BULGARIAN ACADEMY OF SCIENCES

CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **19**, No 1
Sofia • 2019 Print ISSN: 1311-9702; Online ISSN: 1314-4081
DOI: 10.2478/cait-2019-0002

Recent Development in Smart Grid Authentication Approaches: A Systematic Literature Review

Malik Qasaimeh[1], *Raad S. Al-Qassas*[1], *Shadi Aljawarneh*[2]

[1]*King Hussein School of Computing Sciences, Princess Sumaya University for Technology, Amman, 11941 Jordan*
[2]*Faculty of Computer and Information Technology, Jordan University of Science and Technology, Irbid, 22110 Jordan*
E-mails: m.qasaimeh@psut.edu.jo raad@psut.edu.jo saaljawarneh@just.edu.jo

Abstract: *Smart Grid (SG) is a major electricity trend expected to replace traditional electricity systems. SG has faster response to electricity malfunctions and improved utilization of consumed power, and it has two-way communication between providers and consumers. However, SG is vulnerable to attacks and requires robust authentication techniques to provide secure authenticity for its components. This paper analyses previous literature, comprising 27 papers on the status of SG authentication techniques, main components, and kinds of attacks. This paper also highlights the main requirements and challenges for developing authentication approaches for the SG system. This can serve as useful guidance for the development and deployment of authentication techniques for SG systems and helps practitioners select authentication approaches applicable to system needs.*

Keywords: *Smart grid, Authentication, Smart meter, Key management.*

1. Introduction

Internet of Things (IoT) infrastructure needs network intelligence, power, energy optimization, and smart configurations to facilitate the operations of IoT functionalities [1, 2]. IoT is composed of a massive number of smart devices that are connected to the Internet in order to provide desired services to users. Smart devices gather data and send it to servers, which utilize it to serve smart applications such as medical and healthcare applications, intelligent transportation systems, and smart home applications [3, 4]. Smart Grid (SG) consists of millions of interacting and interconnected devices that are considered as the objects of the IoT systems. The concept of SG was developed to preserve power in increasingly demanding digital power distribution systems [5]. The Annual Energy Outlook 2017 forecast that energy supply would increase by over 20% from 2016 to 2040, led by increases in renewables, natural gas, and the improvement of power management and preservation systems [6]. SG consists of sub-networks that cover a wide range of services to provide efficient utilization for power management and various consumption types. This grid consists of smart meters, sensors, substations, transformers, and transmission lines that respond rapidly to changing electricity demands to deliver optimized energy value to consumers.

SG provides enhancement to existing grids with two-way communication between the utility, sensors, and consumers, by deploying smart sensors to monitor and manage power consumption [7-9]. They may consist of advanced sensors such as Phasor Measurement Units (PMUs), which allow many advantages such as automating the re-routes of power based on the current demand of the customers, saving energy by monitoring the consumption continuously and reducing it when possible. PMUs ensure the automatic reporting of outages to guarantee power stability, it may also diagnose problems faster by providing remote controls and solutions to diagnosed problems [10]. The smart grid provides many other advantages, such as reduced electricity losses and theft, reduced electricity cost, lower equipment failures, and the reduction of air emissions [11].

SG architecture may consist of three network categories: Home Area Network (HAN), Neighbourhood Area Network (NAN), and Wide Area Network (WAN). HAN consists of an important component called the Home Energy Management System (HEMS) that enables consumers to collect information about their consumption and electricity usage cost [12]. The NAN is used to collect the measured data from smart meters and PMUs, which it then transmits to the network of the utility company [10] (Fig. 1).

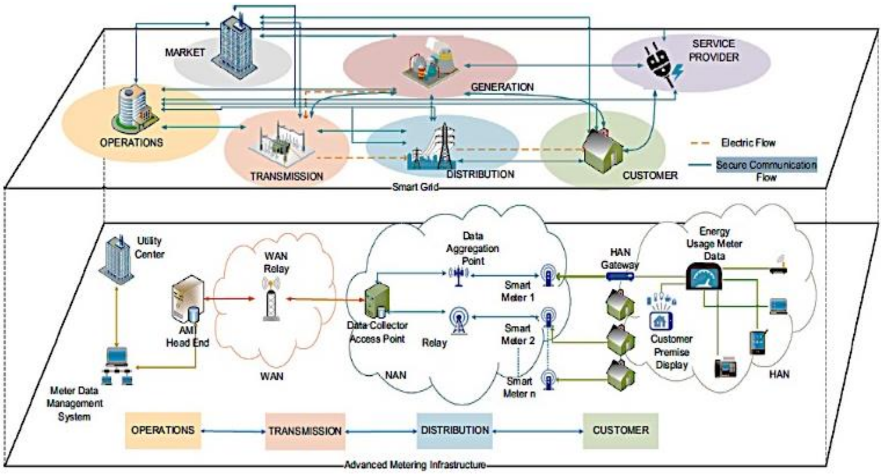

Fig. 1. SMART GRID components [**13**]

The SG infrastructure needs to preserve the security attributes of conventional systems, including confidentiality, integrity, and availability of services and utilities. However, many types of attacks can be deployed to compromise the SG security and functionality, such as eavesdropping and traffic analysis, spoofing, replaying attack, Denial of Services (DoS) and many other attacks that cause serious harm to SG services [14]. Attacks on SG systems range from changing the values of the smart meters to corrupting system utilities. For example, an attacker can corrupt the energy and usage data collected by the smart meters to reduce or increase the bills for artificial energy consumption values [15].

SG authentication is one of the important techniques that need to be implemented in SG communication to assure that sensitive data are transmitted properly between the SG components. The security of the SG highly depends on authentication techniques to ensure the authenticity, integrity, and privacy of the data exchanged between SG components [16]. The authentication technique needs to be optimal in SG networks to prevent attackers from modifying critical information, such as power utilization, which could cause erroneous billing and mendacious and incorrect usage approximation [17]. Utility providers in the SG must consider reliable authentication mechanisms to prevent attackers from invading the secrecy and privacy of the data exchanged among the SG components. Therefore, this paper extends the contribution in [18] and provides a systematic literature review about authentication in SG and studies existing SG techniques to answer questions about the optimum authentication technique to use; for which SG components; and for which threats.

The remainder of this paper is organized as follows. Section 2 discusses related work concerning SG attacks, while Section 3 provides the systematic review process. Section 4 presents and analyses the results, and Section 5 explores the validity of threats, and Section 6 discusses the findings and provides recommendations, then concludes the paper.

2. Related work

Researchers used multiple methods to conduct literature review and analysis for specific topics in computer science and software engineering. These methods include mainly the traditional reviews, scoping reviews, rapid evidence reviews, meta-analysis and systematic review. The traditional reviews usually summaries and categories multiple literature articles to extract conclusions that are related to specific research concerns. However, the traditional reviews usually follow less disciplinary approach on the way the reviews conducted and use less statistical methods to draw the extracted conclusions. An example of traditional reviews for SG security can be found in [19, 20], where various techniques, tools, frameworks and countermeasures were discussed to achieve SG security at both hardware and software levels. Scoping reviews is another method that is used in computer software engineering to identify key concepts and definitions in the literature for a particular topic. It is also used to as precursor of the systematic review aimed to clarify, analyse and examine research gaps on a certain topic. However, it provides less critically evaluation and synthesised outcomes in answering particular research questions compared to systematic review [21].

Rapid evidence reviews, meta-analysis and systematic review share some common processes such as identifying research questions, searching strategies, inclusion and exclusion criteria, study selection and data extraction. However, they differ in the way these processes are applied. For example, rapid evidence reviews investigate and select less studies to provide timely information related to the research gaps and conclusions when compared to systematic review and meta-analysis. On the other hand meta-analysis is a type of systematic review that relies on a standardized statistical analysis methods that are conducted on a large sample of selected studies and usually require more time and consumes more resources when compared to systematic reviews [22].

Previous studies have explored various authentication and authorization schemes in SG, such as comparing between different communication cryptographic algorithms based on the encryption and authentication techniques' characteristics, including resistance to attacks, advantages, and limitations [23]. However, this only reviewed cryptographic algorithms used in authentication. The survey concluded that public key infrastructure needs some simplification so that less effort is needed to manage it, and that stream ciphers are preferred in the energy bill over the block ciphers, because the amount of data exchanged would be less than that needed by the block cipher.

Farouk, Abdelhafez and Fouad [24] reviewed and compared the advantages and disadvantages of SG authentication mechanisms including one-time password, Kerberos, public key authentication, identity-based authentication, and biometric authentication, but they did not consider the threats that these techniques may mitigate. The study concluded that certificate-less authentication is suitable to be used in SG authentication, but that password-based authentication does not achieve mutual authentication, so it is suitable to be used in access control but not suitable in SG authentication.

Ji et al. [25] conducted a review of one-time signature schemes used in multicast authentication in SG and discussed the deployment and practicality issues of these schemes. The practicality issues of the existing signature schemes discussed in the paper include key management, storage cost, and suitability for SG multicast application. As a result, this paper claims that the best theoretical solution for one-time signature is the Time-Valid One-Time Signature (TV-OTS), which periodically refreshes the private keys used to generate signatures, but this scheme still lacks empirical evidence to support its use (i.e. practical results). The study only compared existing studies on the specific category of one-time signature.

