A REVIEW OF CRYPTOGRAPHIC IMPACT IN CYBER-SECURITY ON SMART GRID: THREAT, CHALLENGES AND COUNTERMEASURES

[1]MD MEHEDI HASAN, [2] NOOR AFIZA MOHD ARIFFIN, [3] NOR FAZLIDA MOHD SANI
[1]Department of Computer Science and Information Technology, University Putra Malaysia, Serdang, 43400 Seri Kembangan, Malaysia
[2] Department of Computer Science and Information Technology, University Putra Malaysia, Serdang, 43400 Seri Kembangan, Malaysia
[3] Department of Computer Science and Information Technology, University Putra Malaysia, Serdang, 43400 Seri Kembangan, Malaysia
E-mail: [1]mehedi.upm@gmail.com, [2] noorafiza@upm.edu.my, [3] fazlida@upm.edu.my

ABSTRACT

The continuous development of information communication technology assists the traditional electricity grid to become a modern integrated platform. As Internet-of-Thing's technologies involve in smart grid features together with delivery emerging services utility side to end user via unreliable channel. Due to high dependency of communication system lead catastrophic security vulnerabilities. In addition, loss data security or privacy along hampered core security objectives confidentiality, integrity, availability and broken connection between them. Therefore, significant number of researches worked mitigates those types of threads by the use of cryptographic aspect. It is fascinated to kept data secure and ensures the privacy between two parties during transmission or any kind of data share in distribute manner. In this paper, we present comprehensive survey on cryptographic impact in smart grid for security objectives, requirement, and challenges. Particularly, produces security threats, examined current research work countermeasure technique. We aim to supply deeper understanding about role of cryptographic aspect in smart grid to shed light and guide future research direction for cyber-security protection against from malicious attacker in smart grid application.

Keywords: *Smart Grid, IoT, Cyber-Security, Threats, Authentication, Cryptography*

1. INTRODUCTION

In recent achievement integration based on machine to machine (M2M) communication alongside innovative application of information communication technology significant role play in smart gird. With the implementation of Internet technology in a smart grid allows seamless interactions between all energy systems, device, sensor and networks to improve energy within the gird [1]. The functionality of a conventional grid is a mechanization one-way communication process and infrastructure is relational with less fact plus less sensors while the functionality of a smart grid is digitized two-way service, contact, and communication. The smart grid platform has a greater number of sensors available.

While adopt a future power system that also incorporates advanced sensing, provides effective billing (Real time: 15-20 minute interval) [2],It is a platform providing two-way communications between customers and service provider in which computation and communication between the consumer and the energy supplier on a time to time basis.
Advanced metering infrastructure is an application of in smart grid technology kind of intelligent technology to ensure the correlation between the services providers and users of facilities.[3] Despite numerous advantages with AMI has need to faster, low power, less processing time. Architecture of AMI It comprises four main parts likewise service provider, customer premises, intelligent device, server and smart meter, communication channel. According to The National Institute of Standard and Technology there are six major component exits in the smart grid that are likely bulk generation, distribution, transmission, market, operation, service provider, service provider,

customer [4] Combined through Internet networking technologies such as the IP technology which are adopt variant smart grid components with advanced metering element. In addition, smart grids perform efficiently transmitting, distributing, and communicating with all the component of smart grid. Customer and service provider interact among help of smart meter, sensor, advanced metering infrastructure, meter data management system, and utility server by using communication channel connected between them. So for information protection need to authenticate between each entity as well identification and encryption for secure data transmission [5] [6].

The IoT enables a smarter closer network across the grid infrastructure by allowing two-way communication information transfer or communication between components of smart grid. IoT provides customers, retailers and suppliers along reduce human activity in the management of smart meters, home gateway, intelligent sensors and other connected devices, thereby guaranteeing an optimal atmosphere response for the smart grid. Benefit of IoT applications provide smart grid systems very easy interaction. As Internet-based communications and general public solutions control and monitoring is carried out on smart grid, but might high dependency lead to catastrophe due to some vulnerabilites. However for the attackers could be highly desirable infrastructure [7]. For instance, an intruder can attack the electronic components by decrease the balance between generation and demand in real time due to the falsification of the data generated by the devices [8]. That could be the big focus for cyber terrorism due to the obvious sensitive existence of the smart grid [9]. Thus, it is vital to look more closely at components of the smart grid system and recognize former weaknesses and all potential cyber security threats.
Since smart grid have large amount of component, device and sensor interaction in communication secure/unsecure channel wherein transmission data kept private in between two parties [9]. Beside understand the real identity between two parties during any kind of request and response. So authentication and encryption is most importance for the security perspective in smart grid context [6]. In the last few years demonstrate used to fill security holes by using cryptographic aspect known as authentication [2] for identify to parties communication and encryption mechanism proposed for securely data transfer between them by used of key agreements techniques that have been used in smart meter to the district network along utility server[10],[7]. All smart grid critical infrastructures need to be designed to ensure mitigating cyber threats, which means preserving the core cyber security standards, namely confidentiality, integrity and availability in smart grid infrastructure [5],[11].

Therefore, this study provides the analysis of the current situation and possible cryptographic aspect research guidance on how smart grid security requirement are satisfied with the achievement of security objectives. In the meantime, investigate which way influences security criteria to ensure data security and privacy and mitigates well-known cyber. So first, the study indicates smart grid features, security principle, together with the smart grid core security principles and objectives mainly confidentiality integrity and availability. After that reveal the security requirement meets the objectives and challenges of the smart grid. Furthermore, categorized the CIA triads-based attack is carried out. Moreover, illustrated previous mechanism technique to satisfy the security objectives that are more relevant basis on cryptographic aspect alongside, appeared smart grid security requirements consider to adopt the cryptographic aspect to deal preserve the security and privacy from malicious attacker during data transmission. Finally, cryptographic aspect significance impact has been obtained to protect security and privacy against cyber threats. In the same way countermeasures technique demonstrate advantage and disadvantage with flow potential future research directions in smart grid.

The reminder of this paper is organized as follows in Section 2, we presented discussion about smart grid functionality and features. In section 3, we describing the cyber security objectives and requirements along challenges in smart grid. In section 4, we categorize CIA triad based cyber attack illustrate. In section 5, we demonstrate and review current worked basis on cryptographic aspect and counter measures techniques in smart grid. Finally, we discuss and conclude in section 6 and 7 respectively.

