M.I.; Mahmoud, M.; Alasmary, W.; Fouda, M.M.; Almotairi, K.H.; Fadlullah, Z.M. Privacy-Preserving Federated-Learning-Based Net-Energy Forecasting. In Proceedings of the SoutheastCon 2022, Mobile, AL, USA, 26 March–3 April 2022; pp. 133–139. [CrossRef]
6. Habbak, H.; Mahmoud, M.; Metwally, K.; Fouda, M.M.; Ibrahem, M.I. Load Forecasting Techniques and Their Applications in Smart Grids. *Energies* **2023**, *16*, 1480. [CrossRef]
7. Alsharif, A.; Nabil, M.; Mahmoud, M.M.; Abdallah, M. EPDA: Efficient and privacy-preserving data collection and access control scheme for multi-recipient AMI networks. *IEEE Access* **2019**, *7*, 27829–27845. [CrossRef]
8. Mustapa, M.; Niamat, M.Y.; Deb Nath, A.P.; Alam, M. Hardware-Oriented Authentication for Advanced Metering Infrastructure . *IEEE Trans. Smart Grid* **2018**, *9*, 1261–1270. [CrossRef]
9. Minh, Q.N.; Nguyen, V.H.; Quy, V.K.; Ngoc, L.A.; Chehri, A.; Jeon, G. Edge Computing for IoT-Enabled Smart Grid: The Future of Energy. *Energies* **2022**, *15*, 6140. [CrossRef]
10. Miceli, R. Energy management and smart grids. *Energies* **2013**, *6*, 2262–2290. [CrossRef]
11. Alsharif, A.; Nabil, M.; Sherif, A.; Mahmoud, M.; Song, M. MDMS: Efficient and privacy-preserving multidimension and multisubset data collection for AMI networks. *IEEE Internet Things J.* **2019**, *6*, 10363–10374. [CrossRef]
12. Fadlullah, Z.M.; Fouda, M.M.; Kato, N.; Shen, X.; Nozaki, Y. An early warning system against malicious activities for smart grid communications. *IEEE Netw.* **2011**, *25*, 50–55. [CrossRef]
13. Fouda, M.M.; Fadlullah, Z.M.; Kato, N. Assessing attack threat against ZigBee-based home area network for Smart Grid communications. In Proceedings of the 2010 International Conference on Computer Engineering & Systems, Cairo, Egypt, 30 November–2 December 2010; pp. 245–250. [CrossRef]
14. Fouda, M.M.; Fadlullah, Z.M.; Kato, N.; Lu, R.; Shen, X. Towards a light-weight message authentication mechanism tailored for Smart Grid communications. In Proceedings of the 2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Shanghai, China, 10–15 April 2011; pp. 1018–1023. [CrossRef]
15. Ibrahem, M.I.; Mahmoud, M.; Fouda, M.M.; ElHalawany, B.M.; Alasmary, W. Privacy-preserving and Efficient Decentralized Federated Learning-based Energy Theft Detector. In Proceedings of the GLOBECOM 2022—2022 IEEE Global Communications Conference, Rio de Janeiro, Brazil, 4–8 December 2022; pp. 287–292. [CrossRef]
16. Ibrahem, M.I.; Badr, M.M.; Fouda, M.M.; Mahmoud, M.; Alasmary, W.; Fadlullah, Z.M. PMBFE: Efficient and Privacy-Preserving Monitoring and Billing Using Functional Encryption for AMI Networks. In Proceedings of the 2020 International Symposium on Networks, Computers and Communications (ISNCC), Montreal, QC, Canada, 20–22 October 2020; pp. 1–7. [CrossRef]
17. Abdulaal, M.J.; Ibrahem, M.I.; Mahmoud, M.; Bello, S.A.; Aljohani, A.J.; Milyani, A.H.; Abusorrah, A.M. DRFD: Deep Learning-Based Real-time and Fast Detection of False Readings in AMI. In Proceedings of the SoutheastCon 2022, Mobile, AL, USA, 26 March–3 April 2022; pp. 682–689. [CrossRef]
18. Ibrahem, M.I. Privacy-Preserving and Efficient Electricity Theft Detection and Data Collection for AMI Using Machine Learning. Ph.D. Thesis, Faculty of the College of Graduate Studies, Tennessee Technological University, Cookeville, TN, USA, 2021.