Kumar and Agarwal [26] reviewed different cryptography algorithms and their key generation techniques used for SG authentication. The security of cryptographic algorithms depends on the randomness of keys, so the process of making noise as a seed helps prevention of attacks. The author concluded that lightweight algorithms are preferred in SG rather than conventional algorithms, because they have less memory, and asymmetric algorithms are better used for authentication, whereas symmetric algorithms are best deployed for message encryption.

3. Systematic literature approach

The objective of this paper is to identify and analyse the developments and implementations of authentication techniques used to advance the security of SG components. The Systematic Literature Review (SLR) methodology described in previous studies [27, 28] is implemented in this paper to achieve the stated objective and to answer the research questions. SLR provides a rigorous approach to identify relevant studies that are related to the research questions. This paper mainly investigates the SG authentication techniques published between 2010-2018 in IEEE Xplore (IEEE), ScienceDirect (Elsevier), and Springer Link (Springer) libraries. The search is based on the combination of multiple keywords in order to retrieve literature related to the formulated research questions. The searching process includes inclusion and exclusion phases, shown in Fig. 2, and the process is detailed below.

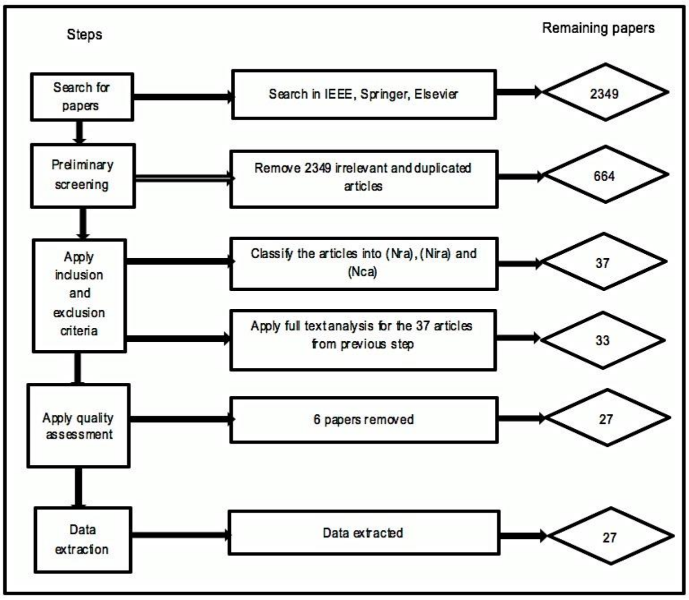
Steps
Remaining papers
Search for papers
Search in IEEE, Springer, Elsevier
2349
Preliminary screening
Remove 2349 irrelevant and duplicated articles
664
Apply inclusion and exclusion criteria
Classify the articles into (Nra), (Nira) and (Nca)
37
Apply full text analysis for the 37 articles from previous step
33
Apply quality assessment
6 papers removed
27
Data extraction
Data extracted
27

Fig. 2. Inclusion and exclusion process flow

3.1. Question formulization

The research questions follow the Population, Intervention, Comparison, and Outcome (PICO) paradigm mentioned in the guidelines for systematic literature review [27]. The *population* represents the articles that propose authentication techniques aimed to improve the security of SG components which are the WAN, LAN, and HAN. The investigated articles are either concerned with one of the components in the SG system or the overall improvement of the SG systems. The *intervention* is the software procedure or methodology that address a specific issue. In this context, the authentication techniques that address given issues is the intervention.

The *comparison* is the methodology or procedure with which the intervention is compared. In this context, the comparison is between different approaches used in the SG authentication process. The *outcome* is the meaningful results of the comparison between the SG authentication to answer the formulated research questions. This systematic review considers three key questions as follows.

RQ1. What approaches are available for SG authentication?

Addressing this question helps understand the special approaches deployed in primary studies in order to provide a robust solution for SG authentication. The objective is to investigate common security models and techniques used in the context of enhancing the SG authentication process.

RQ2. Which SG component should authentication techniques be applied to?

SG components consist of many entities that need to be authenticated to perform a specific task or process besides the requirements of authentication between the SG components. Addressing this question helps in classifying the authentication techniques based on the entities and the components of SG.

RQ3. What types of attacks do these authentication approaches mitigate?

SG components are vulnerable to many types of attacks, such as malicious software, spoofing, viruses, DoS attacks, and many others. Addressing this question helps in understanding the common types of attacks that could threaten the SG system and in classifying the authentication techniques based on the attacks they are intended to mitigate.

3.2. Literature search protocol

3.2.1. Digital libraries investigation

To identify the recent developments in SG authentication, the IEEE Xplore (IEEE), ScienceDirect (Elsevier) and Springer Link (Springer) digital libraries were selected to search for potentially relevant publications between 2010- June 2018. The targeted digital libraries' publications are widely listed with Scopus indexing. Scopus claims to have the largest database of peer-reviewed articles. In order to find the most related research or to identify further articles from these digital libraries, a direct search using various search keywords was conducted, as described in Table 1. Then, based on the PICO paradigm, the search keywords were initially derived. The keywords were concatenated using the Boolean operators AND and OR to create query strings, as shown in Table 1. The table shows the initial closely matched keywords and the derived query strings based on the following specification:

- Population: Power generation industry.
- Intervention: Authentication technique.
- Comparison: SG authentication.
- Outcome: Technique effectiveness.

Table 1. Search keywords

Keywords	Closely matched keywords	Combination using AND/OR (key string)
Smart grid	Electrical grid	Smart grid AND effective AND authentication technique OR key management (S1) Electrical grid AND effective AND authentication technique OR key management (S2)
Authentication techniques	Key management, digital signatures	Smart grid AND effective OR high quality AND digital signatures (S3) Electrical grid AND effective OR high quality AND digital signatures (S4)
Effective	High quality	Smart grid AND high quality AND authentication technique OR key management (S5) Electrical grid AND high quality AND authentication technique OR key management (S6)

3.2.2. Selection execution

The targeted digital libraries were investigated using the query strings defined in Table 1. The key strings revealed different numbers of related articles form each digital library. The revealed articles derived from specific digital libraries were collected in a CSV-format spreadsheet, then a script was developed to find the duplication and the intersection between the spreadsheets to collect the identical articles retrieved based on the key strings. The resulting number of articles was huge, and further selective investigation was needed to assess whether the extracted articles are related to the research questions or not, based on the article title. This process reduced the number of articles to 664. In this stage, the articles that did not consider authentication techniques in SG were excluded. Examples of the papers that were excluded based on title included articles considering authentication technique for smart card, not SG [29], not considering authentication [30], and considering authentication in the context of smart cities, rather than smart grid authentication [31].

The 664 articles were given to first and the second authors (i.e., reviewers) to conduct further refinement independently, based on the exclusion and inclusion process, which was subject to the research questions before the extraction of articles from the identified sources. The objective of this process was to exclude the articles not covering authentication techniques used in SG, or those with an abstract that did not clearly define the authentication technique, or the type of threat mitigated. Based on the exclusion and inclusion process, both reviewers where asked to examine the title and the abstract of the articles and to provide their outcomes into three categories: relevant articles (Nra); articles that propose authentication techniques that are relevant to the research questions, irrelevant articles (Nira); articles that propose techniques that are not relevant to the research questions, and conceivable articles (Nca); and articles that could not be determined as relevant to the research questions based on screening the abstract. Examples of reasons for articles being excluded based on their abstracts include not clearly specifying the authentication technique [32] and/or threats mitigated [33].

The reviewers noticed that some authors proposed their authentication techniques in multiple studies with different motivations, objectives, and/or experimental evaluation. In such cases, the reviewers were asked to investigate the most recent study related to similar authentication techniques and aligned with the research questions. To remove any bias from the reviewers' assessment, the outcomes from the assessment of the first and the second reviewers were passed on to a third reviewer for further assessment. Then a discussion session has been held in the presence of all reviewers to exclude the articles deemed irrelevant by at least one reviewer, which led to generating consensus on a articles for inclusion and exclusion based on their titles and abstracts. Finally, as illustrated in Fig. 2, the full-text analysis was conducted and a total of 33 articles was obtained. The figure shows the study selection process and the total number of articles before and after the exclusion. The initial search on the topic retrieved a very huge number of articles; in the first stage, a total of 664 papers were extracted based on their titles.

The first and second reviewers considered 35 and 31 articles as relevant (Nra), respectively. In the next step, the reviewers agreed based on the screening of the

(Nra), (Nira), and (Nca) to consider only 34 articles as relevant articles (Nra). However, after a further refinement based on the full-text analysis, only 33 articles were considered as relevant articles (i.e., primary studies). Finally, the quality assessment criteria were applied to ensure the validity and rigor of the primary studies and 6 papers were excluded.

3.2.3. Quality assessment

The quality assessment criteria aimed to decrease the bias of articles selection and to ensure that rigorous criteria were applied to assess the quality of the selected articles. These criteria were based on an unbiased strategy to evaluate the selected articles, maximize validity, minimize biases, and identify which articles clearly addressed the research questions, as shown in Table 2.