2. FEATURES OF SMART GRID

There are a lot of features and incentives in the smart grid. This is an interactive machine with people. In addition, it offers multiple ways to create an emerging intelligent platform these are point out below.

2.1 Smart meter

The smart meter is an electronic device that is capable of any overall consumption of electrical devices containing assorted electricity, voltage level, current and power factor. The smart meter is a two-way communication medially the user side and the service side [12]. On the other hand, smart meter enables real-time data collection from the electrical device to 15 minutes of scheduling [13].Within smart meter have microcontroller unit , voltage or current sensors with real and reactive energy measurement, communication protocols, and most of them are equipped with liquid crystal display interface that helps customers not just to know their tariffs and consumption habits, but rather to deliver power quality to the service provider.

2.2 Advanced metering infrastructure (AMI)

An advanced metering infrastructure two-way method of communicate for collecting and measuring energy for billing and statistical purposes on consumptions, Advanced metering infrastructure is advancements invasion activities in near-real-time basis operation [14]. AMI are responsible for processing, analyzing, preserving and supplying metering information collected for billing, failure management, and demand management through smart meter to service company servers. Prices for real-time supply offer useful hints to help both consumers and manufacturers monitor and manage their supplies of energy needs, respectively.

2.3 Demand Response (DR)

One of the key services in smart gird that is full phases of use cloud computing and IoT based application is demand response is a method where the customer requests energy at a certain time where the billing of usage is centered on the peak/off-peak load [15] Demand response aims to encourage end-users to change their energy consumption patterns. Such functionality exists in demand response namely time-based rates such as time-of-use scheduling, critical peak incentives, real-time selling, variable peak pricing and peak traffic pricing, a direct load management program as well as an interactive demand response program are provided in demand response systems run by some electrical system planners and administrators to manage supply and demand.

2.4 Supervisory Control and Data Acquisition (SCADA)

With the service of SCADA responsible on large number such sensors, actuators and smart meters the entire power grid system is tracked. It will provide report information to the utility regularly on demand or in response to certain activities, while still listening to utility demands due to their two-way communication capability with end user side [15].It offers concurrent control, monitoring of the electricity distribution network. It is commonly used in big-scale settings and can also help maintain energy supply reliability and decreases the network's maintenance and operating costs. SCADA-related subsystems are the distribution management function and the energy management functions.

2.5 IoT-based grid technology

Enhanced version of conventional power grid integrated lines with IoT technology based smart grid. One of the most competent concepts is the IoT, which plays a significant role within smart grid [7]. The bi-directional gird framework adopts IoT-based applications. Both IP-based system device operation and require the support of an internet connection, makes the system stable and scalable anywhere as well as remote access anytime. Each gateway can authenticate each other in an encoded data form during the data transmission [10].

3. SECURITY PRINCIPLE OF SMART GRID

The smart grid infrastructure must serve all of the systems adopt with generation, distribution, maintenance, transmission of electricity processes that are carried out. To guarantee that these all transactions communicate appropriately and key goals of preserve security bi-directional connectivity can be accomplished [9]. Smart grids are made up of several devices connected uses by communication channel with each other.

There are main two types of methods that are transmitted between these devices.

Private Data: It relates to data relating to privacy, for example user information, consumer data, reporting data seizing such data by attackers is typically a breach of privacy policy.

Operational Data: It contains command instructions for operational data requires a high security standard to protect intelligent grid systems from potential attacks[16]. Operational information shows the existing loads of transformers, tap-changers, capacitors, defect locations, relay status, present voltage values in real time, circuit interrupting status, etc. The collection by attackers of such data can cause damage to the whole machine process.

3.1 Security objectives

The NIST has identified three principles to preserve and protect the security especially confidentiality, integrity and availability of information in the smart grid [17]. Cyber-security priorities of the smart grid must take care to protect information with the CIA triad. These primary safety principles must certainly be fulfilled in smart grid systems.

3.1.1 Confidentiality

Confidentiality seems to be the defense of data against unauthorized users or disclosure. Thus, only authorized users may have access to the data, and unauthorized users cannot have access to the data. An existing smart grid network can communicate through an unsecured and protected channel based on two-way real-time communication. Smart grid programs provide many sensitive data, e.g. power analysis, billing information, private consumer information etc. confidentiality involves information privacy and it is among the most important concerns for consumer data keep and safe. [18].

3.1.2 Integrity

The data should never be manipulated with by anybody anywhere in the system during transmission. Therefore, the data should not be altered in an unrecognized manner. Integrity is characterized as the protection against unauthorized duplication and destruction of data. Thus, integrity of data needs to be controlled in the smart grid and presented guarantee the reliability of the data/information.

3.1.3 Availability

The smart grid energy platform is supposed to be activated all the time. And it is necessary to ensure that timely and efficient access is made to the information management system. In the smart grid confirm that the information is available. In the mean time authorized parties must be made accessible data when needed without a security compromise. In fact, the security of the information system against corrupt, blocked, delayed sensitive information closely observation must be available. [19]. Availability usually requires avoiding DDoS attacks whenever due to failure make leads to blackouts.

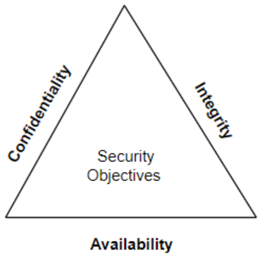

Figure 1: Security Objectives of smart grid

3.2 Security requirement

The objective of cyber protection for the smart grid would be employ the confidentiality, integrity and availability support information settle security policy along provide a robust supply of electricity [18]. Therefore, the development of objectives and requirement should be ensured legally to acquire by comprehensive cyber security goal. According to report of NIST [4],[20],[21] recommends additional basic smart grid protection requirements, including physical grid security.

3.2.1 Authentication

Authentication with identification is the key to verifying the identity of a user or device to protect the smart grid system from unauthorized access. It helps you to check if an object's identity is correct or not. Objects can include users, intelligent devices or network-connected components. Human and machine authentication has been great importance in smart grid. failure of authentication may occurs vulnerability as an attacker access to private information or illegal smart grid-based equipment [16].Authentication including encryption are obligatory safety processes to protect the privacy and integrity of information in the smart grid system [7].