19. Zheng, J.; Gao, D.W.; Lin, L. Smart meters in smart grid: An overview. In Proceedings of the 2013 IEEE Green Technologies Conference (GreenTech), Denver, CO, USA, 4–5 April 2013; pp. 57–64.
20. Andreadou, N.; Guardiola, M.O.; Fulli, G. Telecommunication technologies for smart grid projects with focus on smart metering applications. *Energies* **2016**, *9*, 375. [CrossRef]

21. Abdalzaher, M.S.; Elsayed, H.A.; Fouda, M.M. Employing Remote Sensing, Data Communication Networks, AI, and Optimization Methodologies in Seismology. *IEEE J. Sel. Top. Appl. Earth Obs. Remote Sens.* **2022**, *15*, 9417–9438. [CrossRef]
22. Ibrahem, M.I.; Abdelfattah, S.; Mahmoud, M.; Alasmary, W. Detecting Electricity Theft Cyber-attacks in CAT AMI System Using Machine Learning. In Proceedings of the 2021 International Symposium on Networks, Computers and Communications (ISNCC), Dubai, United Arab Emirates, 31 October–2 November 2021. [CrossRef]
23. Ibrahem, M.I.; Badr, M.M.; Mahmoud, M.; Fouda, M.M.; Alasmary, W. Countering Presence Privacy Attack in Efficient AMI Networks Using Interactive Deep-Learning. In Proceedings of the 2021 International Symposium on Networks, Computers and Communications (ISNCC), Dubai, United Arab Emirates, 31 October–2 November 2021. [CrossRef]
24. Abdalzaher, M.S.; Fouda, M.M.; Ibrahem, M.I. Data privacy preservation and security in smart metering systems. *Energies* **2022**, *15*, 7419. [CrossRef]
25. Li, D.; Aung, Z.; Williams, J.R.; Sanchez, A. Efficient authentication scheme for data aggregation in smart grid with fault tolerance and fault diagnosis. In Proceedings of the 2012 IEEE PES Innovative Smart Grid Technologies (ISGT), Washington, DC, USA, 16–20 January 2012; pp. 1–8.
26. Lee, A.; Brewer, T. Guidelines for smart grid cyber security: Vol. 1, smart grid cyber security strategy, architecture, and high-level requirements. *NISTIR* **2010**, *7628*, 14.
27. Alsharif, A.; Shafee, A.; Nabil, M.; Mahmoud, M.; Alasmary, W. A multi-authority attribute-based signcryption scheme with efficient revocation for smart grid downlink communication. In Proceedings of the 2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Atlanta, GA, USA, 14–17 July 2019; pp. 1025–1032.