Table 2. Quality assessment criteria

No	Question	Answer
Q1	Is the research purpose clearly stated in the article?	Yes/ No/ Indistinctive
Q2	Does the paper topic cover the power generation domain?	Yes/ No/ Indistinctive
Q3	Does the paper use a mechanism, tool, framework, or methodology?	Yes/ No/ Indistinctive
Q4	Is the mechanism, tool, framework, or methodology used in the paper relevant to the research questions?	Yes/ No/ Indistinctive
Q5	Are the authentication approaches fully defined?	Yes/ No/ Indistinctive
Q6	Are the authentication approaches verified?	Yes/ No/ Indistinctive

The scoring for the quality criteria was conducted as follows: **Yes** means that the article clearly answered the criteria without ambiguity, and the criteria are given 1 in this case; **No** means that the article absolutely contrasts the assessment criteria, and hence scores 0; and **Indistinctive** means that the case is ambiguous and needs more reading or partially applied hence the score is 0.5. The papers that passed the qualitative assessment with a percentage greater than 50% are shown in Table 3.

Table 3. Qualitative assessment results

Article ID	Source	Year	Q1	Q2	Q3	Q4	Q5	Q6	Total	Percentage compliance
PS1 [34]	IEEE	2012	1	1	1	1	1	1	6	100
PS2 [35]	IEEE	2012	1	1	1	1	1	0.5	5.5	91.66
PS3 [36]	IEEE	2017	0.5	1	1	1	0.5	0.5	4.5	83.33
PS4 [37]	IEEE	2013	1	1	1	1	1	0.5	5.5	75.00
PS5 [38]	IEEE	2015	0.5	1	0.5	1	0.5	0.5	4	83.33
PS6 [39]	IEEE	2011	1	1	1	1	1	0.5	5.5	66.66
PS7 [40]	IEEE	2013	1	1	1	1	0.5	1	5.5	91.67
PS8 [41]	IEEE	2011	0.5	1	0.5	0.5	1	0.5	4	66.66
PS9 [42]	IEEE	2011	1	1	1	1	1	1	6	100
PS10 [43]	IEEE	2013	0.5	1	0.5	0.5	0.5	0.5	3.5	58.33
PS11 [44]	IEEE	2014	1	1	1	0.5	1	1	5.5	91.67
PS12 [45]	IEEE	2017	1	1	1	1	1	1	6	100
PS13 [46]	IEEE	2012	1	1	1	0.5	1	1	5.5	91.67
PS14 [47]	IEEE	2018	1	1	1	1	1	1	6	100
PS15 [48]	IEEE	2018	1	1	1	1	1	1	6	100
PS16 [49]	Science Direct	2017	1	1	1	1	1	1	6	100

Table 3 (continued)

Article ID	Source	Year	Q1	Q2	Q3	Q4	Q5	Q6	Total	Percentage compliance
PS17 [50]	Science Direct	2016	1	1	1	1	1	1	6	100
PS18 [51]	Science Direct	2018	1	1	1	1	1	1	6	100
PS19 [52]	Science Direct	2015	1	1	1	1	1	1	6	100
PS20 [53]	Science Direct	2018	1	1	1	1	1	1	6	100
PS21 [54]	Science Direct	2018	1	1	1		1	0.5	5.5	91.67
PS22 [55]	Springer Link	2016	1	1	1	0.5	1	0.5	5	83.34
PS23 [56]	Springer Link	2016	1	1	1	1	1	1	6	100
PS24 [57]	Springer Link	2013	0.5	1	1	1	1	0.5	5	83.34
PS25 [58]	Springer Link	2017	1	1	1	1	1	1	6	100
PS26 [59]	Springer Link	2015	1	1	1	1	1	1	6	100
PS27 [60]	IEEE	2014	1	1	1	1	1	1	6	100

3.3. Information extraction

The information extraction process focused on information related to the research questions. The important information extracted included:

The approach used for authentication between the SG components.
An attack that this approach mitigates.
Vulnerabilities it addresses.
The SG component upon which the method was implemented.

4. Results and analysis

4.1. SG authentication approaches (RQ1)

The process for answering this question involved analysis of the techniques on which the authentication is relying. We investigated for each primary study the techniques used to design the authentication approach for the SG components, as shown in Table 4. The authentication techniques have been categorized into a set of approaches illustrated in Table 5. This categorization is identified based on the classification indicated by the authors of the primary studies. Almost all the primary studies use cryptography to some extent to authenticate the SG components, however we have considered the approach as cryptographic-based if it relies on known cryptographic techniques, such as symmetric key encryption, hash function, and Diffie-Hellman, etc. Otherwise, we refer to the main category to which the approach belongs, as indicated by the author of the primary study; for example, if the approach used password techniques to authenticate the SG component, and it deployed one of the encryption techniques in one of its phases, in this case the approach is classified as a password-based approach.

Table 4. Approach used in smart grid authentication

Article ID	Authentication approach	Classification
PS1 [34]	Biometric fingerprint authentication	Biometric
PS2 [35]	Broadcasting symmetric key encryption using MKB (Media Key Block) to distribute and extract the keys	Cryptography (broadcast)
PS3 [36]	Cryptography symmetric key encryption using a hash function to distribute keys	Cryptography (hash)
PS4 [37]	Scalable and automated password-changing approach	Password
PS5 [38]	TESLA-based source authentication	Cryptography (hybrid)
PS6 [39]	Cryptography using pair-wise keys, including message authentication code to check key integrity	Cryptography (hybrid)
PS7 [40]	Signature-based using (TV-OTS)	Signature
PS8 [41]	Cryptographic mutual authentication and two secret values to ensure non-repudiation and integrity	Cryptography (hash)
PS9 [42]	Cryptography using hash-based message authentication code and Diffie-Hellman key establishment	Cryptography (diffie)
PS10 [43]	The secure chip that stores the provider credentials such as IP address, provider address, and associated phone number in a file included in the chip	Hardware
PS11 [44]	Cryptography using Merkel trees depending on a hash function	Cryptography (hash)
PS12 [45]	Hardware authentication approach using Ring Oscillator Physically Unclonable Function (RO PUF) to derive keys	Hardware
PS13 [46]	Password and symmetric key, and one hash function to ensure key integrity	Password
PS14 [47]	Authentication approach based on certificateless cryptosystem	Cryptography (hybrid)
PS15 [48]	Lightweight authentication approach using elliptic curve	Cryptography (elliptic)
PS16 [49]	Cryptography using Diffie-Hellman key establishment and timestamps	Cryptography (diffie)
PS17 [50]	Cryptography based on lightweight Diffie-Hellman	Cryptography (diffie)
PS18 [51]	Authentication approach using elliptic curve cryptography	Cryptography (elliptic)
PS19 [52]	Cryptography using PUF to derive keys	Hardware
PS20 [53]	Enhanced elliptic curve cryptography-based authentication	Cryptography (elliptic)
PS21 [54]	Lightweight elliptic curve approach using third party	Cryptography (elliptic)
PS22 [55]	Cryptography using public key scheme with password data validation at server	Password
PS23 [56]	Source authentication based on the concept of inf-TESLA	Cryptography (hybrid)
PS24 [57]	Cryptography using a hash function with a secret key shared between parties, Hash-based Message Authentication Code (HMAC)	Cryptography (hash)
PS25 [58]	Cryptography used a key exchanged protocol based on chaotic maps	Cryptography (chaotic)
PS26 [59]	Signature and secret key based Efficient Authentication protocol against Pollution Attack (EAPA)	Signature
PS27 [60]	Merkle-tree-based authentication scheme for SG	Cryptography (hash)

Table 5. Approaches frequency distribution used in the studies

Approach		Frequency	Percentage
Cryptography-based	Classification and mapping		
	Hybrid encryption	5	66.67
	Hash function	4	
	Diffie-Hellman	3	
	Elliptic curve	4	
	Chaotic maps	1	
	Broadcast encryption	1	
Password-based		3	11.11
Hardware-based		3	11.11
Signature-based		2	7.40
Biometric-based		1	3.70

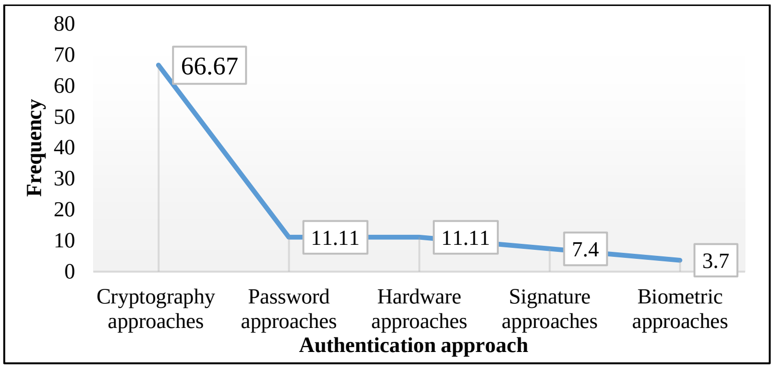

Fig. 3. Frequency distribution of authentication approaches

An exception is given to the hybrid encryption category, where the techniques are either based on multiple encryption methods, such as symmetric key encryption, public key encryption, and other encryption techniques, or the authors of the primary studies did not provide any clear classification of the technique (Table 5, Fig. 3). The following five subsections briefly discuss each category.