3.2.2 Authorization

Authorization also known as access control offers do not give access without permission to the system. Authorization is used for differentiate to identify legitimate and unlawful parties based on authentication for other requirements for cyber-security. Authorization result may harmful for system toward security problems if breached [22]. In addition, access controls in the smart grid are used to ensure that services are only available to the properly identified parties.

3.2.3 Accountability

Accountability means making sure the system's controllability and every activity undertaken by any individual, device, or even any governmental agency is recorded such that no person could even ignore his/her identified actions. It allows false parties to be recognized by proof-able evidence [17]. The monthly customer energy costs demand response signal, valuable grid information etc. might be an illustration of an accountability issue. However, meter data is no longer visible when smart meter during under a cyber attack along attacker can data modified. So, consider this accountability must exist in a smart grid system.

3.2.4 Dependability

Dependability seems to be the ability of a system to accomplish its needs in a timely and accurate manner by prohibiting common and severe internal defects. Dependability implies service delivery in the event of internal defects. The fundamental attributes ensure of truthfulness are availability, reliability, maintenance, and safety. Dependability confirms according to measure reduction of fault tolerance, fault forecasting, fault error, fault detection, fault removal, modifiability.

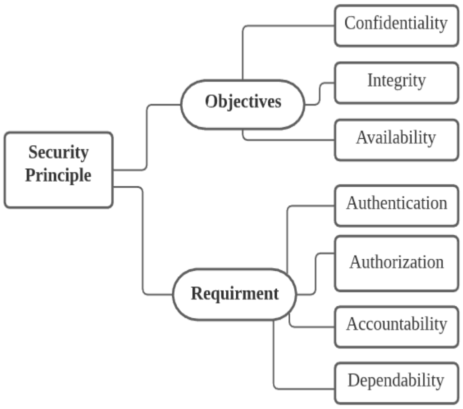

Figure 2: Security Principle of smart grid

3.3 Security Challenges

The smart grid is vulnerable to several problems and risks. Various cyber security challenges are reached due to the lacking of identification and inefficient cryptographic premises [23],[10] In this section discuss accordingly.

3.3.1 Communication

In the smart grid, the network architecture is sophisticated as it integrates a significant number of interoperating devices, sensor gateway, server, monitoring tools that is utmost important data privacy kept while know each other during service delivery. Despite the design of a decentralized smart grid setting the systems need a high degree of security between attacks and security flaws [16]. Attacks may lead to serious harm, blackouts and loss of performance. This is because the system is controlled by attackers [24].

3.3.2 Trustworthy

Due to high accessibility of the power systems that informed the design decisions, customer service is no longer considered trustworthy. Many customers are not abiding by the laws and agreements, for example may deliberately harm the smart meter to serve the duplication report produce.

3.3.3 Consumer Privacy

Ensuring the privacy of customers is an essential feature in smart grid scheme during service transmission information must be well secured and preserved [25]. Smart grid is a very sensitive infrastructure since there are different components used by unsecured channel between the data transmission. Preserving the privacy of the user information must be protected during the information transmission to big challenges prevent unauthorized access. As a daily smart meter transfers data in routine time intervals to the power service provider server these data cover sensitive customer information that would be secured from unauthorized parties.

4. CYBER-THREATS OF SMART GRID

The key fields of smart grid generation, transmission, delivery and consumption must be efficiently and securely met in all domains. In such way that one known component which is the revolutionary technology known as the advanced metering infrastructure is a kind of middleware between the consumer and the service provider [2]. These characteristics accommodate the neighborhood network along the wide area network to the service provider system through the known home area network [19]. Due to the inconsistent technologies used many unknown nodes belong to the network, which is very challenging identify source to the destination through the encrypted data exchange between them. Beside high dependency on communication create scope for malicious intruder to interfere grid system during the transmission. According to above issues raised several security vulnerabilites. In this section we discuss well known security breaches based on the device attack, data attack, privacy attack, network attack in smart grid infrastructure.

Device attack: The goal of device attack is exploiting and controls the device It is also the initial stage of a sophisticated attack.

Data attack: The data attack attempts to unlawfully insert, modify or delete data or monitor commands in the traffic of the communication network in order to deceive the smart grid to make bad decisions/actions.

Network attack: It seeks to use or overwhelm the communication and computing resources of a smart grid and also to result in pause or loss of communication.

Privacy attack: It aims in the analysis of electricity consumption data, to learn/infer private information from users

Table 1: CIA triad-based attack

Security Goal	Attack Types	References
Confidentiality	Eavesdropping, MITM, Traffic Analysis, Replay, Password Pilfering, Masquerading, Sniffing, Data Injection, Forward Secrecy, Impersonates.	[2],[7],[9],[26],[27] [28],[29]
Integrity	Data Tempering, Massage Injection, Data Modification, Wormhole, Spoofing, Phishing, Man-In-The-Middle, Time Synchronization, Insider attack and Anonymity.	[5],[7],[9], [15], [17], [30]
Availability	Jamming attack, Distributed denial of service attack, Low-rate Dos attack, Spoofing Attack, Masquerading, and MITM.	[5],[9],[15],[17],[19] ,[31]

Security precautions are typically divided into three categories in smart grid: network security, cryptography for data privacy and security, and device safety [17],[32]. In next section 5 demonstrate briefly cryptography how does effective impact on smart grid in term of cyber security consideration.