28. Tellbach, D.; Li, Y.F. Cyber-attacks on smart meters in household nanogrid: Modeling, simulation and analysis. *Energies* **2018**, *11*, 316. [CrossRef]
29. Ibrahem, M.I.; Mahmoud, M.; Fouda, M.M.; Alsolami, F.; Alasmary, W.; Shen, X. Privacy Preserving and Efficient Data Collection Scheme for AMI Networks Using Deep Learning. *IEEE Internet Things J.* **2021**, *8*, 17131–17146. [CrossRef]
30. Ibrahem, M.I.; Nabil, M.; Fouda, M.M.; Mahmoud, M.M.E.A.; Alasmary, W.; Alsolami, F. Efficient Privacy-Preserving Electricity Theft Detection With Dynamic Billing and Load Monitoring for AMI Networks. *IEEE Internet Things J.* **2021**, *8*, 1243–1258. [CrossRef]
31. Abdalzaher, M.S.; Fouda, M.M.; Elsayed, H.A.; Salim, M.M. Towards Secured IoT-based Smart Systems Using Machine Learning. *IEEE Access* **2023**. [CrossRef]
32. Herder, C.; Yu, M.D.; Koushanfar, F.; Devadas, S. Physical Unclonable Functions and Applications: A Tutorial. *Proc. IEEE* **2014**, *102*, 1126–1141. [CrossRef]
33. Nabeel, M.; Kerr, S.; Ding, X.; Bertino, E. Authentication and key management for Advanced Metering Infrastructures utilizing physically unclonable functions. In Proceedings of the 2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm), Tainan, Taiwan, 5–8 November 2012; pp. 324–329. [CrossRef]
34. Mohapatra, H.; Mohanta, B.K.; Nikoo, M.R.; Daneshmand, M.; Gandomi, A.H. MCDM Based Routing for IoT Enabled Smart Water Distribution Network. *IEEE Internet Things J.* **2022**, *10*, 4271–4280. [CrossRef]
35. Mohapatra, H.; Rath, A.K. A fault tolerant routing scheme for advanced metering infrastructure: An approach towards smart grid. *Clust. Comput.* **2021**, *24*, 2193–2211. [CrossRef]
36. Abdalzaher, M.S.; Salim, M.M.; Elsayed, H.A.; Fouda, M.M. Machine learning benchmarking for secured iot smart systems. In Proceedings of the 2022 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS), Bali, Indonesia, 24–26 November 2022; pp. 50–56.
37. Salim, M.M.; Elsayed, H.A.; Abdalzaher, M.S.; Fouda, M.M. RF energy harvesting dependency for power optimized two-way relaying D2D communication. In Proceedings of the 2022 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS), Bali, Indonesia, 24–26 November 2022; pp. 297–303.
38. Salim, M.M.; Elsayed, H.A.; Abdalzaher, M.S.; Fouda, M.M. RF Energy Harvesting Effectiveness in Relay-based D2D Communication. In Proceedings of the 2023 International Conference on Computer Science, Information Technology and Engineering (ICCoSITE), Jakarta, Indonesia, 16 February 2023 .
39. Salim, M.M.; Elsayed, H.A.; Elaziz, M.; Fouda, M.M.; Abdalzaher, M.S. An optimal balanced energy harvesting algorithm for maximizing two-way relaying d2d communication data rate. *IEEE Access* **2022**, *10*, 114–178. [CrossRef]
40. Khurana, H.; Bobba, R.; Yardley, T.; Agarwal, P.; Heine, E. Design Principles for Power Grid Cyber-Infrastructure Authentication Protocols. In Proceedings of the 2010 43rd Hawaii International Conference on System Sciences, Honolulu, HI, USA, 5–8 January 2010; pp. 1–10. [CrossRef]
41. Hamdy, O.; Gaber, H.; Abdalzaher, M.S.; Elhadidy, M. Identifying Exposure of Urban Area to Certain Seismic Hazard Using Machine Learning and GIS: A Case Study of Greater Cairo. *Sustainability* **2022**, *14*, 10722. [CrossRef]