4.1.1. Cryptographic-based approaches

Cryptographic techniques were deployed extensively in SG authentication such as hybrid encryption, hash function, Diffie-Hellman, elliptic curve, chaotic maps, and broadcast encryption. Each subcategory is described below.

Hybrid encryption authentication approaches were deployed in PS5, PS6, PS14, PS23, and PS24, with hybrid encryption equivalent to 18.5% of the selected primary studies, and 27.7% from those were classified to fit cryptographic-based approaches; this percentage represents the highest number of studies that fit into one category. The approaches in this category were designed to preserve the low computation power and energy of the SG components, for example PS5 and PS23 deployed the Timed Efficient Stream Loss-tolerant Authentication (TESLA) method, which includes the benefits of lower computation overhead, less overhead of packet communication, and toleration for packet loss. TESLA relies on the concept of symmetric keys, which are first generated in a one-way chain and disclosed in a reversed order, then the messages are buffered before being authenticated. In the approach presented in PS5 the authenticated SG components need to be loosely synchronized, TESLA could be useful for SG components, because the timely gathering of the correct energy data is much more important than real-time processing for the data. PS23 proposes inf-TESLA for multicast streaming data in the SG suitable for long-duration communication and high-volume data rates. Inf-TESLA solves the problem of frequent signing and resynchronization by the deployment of Dual Key Chains technique, to ensure the continuity of the streaming authentication process.

PS6 developed intuitive authentication approach suitable for SG system. The approach relies on the symmetric key encryption and sharing pairwise keys between the grid components, and all transmissions are encrypted before being transmitted. The approach claimed to be suitable for the low power computation of the SG components. PS14 proposed an authentication approach based on a certificate-less cryptosystem relying upon a combination of public key technique and identity-based cryptography. The approach overcomes the problem of costly private key generation in PKI by the use of Key Generation Centre (KGC). It is claimed that the approach provides a lightweight authentication process that guarantees fast execution and provides a central control for the SG component. In PS24, the approach is based on symmetric key encryption and Hash-based Message Authentication Code (HMAC), aiming to provide a mutual authentication between the SG components that require two-factor authentication, whereby the component needs multiple evidence to guarantee successful authentication.

Authentication approaches explicitly based on hash functions were used in PS3, PS8, PS11, and PS27. Authentication approaches based on hash functions were equivalent to 22.22% of the selected primary studies, and 14.8% of these were classified to fit the cryptographic-based approaches. In PS3 the authors used the one-way hash function to overcome the limitation of symmetric encryption, which could be vulnerable to impersonation attacks, and a similar approach was presented in PS8 to mitigate repudiation attack. PS11 and PS27 both used Merkle tree to provide robust authentication for the SG components. A Merkle tree is a binary tree created from a set of leaf tokens, whereby each internal node of the tree is a hash of its left and right child.

The next subcategory are the approaches based on elliptic curve, which were explicitly indicated by the primary studies PS15, PS18, PS20, and PS21. The authentication approaches based on elliptic curve were equivalent to 14.8% of the selected primary studies, and 22.22% of primary studies classified as cryptographic-based approaches. PS15 provides mutual authentication between the SG components based on an SM2 elliptic curve, and the mutual authentication is started once the connection between the SG centre and terminals is initiated. The proposed approach monitors connections that are time-outed to close the session. The proposed approach in PS15 is claimed to provide lightweight computation and power to comply with the limitations of SG devices.

The approach in PS18 is also based on the elliptic curve and designed to overcome the limitation presented in [54], which is found to be vulnerable to the Canetti-Krawczyk model, with some limitations to support the perfect secrecy. An enhanced version of the elliptic curve form used in PS15 was presented in PS20. PS21 proposed a lightweight elliptic curve approach using a third party for participant registration (to initiate the authentication process). The process is terminated once the key session is exchanged between the participants.

The authentication approaches based on Diffie-Hellman comprised 11.11% of the selected primary studies, and 16.66% of the primary studies classified as using cryptographic-based approaches. Diffie-Hellman was deployed in PS9, PS16, and PS17. In PS9 the authors utilized the Diffie-Hellman exchange protocol and hashing code to share the session key and to provide mutual authentication. In PS16 the authors implemented their approach using initialization, authentication, and message transmission phases. Mainly based on Diffie-Hellman, the approach uses discrete logarithm problem to achieve its objectives. In PS17 the proposed approach was based on Diffie-Hellman, using AES and RSA to meet its objectives. Finally, only PS2 and PS25 used the broadcast encryption and chaotic maps to enable the key distribution between the SG components.

4.1.2. Password-based approaches

The authentication approaches classified in this category are equivalent to 11.11% of the selected primary studies. Password-based approaches have been deployed in PS4, PS13, and PS22. In PS4 the authors proposed a password-based authentication approach called SCAPACH which generates a new password at the beginning of each authenticated session. The generated passwords are short living and automatically formed based on multiple parameters, such as local time, geographical location, and device ID, etc., PS13 presented SG-MCPEAK protocol, which provides multilayer password authentication using symmetric keys to provide mutual authentication between the SG components. Finally, PS22 presents two password authentication protocols called SSCA and PSCAb. The first approach utilized the concept of symmetric key encryption, and the second utilized the concept of public key encryption.

4.1.3. Hardware-based approaches

The authentication approaches classified in this category are equivalent to 11.11% of the selected primary studies. The hardware-based approaches were deployed in PS10, PS12 and PS19. In PS10 the authors proposed a smart chip integrated with reliable crypto algorithms to provide SG component users with mobility, security, and high-performance data processing. The proposed chip can operate on multiple crypto algorithms, such as public key, symmetric key, and hash function to provide authentication between the SG components. PS12 proposed an end-to-end hardware-based authentication approach developed using Physically Unclonable Function (PUF) and implemented using Xilinx Spartan 3E FPGA boards. PUFs can be integrated with the microprocessor to provide a unique identity for the device. PS19 also used the PUF concepts to develop hardware ordinated aligned with the requirements of Advanced Metering Infrastructures (AMIs).

4.1.4. Signature-based approaches

The authentication approaches that classified in this category is equivalent to 7.4% of the selected primary studies. The hardware-based approaches were deployed in PS7and PS26. In PS7 the authors utilized the concept of Time-Valid One-Time-Signature (TV-OTS) to create individual signatures by periodically initiating new secret keys using Hash Of Random Subsets (HORS). The authentication approach claimed to provide real-time, multicasting, dynamic, and secure authentication for the SG components. PS26 could be classified also as a hybrid encryption approach, however, we prefer to classify it in this category, since it is of one the few approaches that use signatures during the authentication process. PS26 used both homomorphic signature and Message Authentication Codes (MAC) to secure the authentication process. The homomorphic signature is used to sign the data packets that are initiated from the same resources, and the MAC is used to generate a unique tag for each packet.

4.1.5. Biometric-based approaches

The authentication approaches classified in this category is equivalent to 3.7% of the selected primary studies. The biometric based approaches were deployed in PS1, in which multiple authentication approaches were investigated for their utility in modern networks. The approach used AES to protect the privacy of the fingerprints collected to authenticate the users of the SG systems. The fingerprints were stored in a database and categorized into two categories, which are sparse and rich minutiae fingerprints.

It is worth mentioning that cryptography and hash techniques are heavily deployed on the selected primary studies. The category of hybrid encryption approaches consists of the primary studies that utilize different types of cryptography and hash techniques on equivalent basis. Moreover, it has been noted that some primary studies can fit another category as a secondary classification as indicated in Table 6. For example PS4, PS7, PS10, PS13, PS22 and PS25 can fit into hash functions category as a secondary classification beside of its main classification. PS18 and PS20 can fit into hardware approaches as a secondary classification beside of its main classification. PS4, PS12 and PS19 can fit into signature approaches as a secondary classification beside of its main classification. Finally, PS2 can fit into elliptic curve approaches as a secondary beside of its main classification.

Table 6. Secondary classification of authentication approaches

Article ID	Main classification	Secondary classification
PS2	Cryptography (broadcast)	Cryptography (elliptic curve)
PS4	Password approach	Cryptography (hash function)
PS7	Signature approach	Cryptography (hash function)
PS10	Hardware approach	Cryptography (hash function)
PS13	Password approach	Cryptography (hash function)
PS22	Password approach	Cryptography (hash function)
PS25	Cryptography (chaotic maps)	Cryptography (hash function)
PS18	Cryptography (elliptic curve)	Hardware approach
PS20	Cryptography (elliptic curve)	Hardware approach
PS12	Hardware	Signature approach
PS19	Hardware	Signature approach

4.2. Authenticated SG components (RQ2)

The process for answering this question involved an analysis of the main components of SG that the proposed authentication approach is required to handle and manage. We first refer to the categorization and description of the main SG entities and components. The main components are Wide Area Networks (WAN), Neighbourhood Area Networks (NAN), and Home Area Networks (HAN), as described in [61]. The SG entities are defined as any subcomponents that belong to WAN, NAN, and HAN, for example, customers, smart meters, data collectors, utility providers, home appliances, and so on.