5. CRYPTOGRAPHIC ASPECT AND COUNTERMEASURES

Mention above CIA triad based cyber attack harmful for smart grid component together with customer and service provider. The cyber security solution should protect all parts of a smart grid infrastructure. According to discuss section 3 cyber security objectives required by following security requirement have to be consider [24]. Cryptography aspect provides three major operations develop encryption for data integrity, Confidentiality and authentication for identification along key agreement for getting efficient results [23]

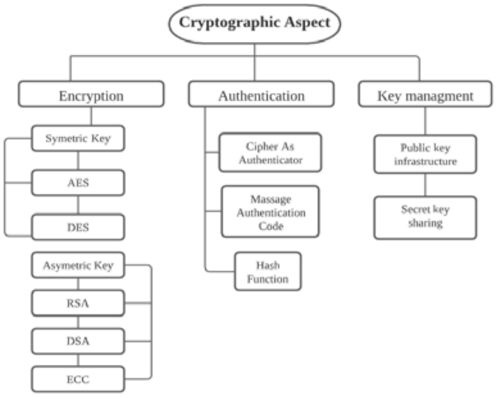

Figure 3: Cryptographic Aspect in Smart Grid

Indeed, if all the cyber security goals to be accomplished in the smart grid would be achieved. Granting the cryptographic aspect plays a major role in providing cyber security requirements to full fill the smart grid cyber security objectives. To ensure the efficiency of cryptographic aspect operation deal with identities, data security is managed by a key agreement for a large number of smart grid components. Combination full pledge of the cryptographic aspect followed by handle the security requirements at which goals are suitable for adjustment of the smart grid features.

5.1 Cryptographic Study

There are several methods have been used to adequately execute cyber security objectives as long as cyber security guidelines are maintained prevent by all over the attack. But in this case cryptography efficient for data security and privacy [11] So, this paper focuses on the cryptographic effective on reserve data security and privacy including cyber threat prevention in the smart grid infrastructure [17],[32]. This section shows some recent proposed solution based on the cryptographic parameter used, i.e., the encryption intent of data protection, authentication for validation of identity between different smart grid components, while the key agreement used for configuration key generation along distribution. Since we know, cryptography guarantees the protection and privacy of private data including operational data.

Table 1: Cryptographic aspect-based research work

Schemes	Research Goal	Compromise Cryptographic Parameter	Compromise Security Objectives	Description: Pros (+) and Cons (-)
[33]	The goal of this study integrates demand response with advanced metering system.	× Encryption √ Authentication × Key management	× Confidentiality × Integrity √ Availability	+Reduced computation cost -Limited capable for authentication only AMI authenticate
[34]	Propose stable cloud approach and for deployment of secure data management for big data frameworks.	√ Encryption √ Authentication × Key management	√ Confidentiality √ Integrity × Availability	+Achieved Identity between two components -Increase communication cost -Used extra hardware device for key management
[35]	Propose authentication and key agreement protocol for mitigation known attack	× Encryption √ Authentication × Key management	√ Confidentiality √ Integrity × Availability	+Achieved smart meter privacy and security -Extra system for authentication so increases
[31]	Propose integration of home area network device to cloud of thing application for monitoring	× Encryption × Authentication √ Key management	× Confidentiality √ Integrity × Availability	+Introduce home area network to CoT established interaction +Vulnerable for MITM and Replay attack
[36]	Propose mechanism for established mutual authentication in home are network to near BAN-GW	√ Encryption √ Authentication × Key management	√ Confidentiality √ Integrity × Availability	+Rate of communication power avoid system goal +Does not provide session key security
[37]	Propose hardware based key management with authentication to deliver efficient smart meter process	√ Encryption √ Authentication √ Key Agreement	√ Confidentiality √ Integrity × Availability	+Provide secret key security +protest identity based known authentication attack -Does not actually got AMI authentication
[38]	This Author goal enhancing the security of massage integrity and data privacy along data keeps availability.	√ Encryption √ Authentication × Key management	√ Confidentiality √ Integrity √ Availability	+Proposed worked mitigate kind of CIA triad attack +Got reliable connection results among smart meter to server -Computation time increase
[39]	Propose this worked suggest the authentication and verification system to minimize Internal and outsider attack	× Encryption √ Authentication × Key management	√ Confidentiality √ Integrity √ Availability	+Reduced computation and communication in overheads +Mitigated several cyber attacks -Does not efficient for perfect forward secrecy.
[40]	The proposed study authentication-based scheme	√ Encryption √ Authentication	√ Confidentiality √ Integrity	+This scheme got better results than RSA approach

	for safe data transmission between smart meter to utility server	√ Key Agreement	√ Availability	+Achieved authentication between smart meter and utility provider -Increase time for verification of session key
[41]	The proposed Similarly for reducing computation and communication overheads based on identify problem delay of sensitive data transmission customer between power sector	√ Encryption √ Authentication × Key Agreement	√ Confidentiality √ Integrity × Availability	+This scheme reached mutual authentication and massage integrity +Minimize cyber attack -use RSA operation made increase key size
[42]	Propose offer effective, comprehensive authentication and key management arrangements.	× Encryption √ Authentication √ Key Agreement	× Confidentiality √ Integrity √ Availability	+prevents the opponent from increasing the attack +This leads to low overhead communications -Increased computation time -High latency of operation communication
[43]	The paper protection and privacy issues are the key subject of the smart gird.	√ Encryption √ Authentication √ Key Agreement	√ Confidentiality √ Integrity × Availability	+Reduced computation and communication cost +mitigation various threat -vulnerable for Dos attack
[44]	The propose mechanism ensure reliable operation in smart grid used identity-based cryptosystem	× Encryption √ Authentication √ Key Agreement	√ Confidentiality √ Integrity × Availability	+Efficient for forward, backward security -Vulnerable for collusion attack
[45]	Propose technique intend to identity-based approach take system ensure data security home area network among neighborhood network.	√ Encryption √ Authentication √ Key Agreement	√ Confidentiality × Integrity √ Availability	+Reduce computational burden +Resist various attack scenario -Proposed technique step by step program wised following this reason create system complexity
[46]	Proposed increase security and reliability for these reasons used PKI based crypto analysis mechanism	× Encryption √ Authentication √ Key Agreement	√ Confidentiality √ Integrity √ Availability	+mitigates several attacks +Achieved lightweight mechanism -High dependency on network technology
[47]	Propose efficient hardware basis authentication and key agreement of smart meter to server	× Encryption √ Authentication √ Key Agreement	× Confidentiality √ Integrity √ Availability	+Efficient for reducing computation and communication time +Resist several attacks -System required many assumption

Notation: Technique Encryption, Authentication, Key Agreemnt (Used √) and (None Used ×)

5.2 Countermeasures

In the latest proposed cryptographic mechanism, we observe that many of the cryptographic aspects used to overcome privacy and protection meanwhile mitigated a well-known cyber attack. According some previous worked illustrate cryptography to accommodate the cryptography aspect whereas some worked used in a single cryptographic aspect or multiple aspects to achieve the aim of cyber security objective. We can already see in section 5.1 which cryptographic parameter has been used to fulfill the security requirements while maintaining the security objectives. So, we can define the effective prospect of encryption, authentication, and key agreement for data protection and privacy guard on smart grid infrastructure from against malicious attackers. There is also some constrained, it is extending for upcoming research trend. Now this section includes a detailed overview how organized the adopt mechanism with cryptographic aspect for development and countermeasures.