42. Abdalzaher, M.S.; Soliman, M.S.; El-Hady, S.M.; Benslimane, A.; Elwekeil, M. A deep learning model for earthquake parameters observation in IoT system-based earthquake early warning. *IEEE Internet Things J.* **2021**, *9*, 8412–8424. [CrossRef]
43. Abdalzaher, M.S.; Elwekeil, M.; Wang, T.; Zhang, S. A deep autoencoder trust model for mitigating jamming attack in IoT assisted by cognitive radio. *IEEE Syst. J.* **2021**, *16*, 3635–3645. [CrossRef]
44. Abdalzaher, M.S.; Moustafa, S.S.; Abd-Elnaby, M.; Elwekeil, M. Comparative performance assessments of machine-learning methods for artificial seismic sources discrimination. *IEEE Access* **2021**, *9*, 65524–65535. [CrossRef]

45. Moustafa, S.S.; Abdalzaher, M.S.; Yassien, M.H.; Wang, T.; Elwekeil, M.; Hafiez, H.E.A. Development of an optimized regression model to predict blast-driven ground vibrations. *IEEE Access* **2021**, *9*, 31826–31841. [CrossRef]
46. Ibrahem, M.I.; Mahmoud, M.; Alsolami, F.; Alasmary, W.; AL-Ghamdi, A.; Shen, X. Electricity Theft Detection for Change-and-Transmit Advanced Metering Infrastructure. *IEEE Internet Things J.* **2022**, *9*, 25565–25580. [CrossRef]
47. Abdulaal, M.J.; Ibrahem, M.I.; Mahmoud, M.M.E.A.; Khalid, J.; Aljohani, A.J.; Milyani, A.H.; Abusorrah, A.M. Real-Time Detection of False Readings in Smart Grid AMI Using Deep and Ensemble Learning. *IEEE Access* **2022**, *10*, 47541–47556. [CrossRef]
48. Moustafa, S.S.; Abdalzaher, M.S.; Naeem, M.; Fouda, M.M. Seismic hazard and site suitability evaluation based on multicriteria decision analysis. *IEEE Access* **2022**, *10*, 69511–69530. [CrossRef]
49. Fadlullah, Z.M.; Fouda, M.M.; Kato, N.; Takeuchi, A.; Iwasaki, N.; Nozaki, Y. Toward intelligent machine-to-machine communications in smart grid. *IEEE Commun. Mag.* **2011**, *49*, 60–65. [CrossRef]
50. Abdalzaher, M.S.; Moustafa, S.S.; Hafiez, H.A.; Ahmed, W.F. An optimized learning model augment analyst decisions for seismic source discrimination. *IEEE Trans. Geosci. Remote Sens.* **2022**, *60*, 1–12. [CrossRef]
51. Elwekeil, M.; Abdalzaher, M.S.; Seddik, K. Prolonging smart grid network lifetime through optimising number of sensor nodes and packet length. *IET Commun.* **2019**, *13*, 2478–2484. [CrossRef]
52. Parvez, I.; Sarwat, A.I.; Wei, L.; Sundararajan, A. Securing metering infrastructure of smart grid: A machine learning and localization based key management approach. *Energies* **2016**, *9*, 691. [CrossRef]
53. Baza, M.I.; Fouda, M.M.; Tag Eldien, A.S.; Mansour, H.A. An efficient distributed approach for key management in microgrids. In Proceedings of the 2015 11th International Computer Engineering Conference (ICENCO), Cairo, Egypt, 29–30 December 2015; pp. 19–24. [CrossRef]
54. He, D.; Chan, S.; Zhang, Y.; Guizani, M.; Chen, C.; Bu, J. An enhanced public key infrastructure to secure smart grid wireless communication networks. *IEEE Netw.* **2014**, *28*, 10–16. [CrossRef]
55. Erol-Kantarci, M.; Mouftah, H.T. Energy-efficient information and communication infrastructures in the smart grid: A survey on interactions and open issues. *IEEE Commun. Surv. Tutor.* **2014**, *17*, 179–197. [CrossRef]
56. Alotaibi, M.; Ibrahem, M.I.; Alasmary, W.; Al-Abri, D.; Mahmoud, M. UBLS: User-Based Location Selection Scheme for Preserving Location Privacy. In Proceedings of the 2021 IEEE International Conference on Communications Workshops (ICC Workshops), Montreal, QC, Canada, 14–23 June 2021. [CrossRef]