We also classified the SG entities that belong to each component. Thus, we investigate the authentication approaches in the primary studies by identifying the components and the entities that the approach needs to handle. This was accomplished by first identifying whwther the authors explicitly mentioned the handled components or entities that the authentication approach tackles. In case the tackled components are not mentioned explicitly, we refer to the process of authentication approach, then the classification is made according to the involved entities and components.

Table 7 shows the classification of the authentication approaches based on the involved entities and components. The frequency distribution of the addressed components is shown in Table 8 and Fig. 4. The figure shows that out of 27 primary studies, 14 (55.57%) handled the HAN authentication, eight handled NAN (29.62%), and four (14.81%) handled WAN. The HAN authentication approaches attracted the highest intentions among the other SG components, since the data processed by HAN mostly consists of private information related to customer data, used by the utility company and other SG components to formulate critical decisions, thus any compromise of HAN data security is particularly serious.

Most HAN authentication approaches target smart meter information. This information is vital and consists of consumers' usage data, which is aggregated and forwarded to the utility company. The smart meter also has the capability to assess the availability of the energy and approve or reject requests from various power ports accordingly. The smart meter can also manage and prioritise the activation of power ports to incentive the cost savings. The proposed authentication approaches are designed to maintain the confidentiality, integrity, authenticity and the availability for entities of HAN, NAN, and WAN. For example, the proposed approaches are designed to assure that the HAN information is not accessible by any other party, and that only the customer and the utility company can exchange the protected information based on a predefined legal agreement. The integrity is also guaranteed by ensuring that smart meter information and other collected information in the HAN is not altered, since any modification of this sensitive data can affect customer consumption of power, billing, and power ports activation processes. Information exchanged between the smart meter, power ports, and customers' needs to be processed only after the identity of each entity is verified. The designed approaches have considered maintaining the availabilities of the SG services by considering several mitigation techniques against attacks that compromise the availability of SG services.

Table 7. Component of the authentication mechanism

Article ID	Entities involved in the authentication approach	Component classification
PS1 [34]	Consumers and smart meters	HAN
PS2 [35]	Between PMU and data concentrator	NAN
PS3 [36]	Consumers and Smart meters	HAN
PS4 [37]	Operators or service providers and meters	WAN
PS5 [38]	Smart meters and utility systems or data collectors	NAN
PS6 [39]	Between gateway and meters, and smart appliances and meters	HAN
PS7 [40]	Between PMU and smart meters	HAN
PS8 [41]	Customers and smart meters	HAN
PS9 [42]	Customers and smart meters	HAN
PS10 [43]	Between smart meters and home appliances	HAN
PS11 [44]	Between data collectors and data centres	WAN
PS12 [45]	Smart meters and utility systems or data collectors	NAN
PS13 [46]	Between HAN controller and appliances	HAN
PS14 [47]	Between electronic vehicles and smart meters	HAN
PS15 [48]	SG control centre and SG terminals	WAN
PS16 [49]	(HAN) gateway	HAN
PS17 [50]	(HAN) gateway	HAN
PS18 [51]	Smart meters and service providers	HAN
PS19 [52]	Between data collectors and data centres	WAN
PS20 [53]	Between smart meters and the BAN gateway	NAN
PS21 [54]	Smart meters and utility systems or data collectors	NAN
PS22 [55]	Smart meters and data collectors	NAN
PS23 [56]	Between PMU and smart meters	HAN
PS24 [57]	Between consumer, smart meters, and control centre	NAN
PS25 [58]	Home appliances	HAN
PS26 [59]	Between consumer, smart meters, and control centre	NAN
PS27 [60]	Smart meters and service providers	HAN

Table 8. Frequency distribution of smart grid components in the studies

SG network component	Frequency	Percentage
Home Area Networks (HAN)	15	55.57
Neighbourhood Area Networks (NAN)	8	29.62
Wide Area Networks (WAN)	4	14.81

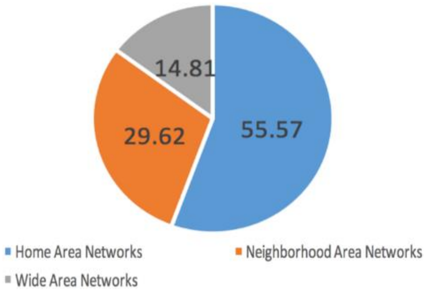

Fig. 4. Frequency distribution of authentication approaches on smart grid components

Fig. 5 and Table 9 show the relationships between the authentication techniques and the targeted SG components. It can be seen that the cryptography-based approaches are mostly used to authenticate the HAN, NAN, and WAN, with noticeably higher deployments in HAN network. Eleven primary studies out of 18 classified as cryptography-based approaches targeted the HAN; five targeted NAN, and two targeted WAN. The other approaches, such as password-based, hardware-based, signature-based, and biometric-based approaches have also been deployed in HAN, with the frequency of one primary study only for each category.

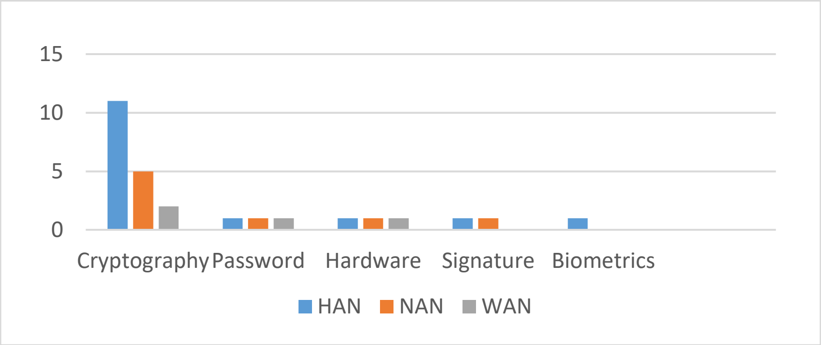

Fig. 5. Relation between SMART GRID components and authentication techniques and smart grid components

The primary studies that focus on HAN and belong to the cryptographic-based approach are PS3, PS6, PS22, PS9, PS16, PS14, PS17, PS18, PS23, and PS25, which are related to hybrid, elliptic curve, Diffie-Hellman, hash function and chaotic map approaches. While those approaches preserve the confidentiality, integrity, and availability of the HAN, they also have other attributes, such as safety for the in-house stakeholders from any serious harms, to protect the smart devices from being corrupted by any false operation of the authentication process. QoS is another important attribute that the primary studies investigated for the components of the SG. Any authentication protocol must consider the trade-off between the robustness of the authentication approaches and the QoS for applications, especially in HAN.

4.3. The mitigated threat of authentication mechanism (R3)

The process for answering this question involved an analysis of the types of threats and attacks that the proposed authentication process mitigated. Each of the primary studies proposed to mitigate one or more different types of threats. Table 10 categorizes the main types of the identified attacks collected from the primary studies, on the base of which we calculated the frequency for each type of attacks in the primary studies to understand the frequency and the distributions of the mitigated attacks. Table 11 and Fig. 6 show the frequency distribution mitigated attacks in the primary studies. It can be seen that the main identified categories for the mitigated attacks are *impersonation*, *eavesdropping*, *brute force*, *Man-in-The-Middle* (MiTM), repudiation, spoofing, replay, and dictionary. A separate category called other *attacks* was identified for the attacks that have only one frequency in the primary studies, including *insider*, *DoS*, *modification*, *pollution*, *quantum computer*, *data forgery*, and *information leakage* attacks.

Table 9. Relation between smart grid components and authentication techniques

Authentication technique	SG component	Frequency
Cryptography-based approaches	HAN	11
	NAN	5
	WAN	2
Password-based approaches	HAN	1
	NAN	1
	WAN	1
Hardware-based approaches	HAN	1
	NAN	1
	WAN	1
Signature-based approaches	HAN	1
	NAN	1
	WAN	0
Biometric-based approaches	HAN	1
	NAN	0
	WAN	0

The analysis shows that the highest mitigated attack in the primary studies was man-in-the-middle, with a percentage of 21.66% of the total identified attacks. Some authors consider that impersonation attack and MiTM are similar, however we classified them in different categories based on the majority of the primary studies' classifications. For example PS6, PS14, PS15, PS16, and PS21 illustrate specific mitigation techniques for MiTM that differ from mitigation techniques for impersonation attack. The percentage of impersonation attack was also high (16.66%) among the total identified attacks in the primary studies. In the context of MiTM and impersonation attack, the authentication approaches aim to prevent any malicious smart meter from masquerading as a legitimate smart meter, and to avoid any illegal third party from accessing the data exchanged between the SG components, to prevent any damage, such as dropping and corrupting the data packet, crippling and degrading the SG network, or launching secondary attacks, such as flooding and DoS attacks.