5.2.1 Encryption

Encryption is a simple tool for safe communication and security of information for every information system. Encryption systems are an important method for protecting the confidentiality and integrity of data in the smart grid. The smart grid gathers data from a large range of smart grid systems, such as smart meters and smart devices, sensor, and network gateway. Data collection without encryption through an insecure channel created lack of privacy. In this context, previously worked assumed that encrypting data would be a solution to the protection of data whereby unauthorized individuals are unable to access any knowledge about the smart grid system. Mechanisms of encryption are designed to ensure the confidentiality, integrity or non-repudiation of information [17]. There are two types of encryption in smart grid symmetric and asymmetric. Symmetric follows one key use for encryption in sender side, same for decryption in receiver side. In addition, symmetric algorithm known as advanced encryption standard (AES) together with data encryption standard (DES). Asymmetric encryption based on Rivest Shamir Adleman (RSA) which is that using two keys for encryption public/private key similarly in decryption side.

Following above direction of encryption principle, author [38] proposed enhancing security of cloud based AMI in smart grid by using Advanced encryption standard by used quantum key distribution to kept data confidentiality, integrity among avoiding network related cyber attack. Another authors [39] proposed lightweight authentication for massage integrity by using Advanced encryption standard during massage encryption and Rivest Shamir Adleman for session key generation to got desire results and protect from several data attack. Demerit of this technique increase computation and communication overheads. According to solve this issues [43] proposed Elliptic curve cryptography based biometric approaches in smart grid for reducing operational time this methodology acquire less computing time as well communication time while prevent several cyber attack. Similarly as privacy preserving between smart meter and cloud based protocol proposed [39] author by using certificate less cryptography for ensure privacy preservation, perfect forward secrecy, semantic security in smart grid. In this system does not control user anonymity.

5.2.2 Authentication

Authentication is known as the proof of true identity between two objects. In smart grid includes numerous customers, smart meter, sensor, advanced metering infrastructure, meter data management system, and utility server etc. It is very important to know that whether identify exact source destination [48]. Authentication perform on three basic fundamental namely as Cipher text as authentication, Massage authentication code (massage digest) and Hash code as an authenticator. Two types of authentication examined in past research. Some author produced one way authentication to demonstrate identification among user and utility server likewise two-way authentications consequently determined.

Therefore, following superior perception author [33] proposed cloud based demand response based on openADR mechanism. This worked shown reduced computation cost but proved only one way authentication between smart meters to server. Moreover designed two way authentication author [34] proposed secure processing of smart meter by used cloud approaches to reaching the confidentiality, integrity and appeared two way authentication. In the same direction another scheme [37] proposed scalable full security in smart metering this worked perform on Massage authentication basis operation for identification and data integrity. We compared usable different authentication protocol in Table 2 most of the author performs on two-way authentication by help of massage authentication and hash-based authenticator. Basically, authentication depends on cryptographic aspect likely encryption and distributed key management set up authentication between among in smart grid components. Otherwise, the results have not been obtained and the security requirement has not maintained.

5.2.3 Key Management

Key management is vital important for encryption and authentication. It represents crucial cryptographic mechanisms for smart grid to maintain data privacy. Moreover, cryptographic countermeasures not only depend on authentication or encryption similar reinforcement by key management. Insufficient key management may result in potential key disclosure for the attackers, and even endangering the whole aim of safe communication inside the smart grid. Therefore, key management is based on cryptographic primitive distinct process to making the secure smart grid. It is following Public key infrastructure the identity of the two parties shall be checked by a certificate provided by a third party name the Certificate authority (CA). This mechanism done before the connectivity between them. Another approach shared key management which is performing four basic criteria key generation, key distribution, key sorting, and key updating. Due to distributed nature of communication exist in smart grid. Several key management introduced specially in power sector [17] which has follows to secure management, evolve-ability, scalability, efficiency.

In [2] the author proposed secure lightweight scheme for smart grid this worked based on Elliptic curve cryptography for data privacy and hash function suggest by authenticator along transmission between unsecure channel. Unfortunately, did not mention massage integrity between sender and receiver. Similar approaches [43] proposed by author for mutual authentication within used Public key infrastructure biometric approaches for ensure data integrity and mitigation cyber attack another author introduce basis on symmetric cryptography for key development and perform in smart grid. This worked resists several attacks and serve scalability between customer and utility provider. To making efficiency in smart components in this direction author [3] proposed multi factor scheme for key establishment by using fuzzy extractor based technique to reached the security objectives.

Individuals work from the previous methodology to prevent cyber attacks and to protect data protection and privacy during the transition of any services. Thus, in this direction, the previous proposed framework is designed to mitigate many attacks by using the cryptographic aspect and to preserve protection and privacy that are worthy of the need for smart grid security and while pursuing security objectives. According to table 2, we examined those attacks are respectively mitigated by the following research presenting in table 3.

6. DISCUSSION AND FUTURE DIRECTION

So far, we have studied possible security principles, cyber threat and cryptographic aspect premise counter-measures technique at examined current security technologies showed in the smart grid. We note that a number of surveys are already performed regarding security and privacy topics moreover, for the sustainability of the smart grid as a whole focus of relevant our review, [1], [7], [10] [12], [15],[23]. According to previous survey there have low attention about cryptographic aspect to deliver information given in term of specific aspect are evaluated therefore, we motivated as know in heterogeneous smart grid features interaction with a major component such as bulk generation, distribution, transmission, market, operation, service provide and customer with the aid of a secure/unsecure channel. Due to heavy reliance and real-time transmission, it is very necessary to recognize the exact user who interacts with each other and data must private inside the grid components. So, it very important to used cryptographic aspect use in smart grid because it provides data security and privacy along real source to destination during pass any kind of data. For these reasons we evaluate cryptographic aspect in deep way to help for easy to accomplish the future knowledge about it and get possible research flow in smart grid.