57. Badr, M.M.; Mahmoud, M.; Fang, Y.; Abdulaal, M.; Aljohani, A.J.; Alasmary, W.; Ibrahem, M.I. Privacy-Preserving and Communication-Efficient Energy Prediction Scheme Based on Federated Learning for Smart Grids. *IEEE Internet Things J.* **2023**. [CrossRef]
58. Liu, J.; Xiao, Y.; Li, S.; Liang, W.; Chen, C.P. Cyber security and privacy issues in smart grids. *IEEE Commun. Surv. Tutor.* **2012**, *14*, 981–997. [CrossRef]
59. Wazid, M.; Das, A.K.; Kumar, N.; Rodrigues, J.J.P.C. Secure Three-Factor User Authentication Scheme for Renewable-Energy-Based Smart Grid Environment . *IEEE Trans. Ind. Inform.* **2017**, *13*, 3144–3153. [CrossRef]
60. Moustafa, S.S.; Abdalzaher, M.S.; Abdelhafiez, H. Seismo-Lineaments in Egypt: Analysis and Implications for Active Tectonic Structures and Earthquake Magnitudes. *Remote Sens.* **2022**, *14*, 6151. [CrossRef]
61. Abdalzaher, M.S.; Elsayed, H.A. Employing data communication networks for managing safer evacuation during earthquake disaster. *Simul. Model. Pract. Theory* **2019**, *94*, 379–394. [CrossRef]
62. Abd Alzaher, M.S.; Elsayed, H.A.; Kayed, S.I.; Anis, W.R. Road Traffic Modeling using Data Communication Networks. *Int. J. Comput. Appl.* **2011**, *975*, 8887. [CrossRef]
63. Wu, Y.; Wang, Z.; Huangfu, Y.; Ravey, A.; Chrenko, D.; Gao, F. Hierarchical operation of electric vehicle charging station in smart grid integration applications—An overview. *Int. J. Electr. Power Energy Syst.* **2022**, *139*, 108005. [CrossRef]
64. Ghamry, E.; Mohamed, E.K.; Abdalzaher, M.S.; Elwekeil, M.; Marchetti, D.; De Santis, A.; Hegy, M.; Yoshikawa, A.; Fathy, A. Integrating pre-earthquake signatures from different precursor tools. *IEEE Access* **2021**, *9*, 33268–33283. [CrossRef]
65. Moustafa, S.S.; Abdalzaher, M.S.; Khan, F.; Metwaly, M.; Elawadi, E.A.; Al-Arifi, N.S. A Quantitative Site-Specific Classification Approach Based on Affinity Propagation Clustering. *IEEE Access* **2021**, *9*, 155297–155313. [CrossRef]
66. Elhadidy, M.; Abdalzaher, M.S.; Gaber, H. Up-to-date PSHA along the Gulf of Aqaba-Dead Sea transform fault. *Soil Dyn. Earthq. Eng.* **2021**, *148*, 106835. [CrossRef]
67. Abdalzaher, M.S.; El-Hadidy, M.; Gaber, H.; Badawy, A. Seismic hazard maps of Egypt based on spatially smoothed seismicity model and recent seismotectonic models. *J. Afr. Earth Sci.* **2020**, *170*, 103894. [CrossRef]
68. Pande, A.S.; Thool, R.C. Survey on logical key hierarchy for secure group communication. In Proceedings of the 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), Pune, India, 9–10 September 2016; pp. 1131–1136.
69. Ghosal, A.; Conti, M. Key management systems for smart grid advanced metering infrastructure: A survey. *IEEE Commun. Surv. Tutorials* **2019**, *21*, 2831–2848. [CrossRef]
70. Amara, M.; Siad, A. Elliptic Curve Cryptography and its applications. In Proceedings of the International Workshop on Systems, Signal Processing and Their Applications, WOSSPA, Tipaza, Algeria, 9–11 May 2011; pp. 247–250. [CrossRef]
71. Fujiwara, T.; Kasami, T.; Kitai, A.; Lin, S. On the undetected error probability for shortened hamming codes. *IEEE Trans. Commun.* **1985**, *33*, 570–574. [CrossRef]

72. Singh, A. Error detection and correction by hamming code. In Proceedings of the 2016 International Conference on Global Trends in Signal Processing, Information Computing and Communication, Jalgaon, India, 22–24 December 2016; pp. 35–37.