The analysis also shows that the replay attack was counted with high frequency, representing 18.33% of the total identified attacks in the primary studies, particularly in PS13, PS14, PS15, PS16, PS17, PS18, PS20, PS21, PS25, and PS26, which specified how their proposed techniques help mitigate the replay attack. The proposed authentication approaches aimed to prevent attackers from interrupting the data transmitted between smart meters, in which the attacker can replay the information after performing some modifications with the intention of illegal access to the SG components. Eavesdropping was also mitigated with a percentage of 10.00% from the total identified attacks in the primary studies, particularly in PS4, PS5, PS12, PS15, PS17, and PS25, to prevent the attackers from listening or recording the data transmission between the SG components, particularly between the smart meters and the customer applications. Eavesdropping compromises system privacy and enables illegitimate actions, such as theft of smart meters' data (e.g., for studying the system and customer behavioural patterns) and customer identity fraud.

Table 10. Threats mitigated using the authentication approach

No	Article ID	Threat (attack) mitigated
1	PS1 [34]	Impersonation
2	PS2 [35]	Information leakage by crackers
3	PS3 [36]	Impersonation
4	PS4 [37]	Eavesdropping, brute force
5	PS5 [38]	Eavesdropping, MiTM
6	PS6 [39]	MiTM, impersonation
7	PS7 [40]	Brute force
8	PS8 [41]	Repudiation
9	PS9 [42]	Spoofing, MiTM
10	PS10 [43]	Impersonation, data forgery
11	PS11 [44]	Quantum computer
12	PS12 [45]	Eavesdropping, spoofing, MiTM
13	PS13 [46]	MiTM, off-line dictionary, replay
14	PS14 [47]	Impersonation, MiTM, repudiation, replay
15	PS15 [48]	Replay, impersonation, message injection, MiTM, eavesdropping
16	PS16 [49]	Impersonation, MiTM, replay
17	PS17 [50]	Replay, MiTM, eavesdropping
18	PS18 [51]	Impersonation, MiTM, replay
19	PS19 [52]	Spoofing
20	PS20 [53]	Replay, modification, DoS, insider
21	PS21 [54]	Replay, impersonation, MiTM
22	PS22 [55]	Off-line dictionary
23	PS23 [56]	MiTM
24	PS24 [57]	Brute force, impersonation
25	PS25 [58]	Eavesdropping, dictionary, replay
26	PS26 [59]	Pollution (inject fake data packets), replay
27	PS27 [60]	Replay, modification

Table 11. Frequency distribution of SMART GRID threats mitigated in the studies

Threat	Frequency	Percentage
Impersonation	10	16.66
Eavesdropping	6	10.00
Brute Force	3	5.00
MiTM	13	21.66
Repudiation	2	3.33
Spoofing	3	5.00
Replay	11	18.33
Dictionary	3	5.00
Other attacks (insider, DOS, modification, pollution, quantum computer, data forgery, information leakage)	9	15.00
Total	60	100

Brute force, dictionary, and spoofing attacks were counted equivalently with a frequency of 5.00% each from the total identified attacks in the primary studies. The mitigation against brute force and dictionary attacks aimed to prevent compromising SG security by obtaining passwords that play important roles in authentication between users, smart meters, and other parts of the SG system, such as gateways and data aggregation points, and extending all the way to the utility company itself. The passwords are usually stored in tables, which are protected by the authentication techniques proposed by the primary studies from access by illegitimate third parties.

Spoofing was also handled by providing mutual authentication between the SG entities and components to prevent adversaries from obtaining the encryption/ decryption keys and from harassing the authentication processes. Finally, all the attacks counted in a low frequency in the primary studies, such as insider, DoS, modification, pollution, quantum computer, data forgery, and information leakage attacks, were categorized in *other attacks*, which collectively represent 15.00% of mitigated attacks in the primary studies.

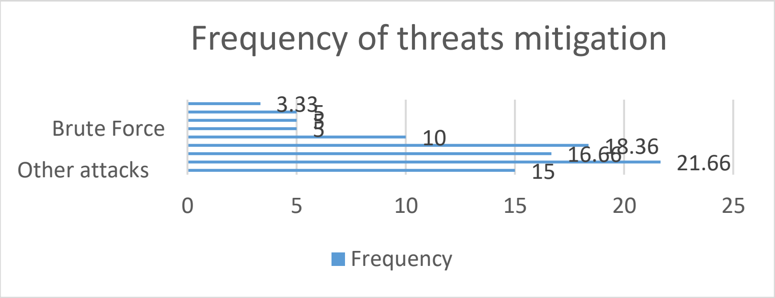

Fig. 6. Frequency distribution of threats mitigation in smart grid

5. Validity

5.1. Resolving searching bias

To alleviate the selection bias of the primary studies and raise the possibility that the results being searched were representative to the target population, two different approaches were used. The first approach was used in [62] to improve the search string in the selected digital libraries (IEEE, Elsevier, and Springer). The approach is based on the pre-definition of key papers representing what is called a validation set. The papers in the set were recognized by searching in Google Scholar, a very extensive source of the published papers, by means of general searching terms such as “smart grid authentication”. Naturally general search terms return a huge number of retrieved papers, only a small subset of which (i.e., seven papers in this case) may be related to the selected digital libraries added to the validation set.

Subsequently, the identified key strings are used on the selected digital libraries to observe whether the validation set has been retrieved from the selected digital libraries using the key strings. This process was repeated iteratively until we defined optimised key strings. Additionally, with the objective to further eliminate the selection bias, manual searching was done to recover the primary papers that might have been missing in the formal search. The utility and significance of this approach has been emphasized in [63]. Finally, the references of the primary papers were scanned, but no additional papers were found that met the inclusion and exclusion standards.

5.2. Resolving of review bias

The researchers dynamically discussed and settled on the aims of the review prior to and during the course of the review process. To limit reviewer bias, each paper was reviewed independently by three reviewers while incorporating the inclusion and exclusion criteria, and then another round of verification was applied by the three reviewers, to resolve any conflicting results. The main motive was to make sure that the reviewers had similar interpretations of the inclusion and exclusion criteria, which implies that there was a similar understanding of the inclusion and exclusion criteria. Two main pilots were undertaken prior to applying the criterion on the title and abstract, each with eight papers, and the reviewers convened after each pilot. Immediately after the first pilot the reviewers met to discuss the experience and resolve and issues concerning interpretation of the criteria.

6. Discussion and conclusions

6.1. Importance of SG authentication

SG is prone to security weaknesses, including risk of cyber-attacks, improper or no authentication among the communicating components and entities, exposure of private information, and unauthorised access to resources. Both traditional and SG networks have their own defined requirements. The primary purpose of the SG is to make information available, followed by integrity, confidentiality, and privacy. Authentication of the entities are needed prior to accessing the network and related resources (e.g., a user or a device), with subsequent verification of authorisation for valid permissions. SG faces authentication challenges, such as the link between SG components and communication protocols to other communication networks (e.g., the Internet) increasing security threats and attacks, such as replay, MiTM and impersonation attacks. Additionally, device cryptographic keys could be breached. Thus, it is important to deploy efficient and secure authentication protocols to safeguard the security and privacy of smart gird components.

6.2. Summary and analysis

In this paper a total of 27 primary studies was investigated, and the analysis revealed, that the majority of the studies used the cryptographic approach in order to authenticate the SG components. Cryptographic-based approach relies on known cryptographic techniques, such as symmetric key encryption, hash function, Diffie-Hellman. The data analysis showed that eleven out of the 18 papers showed the use of cryptographic approach while targeting HAN; however, the other five articles gave the central focus to NAN, and the remaining two focused on WAN. The analysis revealed that 55.57%, 14.81%, and 26.62% of the authentication mechanisms focussed on HAN, WAN, and NAN, respectively. The authentication approaches for HAN gained highest attention, due to the overriding importance of customers' personal information. This data is sent to the utility company to help make critical decisions, and any leak in HAN data would be particularly serious.

In SG, the authentication approaches allow integrity, confidentiality, and authenticity to ensure the availability of NAN, HAN, and WAN. These approaches restrict access to unauthorised parties and maintain information flow between utility companies and customers. They also help protect in-house stakeholders against other serious harms, and smart devices from getting corrupted. A trade-off between security robustness and application QoS is involved, particularly in the HAN network.

The analysis shows that the highest mitigated attack in the primary studies was MiTM, with 21.66% of the total identified attacks in the primary studies, followed by impersonation attack (16.66%). In MiTM and impersonation attack, the authentication approaches aim to prevent any malicious smart meter from masquerading as a legitimate smart meter and to avoid any illegal third party from accessing the exchanged data between the SG components, to prevent any damage such as dropping and corrupting the data packet. 18.33% of total attacks mitigated in the primary studies for reply attack, followed by 10.00% for eavesdropping attacks, to prevent fraud of customer identity and data theft of smart meters. Dictionary, brute force, and spoofing attacks accounted for 5.00% each in the primary studies. Finally, attacks like insider, modification, pollution, DoS, data forgery, information leakage, and quantum computer accounted for low percentages, and were classified in the category of other attacks, with a collective percentage of 15.00%.

6.3. Lessons learned for developing smart gird authentication

The challenges and requirements for development of SG authentication can be summarised as follows.

Since SG integrates several subsystems and systems, it is prone to different types of attacks that could harm not only devices themselves and individual consumers, but also communities, industrial networks, and power grids. In SG, communications between entities and components need to be effective, secure, and private, since most functions running over them could be running autonomously. Changes in policies for privacy, efficiency, and security are also possible due to their different characteristics and components.