Otherwise, it does not compromise due to the high dependency of communication link and latency. If the hunt for the actual sender or recipient has not been achieved, we will lose privacy and change data during the transmission. According to [4] NIST, some basic security concept must exist during the transmission of any information between the two parties. To maintain security priorities the security requirement must be addressed in order to maintain smart grid challenges.

To deal with the following concern previously provided several methods to set up individual and shared cryptographic aspect to reach the proposed goal. This paper point of view cryptographic aspect how to accomplish the security objectives by used following security requirements basically target protect the confidentiality, integrity, availability, non-repudiation. So, we examined based on the cryptographic aspect feature, parameter and protocol efficient role play for identification between two entities during securely data transmission in smart grid infrastructure. Furthermore, we are defined security requirement, challenges then construct categorized attack scenario basis on security objectives. In addition, adds cryptographic aspect split which is occupied effectively compromise security requirement and save security objectives.

According previous literature to deal arrive the goal and maintained challenges which cryptographic parameter compromised for obtaining the security objectives it is effectively plotted in cryptographic study section. Similar work while countermeasures technique, it is showed that impact of encryption, authentication and key agreement meet with the security objectives and relive from well known cyber attack. On the other hand, some weakness has been established due to the cryptographic aspects refers to table 1 pros and cons section and below. Revealed previous cryptographic aspect basis worked presented in table 1 and section 5.2 accordingly. We clearly displayed encryption is most valuable element for supply confidentiality, integrity and non repudiation for data security and privacy according to maintain this issue most of the authors commonly used as encryption/decryption by used symmetric and asymmetric technique unfortunately public key infrastructure raised computation burden and increased communication for session established and distribution. Others way asymmetric key cryptography it is comfortable and facilitates non-repudiation. By the side of symmetric key encryption low process and lightweight but system makes vulnerable for integrity and confidentiality related attack even more damage when it compromised. Precisely authentication is important for verifying the identities but failure of authentication basically one way technique built forward secrecy along anonymity problem. For this situation, mutual authentication in the smart grid is preferable. we evaluated after opined key agreement from previously worked securely across all components with the assistance of encryption and authentication more specifically preserve data privacy and protection between two absolute identities during transmission from malicious intruder and attacker. Most of the key agreements protocol similar as authentication-based technique, hybrid technique and others are presented that has been done effectively to completely fulfill security goals and prevent well-known cyber attacks in the smart grid. However key agreement need high resources for system development and some of key agreements based protocols take much more time this reason formed communication latency to scope for denial of service another demerit lower fast than symmetric key cryptography.

6.1 Future Direction

So far, we have studied the cryptographic effect are critical to maintaining data protection and privacy in a smart grid framework. Many resources are available for the versatile, stable and effective transmission of data in smart grid system [14]. Besides posed some possible weakness consequently should be improves these are indicated Table 2 and it should be very important to make sure all cryptographic aspects included within system with less computation and communication power. Due to the attacker data should be encrypted end to end while transmitted efficiently among smart grid components. There are different intelligent systems communicating with the computer to the person in the smart grid. To further it is of the utmost importance to balance the mutual identity beyond entire smart grid components during data transmission and to transfer any kind of service in action without any cyber attack.

Table 1: Resistance Cyber Attack in Smart Grid

SCHEMES	ATTACKS IN SMART GRID										
	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11
[2]	√	√	√	√	√	√	×	×	×	×	√
[25]	√	√	√	×	√	×	×	×	×	×	×
[27]	√	√	√	√	×	×	×	×	×	×	√
[41]	√	√	√	×	×	×	×	√	×	√	×
[46]	√	√	√	√	×	×	×	×	×	×	×
[49]	√	√	√	√	×	×	×	√	√	×	×
[42]	×	×	×	×	×	×	×	√	×	√	√
[50]	×	×	×	×	×	√	×	×	√	×	×
[47]	×	×	×	×	×	√	×	×	×	√	√
[36]	√	√	×	×	×	×	×	×	×	×	×

A1. Replay attack, A2. MITM, A3. Impersonation Attack, A4. Forward secrecy,
A5. User Anonymity, A6. Eavesdropping, A7. Unknown key share Attack,
A8. Insider Attack, A9. Sybil Attack, A10. Forgery Attack, A11. Dos Attack

7. CONCLUSION

The cyber safety in the smart grid has been attracted by the government, industry and academia as a new research field. Due to the different types of holes, cyber security requirements are very crucial. Therefore, this paper, we examined at the cryptographic aspect to maintain whereby meets the requirements along to the objectives for assure the data security and privacy within each components of smart grid. Furthermore, we are also summarized security objectives, requirements and challenges. Furthermore, according to the previous studied analyze cyber security threats and defense strategies. Suggestions for strengthening smart grid security are explained basis on cryptographic aspects protocol. We observed that for data security and privacy from unauthorized access cryptographic aspect effective role in this field on the other hand, cyber awareness in the smart grid is still in progress according to the review perspective cyber protection and data privacy depth constructions are required to defense against cyber attacks and vulnerabilities. With this article, more detailed understanding of smart grid reliability, it requirements and goals, and future studies can be obtained by readers. In terms of the cryptographic component solution strategy, the current gap could help to make decisions on potential research in this smart grid infrastructure.

ACKNOWLEDGEMENT:

This research was supported by Universiti Putra Malaysia (UPM). Special thanks to supervisor of the research project Dr. Noor Afiza Mohd Ariffin and to the committee member Assc. Prof. Dr. Nor Fazlida Mohd Sani.

REFERENCES:

[1] V. C. Gungor *et al.*, “A Survey on Smart Grid Potential Applications and Communication Requirements,” vol. 9, no. 1, pp. 28–42, 2013.

[2] S. Garg, K. Kaur, and G. Kaddoum, “Secure and Lightweight Authentication Scheme for Smart Metering Infrastructure in Smart Grid,” *IEEE Trans. Ind. Informatics*, vol. PP, no. c, p. 1, 2019, doi: 10.1109/TII.2019.2944880.