73. Zeng, Q.; Li, H.; Peng, D. Frequency-hopping based communication network with multi-level QoSs in smart grid: Code design and performance analysis. *IEEE Trans. Smart Grid* **2012**, *3*, 1841–1852. [CrossRef]
74. Verma, H. Field programmable gate arrays. *IEEE Potentials* **1999**, *18*, 34–36. [CrossRef]
75. Gai, K.; Qiu, M.; Ming, Z.; Zhao, H.; Qiu, L. Spoofing-jamming attack strategy using optimal power distributions in wireless smart grid networks. *IEEE Trans. Smart Grid* **2017**, *8*, 2431–2439. [CrossRef]
76. Yilmaz, Y.; Uludag, S. Mitigating iot-based cyberattacks on the smart grid. In Proceedings of the 2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA), Cancun, Mexico, 18–21 December 2017; pp. 517–522.
77. Yılmaz, Y.; Uludag, S. Timely detection and mitigation of IoT-based cyberattacks in the smart grid. *J. Frankl. Inst.* **2021**, *358*, 172–192. [CrossRef]
78. Nicanfar, H.; Jokar, P.; Beznosov, K.; Leung, V.C. Efficient authentication and key management mechanisms for smart grid communications. *IEEE Syst. J.* **2013**, *8*, 629–640. [CrossRef]
79. Kamto, J.; Qian, L.; Fuller, J.; Attia, J. Light-weight key distribution and management for advanced metering infrastructure. In Proceedings of the 2011 IEEE GLOBECOM Workshops (GC Wkshps), Houston, TX, USA, 5–9 December 2011; pp. 1216–1220.
80. Li, N. Error detection and correction by hamming code. *Int. Conf. Comput. Eng. Technol.* **2010**, *4*, 634–637.
81. Wan, G. Wang, Y.Y.; Shi, S. SKM: Scalable Key Management for Advanced Metering Infrastructure in Smart Grids. *IEEE Trans. Ind. Electron.* **2014**, *61*, 7055–7066. [CrossRef]
82. Sauter, T.; Lobashov, M. End-to-End Communication Architecture for Smart Grids. *IEEE Trans. Ind. Electron.* **2011**, *58*, 1218–1228. [CrossRef]
83. Wallner, D.; Harder, E.; Agee, R. *Key Management for Multicast: Issues and Architectures*; Technical Report; National Security Agency: Fort Meade, MD, USA, 1999.
84. Yu, K.; Arifuzzaman, M.; Wen, Z.; Zhang, D.; Sato, T. A key management scheme for secure communications of information centric advanced metering infrastructure in smart grid. *IEEE Trans. Instrum. Meas.* **2015**, *64*, 2072–2085.
85. Kim, V.K.; Thottan, M. Resilient End-to-End Message Protection for Cyber-Physical System Communications. *IEEE Trans. Smart Grid* **2018**, *9*, 2478–2487. [CrossRef]
86. Badra, M.; Serhrouchni, A. A new secure session exchange key protocol for wireless communications. In Proceedings of the 14th IEEE Proceedings on Personal, Indoor and Mobile Radio Communications, PIMRC 2003, Beijing, China, 7–10 September 2003; Volume 3, pp. 2765–2769. [CrossRef]
87. Mohammadali, A.; Haghighi, M.S.; Tadayon, M.H.; Mohammadi-Nodooshan, A. A Novel Identity-Based Key Establishment Method for Advanced Metering Infrastructure in Smart Grid. *IEEE Trans. Inf. Forensics Secur.* **2018**, *9*, 2834–2842. [CrossRef]
88. Nicanfar, H.; Leung, V.C.M. Multilayer consensus ECCbased password authenticated key-exchange (MCEPAK) protocol for smart grid system. In Proceedings of the IEEE International Conference on Communications (ICC), Ottawa, ON, Canada, 10–15 June 2012; pp. 6716–6720. [CrossRef]
89. Nicanfar, P.J.; Leung, V.C.M. Smart grid authentication and key management for unicast and multicast communications . In Proceedings of the IEEE PES Innovative Smart Grid Technologies, Perth, Australia, 13–16 November 2011. [CrossRef]
90. Tsai, J.L.; Lo, N.W. Secure Anonymous Key Distribution Scheme for Smart Grid. *IEEE Trans. Smart Grid* **2016**, *7*, 906–914. [CrossRef]
91. Liu, N.; Chen, J.; Zhu, L.; Zhang, J.; He, Y. A Key Management Scheme for Secure Communications of Advanced Metering Infrastructure in Smart Grid. *IEEE Trans. Ind. Electron.* **2013**, *60*, 4746–4756. [CrossRef]
92. Wu, D.; Zhou, C. Fault-Tolerant and Scalable Key Management for Smart Grid. *IEEE Trans. Smart Grid* **2011**, *2*, 375–381. [CrossRef]
93. Herzberg, A.; Mass, Y.; Mihaeli, J.; Naor, D.; Ravid, Y. Access control meets public key infrastructure, or: Assigning roles to strangers. In Proceedings of the 2000 IEEE Symposium on Security and Privacy. S&P 2000, Berkeley, CA, USA, 14–17 May 2000; pp. 2–14
94. David, P.; Olivier, S. Security and Cryptography for Networks. In Proceedings of the 9th International Conference, SCN 2014, Amalfi, Italy, 3–5 September 2014; Springer: Berlin/Heidelberg, Germany, 2014; pp. 21–39.