SG authentication approaches need to consider the limited available resources (i.e., computational capacity and low memory) for smart meters. As a result, for SG communication, the design of authentication approach needs to ensure no unnecessary burden is placed on smart metering resources, which are already constrained. This means that SG communication needs to maintain minimal exchange of messages amongst smart meters in a secured authentication framework. The key issues associated with smart meters include memory constraints, restrictions of sources, and limitations of computational bandwidth.

The authentication system for the SG should ensure protection of components and entities against attacks by adversaries, such as agents of industrial espionage, disgruntled employees, and terrorists. Also, it should safeguard against inadvertent events and unintended compromises of SG data due to equipment failures, user errors, and natural disasters. Timely and dependable access to power system data and real-time use of information are of high importance. Even a slight delay or availability loss in grid systems could degrade the delivery system and undermine the power quality considerably. In the power system, the data is protected via integrity that allows preserving authenticity and nonrepudiation. If loss of integrity and critical data destruction continue, these could result in more security problems in the power management system and erroneous decision making. Confidentiality protects against unauthorised disclosure of sensitive data to the public or attackers attempting to access the system.

Supporting authentications that are repeated numerous times in billions of devices require a fast and lightweight protocol. Mutual authentication amongst different entities of the SG system is provided by an integrated, distributed, lightweight and fast authentication protocol. Maximum use of shared resources with low overhead is possible with an integrated distributed protocol. The SG security protocol should also safeguard against known security attacks.

In SG, instead of being passive players, users can actively play roles to minimise energy consumption by maintaining communication with providers. Many machines, such as smart meters, sensing devices, and control systems may be present between the provider and end-users for two-way communication. Multiple techniques and mechanisms can be required in the practical deployment of SG authentication. For instance, there may be a need for just symmetric cipher-based or public key-based systems, or both. Moreover, there may be a need for the components and entities to store some validation data regarding each user and server, or the server may not store the credentials for validation (considered as identity-based systems). Also, there could be other requirements, like user password changes and expiration.

6.4. Direction for future studies

Despite accomplishing the objective of this research, the researcher has still been bound by some limitations that can be addressed in future studies. In particular, the literature search only yielded a limited number of past papers (i.e., the primary studies), and we suggest a more extensive research based on new research questions to focus on the security and privacy attributes of SG system, to obtain a detailed observation of the current status of SG security.

References

1. Reka, S. S., T. Dragicevic. Future Effectual Role of Energy Delivery: A Comprehensive Review of Internet of Things and Smart Grid. – Renewable and Sustainable Energy Reviews, Vol. **91**, 2018, pp. 90-108.
2. Yang, Q. 13 – Internet of Things Application in Smart Grid: A Brief Overview of Challenges, Opportunities, and Future Trends. – In: Smart Power Distribution Systems. Q. Yang, T. Yang, and W. Li, Eds. Academic Press, 2019, pp. 267-283.
3. Qasaimeh, M., R. S. Al-Qassas, S. Tedmori. Software Randomness Analysis and Evaluation of Lightweight Ciphers: The Prospective for IoT Security. – Multimedia Tools and Applications, Vol. **77**, 2018, pp. 18415-18449.
4. Tsiatsis, V., S. Karnouskos, J. Höller, D. Boyle, C. Mulligan. Chapter 12 – Smart Grid. – In: Internet of Things. Second Edition. V. Tsiatsis, S. Karnouskos, J. Höller, D. Boyle, and C. Mulligan, Eds. Academic Press, 2019, pp. 257-268.
5. Min-Xiang, H. H., C. He, R. Li, L. Zeng. Comprehensive Performance Evaluation Strategy for Communication Networks Selection in Smart Grid. – Cybernetics and Information Technologies, Vol. **16**, 2016, pp. .
6. EIA, Annual Energy Outlook 2017, 2018.
7. Faheem, M., S. B. H. Shah, R. A. Butt, B. Raza, M. Anwar, M. W. Ashraf, et al. Smart Grid Communication and Information Technologies in the Perspective of Industry 4.0: Opportunities and Challenges. – Computer Science Review, Vol. **30**, 2018, pp. 1-30.

8. Demir, K., H. Ismail, T. Vateva-Gurova, N. Suri. Securing the Cloud-Assisted Smart Grid. – International Journal of Critical Infrastructure Protection, Vol. **23**, 2018, pp. 100-111.
9. Atanasov, I., E. Pencheva. Reducing Energy Consumption by Using Smart Metering Intelligent Systems. – Cybernetics and Information Technologies, Vol. **16**, 2016, pp. 113-124.
10. Kuzlu, M., M. Pipattanasomporn, S. Rahman. Communication Network Requirements for Major Smart Grid Applications in HAN, NAN and WAN. – Computer Networks, Vol. **67**, 2014, pp. 74-88.
11. Bayindir, R., I. Colak, G. Fulli, K. Demirtas. Smart Grid Technologies and Applications. – Renewable and Sustainable Energy Reviews, Vol. **66**, 2016, pp. 499-516.
12. Nge, C. L., I. U. Ranaweera, O.-M. Midtgård, L. Norum. A Real-Time Energy Management System for Smart Grid Integrated Photovoltaic Generation with Battery Storage. – Renewable Energy, Vol. **130**, 2019, pp. 774-785.
13. Desai, S., R. Alhadad, N. Chilamkurti, A. Mahmood. A Survey of Privacy Preserving Schemes in IoE Enabled Smart Grid Advanced Metering Infrastructure. – Cluster Computing, 2018.
14. Kim, J., L. Tong. Against Data Attacks on Smart Grid Operations: Attack Mechanisms and Security Measures. – In: Cyber Physical Systems Approach to Smart Electric Power Grid. S. K. Khaitan, J. D. McCalley, and C. C. Liu, Eds. Berlin, Heidelberg, Springer, 2015, pp. 359-383.
15. Lei, H., B. Chen, K. L. Butler-Purry, C. Singh. Security and Reliability Perspectives in Cyber-Physical Smart Grids. – In: Proc. of IEEE Innovative Smart Grid Technologies – Asia (ISGT'18 Asia), 2018, pp. 42-47.
16. Ayday, E., S. Rajagopal. Secure Device Authentication Mechanisms for the Smart Grid-Enabled Home Area Networks. 2013.
17. Limbasiya, T., A. Arya. Attacks on Authentication and Authorization Models in Smart Grid. – In: Smart Micro-Grid Systems Security and Privacy, A. V. D. M. Kayem, S. D. Wolthusen, and C. Meinel, Eds. Cham, Springer International Publishing, 2018, pp. 53-70.
18. Qasaimeh, M., R. Turab, R. S. Al-Qassas. Authentication Techniques in Smart Grids: A Systematic Review. – TELKOMNIKA (Telecommunication, Computing, Electronics and Control), Vol. **17**, 2019.
19. Wang, F., Z. Lei, X. Yin, Z. Li, Z. Cao, Y. Wang. Information Security in the Smart Grid: Survey and Challenges. Singapore, 2018, pp. 55-66.
20. Gupta, B. B., T. Akhtar. A Survey on Smart Power Grid: Frameworks, Tools, Security Issues, and Solutions. – Annals of Telecommunications, Vol. **72**, 2017, pp. 517-549.
21. Munn, Z., M. D. J. Peters, C. Stern, C. Tufanaru, A. McArthur, E. Aromataris. Systematic Review or Scoping Review? Guidance for Authors when Choosing Between a Systematic or Scoping Review Approach. – BMC Medical Research Methodology, Vol. **18**, 2018, p. 143.
22. Kitchenham, B., L. Madeyski, D. Budgen, J. Keung, P. Brereton, S. Charters, et al. Robust Statistical Methods for Empirical Software Engineering. – Empirical Software Engineering, Vol. **22**, 2017, pp. 579-630.
23. Sharma, M., A. Agarwal. Survey on Authentication and Encryption Techniquesfor Smart Grid Communication. – In: Proc. of 7th India International Conference on Power Electronics (IICPE'16), 2016, pp. 1-5.
24. Farouk, A., A. A. Abdelhafez, M. M. Fouad. Authentication Mechanisms in Grid Computing Environment: Comparative Study. – In: Proc. of International Conference on Engineering and Technology (ICET'12), 2012, pp. 1-6.
25. Ji, C., J. Kim, J. Lee, M. Hong. Review of One-Time Signatures for Multicast Authentication in Smart Grid. – In: Proc. of 12th International Conference & Expo on Emerging Technologies for a Smarter World (CEWIT'15), 2015, pp. 1-4.
26. Kumar, A., A. Agarwal. Research Issues Related to Cryptography Algorithms and Key Generation for Smart Grid: A Survey. – In: Proc. of 7th India International Conference on Power Electronics (IICPE'16), 2016, pp. 1-5.
27. Leander, G., C. Paar, A. Poschmann, K. Schramm. New Lightweight DES Variants. Berlin, Heidelberg, Springer, 2007.