[3] P. Gope, “PMAKE : Privacy-aware multi-factor authenticated key establishment scheme for Advance Metering Infrastructure in smart grid,” *Comput. Commun.*, vol. 152, no. October 2019, pp. 338–344, 2020, doi: 10.1016/j.comcom.2019.12.042.

[4] NIST, “NIST Special Publication 1108R2 NIST Framework and Roadmap for Smart Grid Interoperability Standards , NIST Special Publication 1108R2 NIST Framework and Roadmap for Smart Grid Interoperability Standards,” *Nist Spec.*

Publ., pp. 1–90, 2012.

[5] M. Benmalek and Y. Challal, "MK-AMI: Efficient multi-group key management scheme for secure communications in AMI systems," *IEEE Wirel. Commun. Netw. Conf. WCNC*, vol. 2016-Septe, no. Wcnc, pp. 1–6, 2016, doi: 10.1109/WCNC.2016.7565124.

[6] N. Saxena and B. J. Choi, "for Smart Grid Communications," vol. 12, no. 3, pp. 1–12, 2016.

[7] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Comput. Networks*, vol. 169, p. 107094, 2020, doi: 10.1016/j.comnet.2019.107094.

[8] R. E. Pérez-Guzmán, Y. Salgueiro-Sicilia, and M. Rivera, "Communication systems and security issues in smart microgrids," *Proc. - 2017 IEEE South. Power Electron. Conf. SPEC 2017*, vol. 2018-Janua, pp. 1–6, 2018, doi: 10.1109/SPEC.2017.8333659.

[9] M. Z. Gunduz and R. Das, "Analysis of cyber-attacks on smart grid applications," *2018 Int. Conf. Artif. Intell. Data Process. IDAP 2018*, pp. 1–5, 2019, doi: 10.1109/IDAP.2018.8620728.

[10] M. Benmalek, Y. Challal, and A. Derhab, "Authentication for Smart Grid AMI Systems: Threat Models, Solutions, and Challenges," in *Proceedings - 2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises, WETICE 2019*, Jun. 2019, pp. 208–213, doi: 10.1109/WETICE.2019.00052.

[11] J. Xia and Y. Wang, "Secure key distribution for the smart grid," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1437–1443, 2012, doi: 10.1109/TSG.2012.2199141.

[12] X. Liu, L. Golab, W. Golab, I. F. Ilyas, and S. Jin, "Smart meter data analytics: Systems, algorithms, and benchmarking," *ACM Trans. Database Syst.*, vol. 42, no. 1, Nov. 2016, doi: 10.1145/3004295.

[13] M. Nabeel, S. Kerr, X. Ding, and E. Bertino, "Authentication and key management for Advanced Metering Infrastructures utilizing physically unclonable functions," *2012 IEEE 3rd Int. Conf. Smart Grid Commun. SmartGridComm 2012*, pp. 324–329, 2012, doi: 10.1109/SmartGridComm.2012.6486004.

[14] V. Kounev and D. Tipper, "Advanced metering and demand response communication performance in Zigbee based HANs," *Proc. - IEEE INFOCOM*, pp. 3405–3410, 2013, doi: 10.1109/INFCOM.2013.6567172.

[15] K. Kimani, V. Oduol, and K. Langat, "Cyber security challenges for IoT-based smart grid networks," *Int. J. Crit. Infrastruct. Prot.*, vol. 25, pp. 36–49, 2019, doi: 10.1016/j.ijcip.2019.01.001.

[16] S. Shapsough, F. Qatan, R. Aburukba, F. Aloul, and A. R. Al Ali, "Smart grid cyber security: Challenges and solutions," *Proc. - 2015 Int. Conf. Smart Grid Clean Energy Technol. ICSGCE 2015*, pp. 170–175, 2016, doi: 10.1109/ICSGCE.2015.7454291.

[17] Z. El Mrabet, N. Kaabouch, H. El Ghazi, and H. El Ghazi, "Cyber-security in smart grid: Survey and challenges," *Comput. Electr. Eng.*, vol. 67, pp. 469–482, 2018, doi: 10.1016/j.compeleceng.2018.01.015.

[18] D. B. Rawat and C. Bajracharya, "Cyber security for smart grid systems: Status, challenges and perspectives," *Conf. Proc. - IEEE SOUTHEASTCON*, vol. 2015-June, no. June, 2015, doi: 10.1109/SECON.2015.7132891.

[19] R. K. Pandey and S. M. Ieee, "Cyber Security Threats - Smart Grid Infrastructure," 2016.

[20] X. Di Wang, W. Z. Meng, and Y. N. Liu, "Lightweight privacy-preserving data aggregation protocol against internal attacks in smart grid," *J. Inf. Secur. Appl.*, vol. 55, p. 102628, 2020, doi: 10.1016/j.jisa.2020.102628.

[21] A. Anzalchi and A. Sarwat, "A survey on security assessment of metering infrastructure in Smart Grid systems," *Conf. Proc. - IEEE SOUTHEASTCON*, vol. 2015-June, no. June, 2015, doi: 10.1109/SECON.2015.7132989.

[22] F. M. Pires, L. Leon Quinonez, and L. De Souza Mendes, "A Cloud-Based System Architecture for Advanced Metering in Smart Cities," *2019 IEEE 10th Annu. Inf. Technol. Electron. Mob. Commun. Conf. IEMCON 2019*, pp. 1087–1091, 2019, doi: 10.1109/IEMCON.2019.8936283.

[23] A. Ghosal and M. Conti, "Key Management Systems for Smart Grid Advanced Metering Infrastructure: A Survey," *IEEE Commun. Surv. Tutorials*,

vol. 21, no. 3, pp. 2831–2848, 2019, doi: 10.1109/COMST.2019.2907650.

[24] M. B. Line, I. A. Tøndel, M. G. Jaatun, and S. Member, “Cyber Security Challenges in Smart Grids,” pp. 1–8.

[25] A. A. Khan, V. Kumar, M. Ahmad, S. Rana, and D. Mishra, “PALK: Password-based anonymous lightweight key agreement framework for smart grid,” *Int. J. Electr. Power Energy Syst.*, vol. 121, no. May, p. 106121, 2020, doi: 10.1016/j.ijepes.2020.106121.