95. Huth, C.; Zibuschka, J.; Duplys, P.; Güneysu, T. Securing systems on the Internet of Things via physical properties of devices and communications. In Proceedings of the 2015 Annual IEEE Systems Conference (SysCon), Vancouver, BC, Canada, 13–16 April 2015; pp. 8–13. [CrossRef]
96. Seferian, V.; Kanj, R.; Chehab, A.; Kayssi, A. PUF and ID-based key distribution security framework for advanced metering infrastructures. In Proceedings of the 2014 IEEE International Conference on Smart Grid Communications (SmartGridComm), Venice, Italy, 3–6 November 2014; pp. 933–938. [CrossRef]
97. Kodýtek, F.; Lórencz, R. A Design of Ring Oscillator Based PUF on FPGA. In Proceedings of the 2015 IEEE 18th International Symposium on Design and Diagnostics of Electronic Circuits & Systems, Belgrade, Serbia, 22–24 April 2015; pp. 37–42. [CrossRef]
98. Wang, J.; Wu, L.; Choo, K.K.R.; He, D. Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure. *IEEE Trans. Ind. Inform.* **2019**, *16*, 1984–1992. [CrossRef]
99. Fouda, M.M.; Fadlullah, Z.M.; Kato, N.; Lu, R.; Shen, X.S. A Lightweight Message Authentication Scheme for Smart Grid Communications. *IEEE Trans. Smart Grid* **2011**, *2*, 675–685. [CrossRef]
100. Jo, H.J.; Kim, I.S.; Lee, D.H. Efficient and Privacy-Preserving Metering Protocols for Smart Grid Systems. *IEEE Trans. Smart Grid* **2016**, *7*, 1732–1742. [CrossRef]

101. Saxena, N.; Choi, B.J.; Lu, R. Authentication and Authorization Scheme for Various User Roles and Devices in Smart Grid. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 907–921. [CrossRef]
102. Li, H.; Lu, R.; Zhou, L.; Yang, B.; Shen, X. An Efficient Merkle-Tree-Based Authentication Scheme for Smart Grid. *IEEE Syst. J.* **2014**, *8*, 655–663. [CrossRef]
103. Chan, A.C.F.; Zhou, J. Cyber Physical Device Authentication for the Smart Grid Electric Vehicle Ecosystem. *IEEE J. Sel. Areas Commun.* **2014**, *32*, 1509–1517. [CrossRef]
104. Gazdar, T.; Rachedi, A.; Benslimane, A.; Belghith, A. A distributed advanced analytical trust model for VANETs. In Proceedings of the 2012 IEEE Global Communications Conference (GLOBECOM), Anaheim, CA, USA, 3–7 December 2012; pp. 201–206. [CrossRef]
105. Abdalzaher, M.S.; Muta, O. A game-theoretic approach for enhancing security and data trustworthiness in IoT applications. *IEEE Internet Things J.* **2020**, *7*, 11250–11261. [CrossRef]
106. Abdalzaher, M.S.; Seddik, K.; Muta, O. Using Stackelberg game to enhance cognitive radio sensor networks security. *IET Commun.* **2017**, *11*, 1503–1511. [CrossRef]
107. Abdalzaher, M.S.; Seddik, K.; Muta, O.; Abdelrahman, A. Using Stackelberg game to enhance node protection in WSNs. In Proceedings of the 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 9–12 January 2016; pp. 853–856.