28. Kitchenham, B. A. Systematic Review in Software Engineering: Where We Are and Where We Should Be Going. – In: Proc. of 2nd International Workshop on Evidential Assessment of Software Technologies, Lund, Sweden, 2012.
29. Tsaur, W., C. Wu. A Secure Smart-Card-Based Password Authenticated Key Agreement Scheme in Multi-Server Environments. – In: Proc. of IEEE Second International Conference on Social Computing, 2010, pp. 999-1003.
30. Warnier, M., S. Dulman, Y. Koç, E. Pauwels. Distributed Monitoring for the Prevention of Cascading Failures in Operational Power Grids. – International Journal of Critical Infrastructure Protection, Vol. **17**, 2017, pp. 15-27.
31. Sharma, G., S. Kalra. A Secure Remote User Authentication Scheme for Smart Cities e-Governance Applications. – Journal of Reliable Intelligent Environments, Vol. **3**, 2017, pp. 177-188.
32. Chang, S., T. William, W. Wu, B. Cheng, H. Chen, P. Hsu. Design of an Authentication and Key Management System for a Smart Meter Gateway in AMI. – In: Proc. of IEEE 6th Global Conference on Consumer Electronics (GCCE'17), 2017, pp. 1-2.
33. Cho, S., H. Li, B. J. Choi. PALDA: Efficient Privacy-Preserving Authentication for Lossless Data Aggregation in Smart Grids. – In: Proc. of IEEE International Conference on Smart Grid Communications (SmartGridComm), 2014, pp. 914-919.
34. Qinghai, G. Biometric Authentication in Smart Grid. – In: Proc. of International Energy and Sustainability Conference (IESC'12), 2012, pp. 1-5.
35. Fangming, Z., Y. Hanatani, Y. Komano, B. Smyth, S. Ito, T. Kambayashi. Secure Authenticated Key Exchange with Revocation for Smart Grid. – In: Proc. of IEEE PES Innovative Smart Grid Technologies (ISGT'12), 2012, pp. 1-8.
36. Tavasoli, M., S. Alishahi, M. Zabihi, H. Khorashadizadeh, A. H. Mohajerzadeh. An Efficient NSKDP Authentication Method to Secure Smart Grid. – In: Proc. of IEEE International Conference on Smart Energy Grid Engineering (SEGE'17), 2017, pp. 276-280.
37. Tabassum, R., K. Nahrstedt, E. Rogers, K. Lui. SCAPACH: Scalable Password-Changing Protocol for Smart Grid Device Authentication. – In: Proc. of 22nd International Conference on Computer Communication and Networks (ICCCN'13), 2013, pp. 1-5.
38. Doh, I., J. Lim, K. Chae. Secure Authentication for Structured Smart Grid System. – In: Proc. of 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 2015, pp. 200-204.
39. Ayday, E., S. Rajagopal. Secure, Intuitive and Low-Cost Device Authentication for Smart Grid Networks. – In: Proc. of IEEE Consumer Communications and Networking Conference (CCNC'11), 2011, pp. 1161-1165.
40. Cairns, K., C. Hauser, T. Gamage. Flexible Data Authentication Evaluated for the Smart Grid. – In: Proc. of IEEE International Conference on Smart Grid Communications (SmartGridComm), 2013, pp. 492-497.
41. Choi, J., I. Shin, J. Seo, C. Lee. An Efficient Message Authentication for Non-Repudiation of the Smart Metering Service. – In: Proc. of First ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering, 2011, pp. 331-333.
42. Fouda, M. M., Z. M. Fadlullah, N. Kato, R. Lu, X. S. Shen. A Lightweight Message Authentication Scheme for Smart Grid Communications. – IEEE Transactions on Smart Grid, Vol. **2**, 2011, pp. 675-685.
43. Lee, Y., E. Kim, Y. Kim, H. Jeon, M. Jung. A Study on Secure Chip for Message Authentication between a Smart Meter and Home Appliances in Smart Grid. – In: Proc. of International Conference on IT Convergence and Security (ICITCS'13), 2013, pp. 1-3.
44. Muñoz, M. C., M. Moh, T. Moh. Improving Smart Grid Authentication Using Merkle Trees. – In: Proc. of 20th IEEE International Conference on Parallel and Distributed Systems (ICPADS'14), 2014, pp. 793-798.
45. Nath, A. P. D., F. Amsaad, M. Choudhury, M. Niamat. Hardware-Based Novel Authentication Scheme for Advanced Metering Infrastructure. – In: Proc. of IEEE National Aerospace and Electronics Conference (NAECON) and Ohio Innovation Summit (OIS'16), 2016, pp. 364-371.

46. Nicanfar, H., V. C. M. Leung. Smart Grid Multilayer Consensus Password-Authenticated Key Exchange Protocol. – In: Proc. of IEEE International Conference on Communications (ICC'12), 2012, pp. 6716-6720.
47. Saxena, N., B. J. Choi. Integrated Distributed Authentication Protocol for Smart Grid Communications. – IEEE Systems Journal, Vol. **12**, 2018, pp. 2545-2556.
48. Li, W., R. Li, K. Wu, R. Cheng, L. Su, W. Cui. Design and Implementation of an SM2-Based Security Authentication Scheme with the Key Agreement for Smart Grid Communications. – IEEE Access, 2018, pp. 15-22.
49. Li, X., F. Wu, S. Kumari, L. Xu, A. K. Sangaiah, K.-K. R. Choo. A Provably Secure and Anonymous Message Authentication Scheme for Smart Grids. – Journal of Parallel and Distributed Computing, 2017.
50. Mahmood, K., S. Ashraf Chaudhry, H. Naqvi, T. Shon, H. Farooq Ahmad. A Lightweight Message Authentication Scheme for Smart Grid Communications in Power Sector. – Computers & Electrical Engineering, Vol. **52**, 2016, pp. 114-124.
51. Abbasinezhad-Mood, D., M. Nikooghadam. Design and Hardware Implementation of a Security-Enhanced Elliptic Curve Cryptography Based Lightweight Authentication Scheme for Smart Grid Communications. – Future Generation Computer Systems, Vol. **84**, 2018, pp. 47-57.
52. Nabeel, M., X. Ding, S.-H. Seo, E. Bertino. Scalable End-to-End Security for Advanced Metering Infrastructures. – Information Systems, Vol. **53**, 2015, pp. 213-223.
53. Abbasinezhad-Mood, D., M. Nikooghadam. Design of an Enhanced Message Authentication Scheme for Smart Grid and Its Performance Analysis on an ARM Cortex-M3 Microcontroller. – Journal of Information Security and Applications, Vol. **40**, 2018, pp. 9-19.
54. Mahmood, K., S. A. Chaudhry, H. Naqvi, S. Kumari, X. Li, A. K. Sangaiah. An Elliptic Curve Cryptography Based Lightweight Authentication Scheme for Smart Grid Communication. – Future Generation Computer Systems, Vol. **81**, 2018, pp. 557-565.
55. Wang, Y. Secure Communication and Authentication Against Off-line Dictionary Attacks in Smart Grid Systems. – In: Security of Industrial Control Systems and Cyber-Physical Systems, Cham, 2017, pp. 103-120.
56. Câmara, S., D. Anand, V. Pillitteri, L. Carmo. Multicast Delayed Authentication for Streaming Synchrophasor Data in the Smart Grid. – IFIP Advances in Information and Communication Technology, Vol. **471**, 2016, pp. 32-46.
57. Al Hamadi, H. M. N., C. Y. Yeun, M. J. Zemerly. A Novel Security Scheme for the Smart Grid and SCADA Networks. – Wireless Personal Communications, Vol. **73**, 2013, pp. 1547-1559.
58. Bayat, M., M. B. Atashgah, M. R. Aref. A Secure and Efficient Chaotic Maps Based Authenticated Key-Exchange Protocol for Smart Grid. – Wireless Personal Communications, Vol. **97**, 2017, pp. 2551-2579.
59. Wen, M., J. Lei, Z. Bi, J. Li. EAPA: An Efficient Authentication Protocol against Pollution Attack for Smart Grid. – Peer-to-Peer Networking and Applications, Vol. **8**, 2015, pp. 1082-1089.
60. Li, H., R. Lu, L. Zhou, B. Yang, X. Shen. An Efficient Merkle-Tree-Based Authentication Scheme for Smart Grid. – IEEE Systems Journal, Vol. **8**, 2014, pp. 655-663.
61. Abdullah, M. D. H., Z. M. Hanapi, Z. A. Zukarnain, M. A. Mohamed. Attacks, Vulnerabilities and Security Requirements in Smart Metering Networks. – KSII Transactions on Internet & Information Systems, Vol. **9**, 2015.
62. Jabangwe, R., J. Börstler, D. Šmite, C. Wohlin. Empirical Evidence on the Link between Object-Oriented Measures and External Quality Attributes: A Systematic Literature Review. – Empirical Software Engineering, Vol. **20**, 2015, pp. 640-693.
63. Garousi, V., M. Felderer, M. V. Mäntylä. Guidelines for Including Grey Literature and Conducting Multivocal Literature Reviews in Software Engineering. – Information and Software Technology, Vol. **106**, 2019, pp. 101-121.

Received: 06.01.2019; Second Version: 12.02.2019; Accepted: 19.02.2019 (*fast track*)