108. Abdalzaher, M.S.; Seddik, K.; Elsabrouty, M.; Muta, O.; Furukawa, H.; Abdel-Rahman, A. Game theory meets wireless sensor networks security requirements and threats mitigation: A survey. *Sensors* **2016**, *16*, 1003. [CrossRef] [PubMed]
109. Abdalzaher, M.S.; Muta, O.; Seddik, K.; Abdel-Rahman, A.; Furukawa, H. B-18-40 A Simplified Stackelberg Game Approach for Securing Data Trustworthiness in Wireless Sensor Networks. In Proceedings of the 2016 IEICE General Conference, IEICE, Fukuoka, Japan, 15–18 March 2016; p. 538.
110. Abdalzaher, M.S.; Muta, O. Employing game theory and TDMA protocol to enhance security and manage power consumption in WSNs-based cognitive radio. *IEEE Access* **2019**, *7*, 132923–132936. [CrossRef]
111. Abdalzaher, M.S.; Seddik, K.; Muta, O. An effective Stackelberg game for high-assurance of data trustworthiness in WSNs. In Proceedings of the 2017 IEEE Symposium on Computers and Communications (ISCC), Heraklion, Greece, 3–6 July 2017; pp. 1257–1262.
112. Abdalzaher, M.S.; Seddik, K.; Muta, O. Using repeated game for maximizing high priority data trustworthiness in wireless sensor networks. In Proceedings of the 2017 IEEE Symposium on Computers and Communications (ISCC), Heraklion, Greece, 3–6 July 2017; pp. 552–557.
113. Abdalzaher, M.S.; Samy, L.; Muta, O. Non-zero-sum game-based trust model to enhance wireless sensor networks security for IoT applications. *IET Wirel. Sens. Syst.* **2019**, *9*, 218–226. [CrossRef]
114. Blanchet, B. An efficient cryptographic protocol verifier based on prolog rules. *Proc. CSFW* **2001**, *1*, 82–96.
115. Blanchet, B.; Smyth, B.; Cheval, V.; Sylvestre, M. ProVerif 2.00: Automatic Cryptographic Protocol Verifier, User Manual and Tutorial. 2018; pp. 5–16. Available online: https://bblanche.gitlabpages.inria.fr/proverif/manual.pdf (accessed on 1 August 2022).
116. Armando, A.; Basin, D.; Boichut, Y.; Chevalier, Y.; Compagna, L.; Cuellar, J.; Vigneron, L. The AVISPA Tool for the Automated Validation of Internet Security Protocols and Applications. Lecture Notes in Computer Science. *Lect. Notes Comput. Sci.* **2005**, *135*, 3576. [CrossRef]
117. How AVISPA Tool Validates Security Protocols and Applications? Learn Ethical Hacking and Penetration Testing Online. 4 October 2021. Available online: https://www.hackingloops.com/avispa-tool/ (accessed on 6 May 2022).
118. Lafourcade, P.; Terrade, V.; Vigier, S. Comparison of cryptographic verification tools dealing with algebraic properties. In Proceedings of the International Workshop on Formal Aspects in Security and Trust, Eindhoven, The Netherlands, 5–6 November 2009; pp. 173–185.
119. Cremers, C.J.; Lafourcade, P.; Nadeau, P. Comparing state spaces in automatic security protocol analysis. In *Formal to Practical Security*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 70–94.
120. Al Hamadi, H.; Yeun, C.; Zemerly, M.; Al-Qutayri, M.; Gawanmeh, A. Verifying mutual authentication for the DLK protocol using ProVerif tool. *Int. J. Inf. Secur. Res.* **2012**, *2*, 256–265. [CrossRef]