[26] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. P. Chen, “Cyber security and privacy issues in smart grids,” *IEEE Commun. Surv. Tutorials*, vol. 14, no. 4, pp. 981–997, 2012, doi: 10.1109/SURV.2011.122111.00145.

[27] P. Kumar, A. Gurtov, M. Sain, A. Martin, and P. H. Ha, “Lightweight Authentication and Key Agreement for Smart Metering in Smart Energy Networks,” *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 4349–4359, 2019, doi: 10.1109/TSG.2018.2857558.

[28] M. Hasan and H. Hassan, “A THREE LAYER SECURITY APPROACH USING HONEYPOT TO MITIGATE DDOS ATTACK IN CLOUD-IOT ECOSYSYTEM,” pp. 16–19, 2020.

[29] M. Kamal and M. Tariq, “Light-weight security for advanced metering infrastructure,” *IEEE Veh. Technol. Conf.*, vol. 2019-April, pp. 1–5, 2019, doi: 10.1109/VTCSpring.2019.8746620.

[30] L. Zhang, S. Tang, and H. Luo, “Elliptic curve cryptography-based authentication with identity protection for smart grids,” *PLoS One*, vol. 11, no. 3, pp. 1–15, 2016, doi: 10.1371/journal.pone.0151253.

[31] B. Alohali, M. Merabti, and K. Kifayat, “A cloud of things (CoT) based security for home area network (HAN) in the smart grid,” in *Proceedings - 2014 8th International Conference on Next Generation Mobile Applications, Services and Technologies, NGMAST 2014*, Dec. 2014, pp. 326–330, doi: 10.1109/NGMAST.2014.50.

[32] P. Jokar, N. Arianpoo, and V. C. M. Leung, “A survey on security issues in smart grids,” *Secur. Commun. Networks*, vol. 9, no. 3, pp. 262–273, 2016, doi: 10.1002/sec.559.

[33] “safarzadeh2017.”

[34] A. Brito *et al.*, “Secure end-to-end processing of smart metering data,” *J. Cloud Comput.*, vol. 8, no. 1, Dec. 2019, doi: 10.1186/s13677-019-0141-z.

[35] V. Odelu, A. K. Das, M. Wazid, and M. Conti, “Provably Secure Authenticated Key Agreement Scheme for Smart Grid,” *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1900–1910, May 2018, doi: 10.1109/TSG.2016.2602282.

[36] L. Yan, Y. Chang, and S. Zhang, “A lightweight authentication and key agreement scheme for smart grid,” *Int. J. Distrib. Sens. Networks*, vol. 13, no. 2, 2017, doi: 10.1177/1550147717694173.

[37] M. Nabeel, X. Ding, S. H. Seo, and E. Bertino, “Scalable end-to-end security for advanced metering infrastructures,” *Inf. Syst.*, vol. 53, pp. 213–223, 2015, doi: 10.1016/j.is.2015.01.004.

[38] R. C. Diovu and J. T. Agee, “Enhancing the security of a cloud-based smart grid AMI network by leveraging on the features of quantum key distribution,” *Trans. Emerg. Telecommun. Technol.*, vol. 30, no. 6, Jun. 2019, doi: 10.1002/ett.3587.

[39] N. Saxena and B. J. Choi, “Integrated Distributed Authentication Protocol for Smart Grid Communications,” *IEEE Syst. J.*, vol. 12, no. 3, pp. 2545–2556, Sep. 2018, doi: 10.1109/JSYST.2016.2574699.

[40] S. M. Farooq, S. M. Suhail Hussain, and T. S. Ustun, “Elliptic Curve Digital Signature Algorithm (ECDSA) Certificate Based Authentication Scheme for Advanced Metering Infrastructure,” *2019 Innov. Power Adv. Comput. Technol. i-PACT 2019*, pp. 1–6, 2019, doi: 10.1109/i-PACT44901.2019.8959967.

[41] K. Mahmood, S. Ashraf Chaudhry, H. Naqvi, T. Shon, and H. Farooq Ahmad, “A lightweight message authentication scheme for Smart Grid communications in power sector,” *Comput. Electr. Eng.*, vol. 52, pp. 114–124, 2016, doi: 10.1016/j.compeleceng.2016.02.017.

[42] “he2014.”

[43] A. A. Khan, V. Kumar, and M. Ahmad, “An elliptic curve cryptography based mutual authentication scheme for smart grid communications using biometric approach,” *J. King Saud Univ. - Comput. Inf. Sci.*, no. xxxx, pp. 0–7, 2019, doi: 10.1016/j.jksuci.2019.04.013.

[44] Z. Wan, G. Wang, Y. Yang, and S. Shi, "SKM: Scalable key management for advanced metering infrastructure in smart grids," *IEEE Trans. Ind. Electron.*, vol. 61, no. 12, pp. 7055–7066, 2014, doi: 10.1109/TIE.2014.2331014.

[45] A. Mohammadali, M. S. Haghighi, M. H. Tadayon, and A. Mohammadi-Nodooshan, "A Novel Identity-Based Key Establishment Method for Advanced Metering Infrastructure in Smart Grid," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 2834–2842, 2018, doi: 10.1109/TSG.2016.2620939.

[46] M. F. Moghadam, M. Nikooghadam, A. H. Mohajerzadeh, and B. Movali, "A lightweight key management protocol for secure communication in smart grids," *Electr. Power Syst. Res.*, vol. 178, no. August 2019, p. 106024, 2020, doi: 10.1016/j.epsr.2019.106024.

[47] M. Delavar, S. Mirzakuchaki, M. H. Ameri, and J. Mohajeri, "PUF-based solutions for secure communications in Advanced Metering Infrastructure (AMI)," *Int. J. Commun. Syst.*, vol. 30, no. 9, 2017, doi: 10.1002/dac.3195.

[48] N. A. M. Ariffin, F. A. Rahim, A. Asmawi, and Z. A. Ibrahim, "Vulnerabilities detection using attack recognition technique in multi-factor authentication," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 18, no. 4, pp. 1998–2003, 2020, doi: 10.12928/TELKOMNIKA.V18I4.14898.

[49] K. Wu, R. Cheng, W. Cui, and W. Li, "A lightweight SM2-based security authentication scheme for smart grids," *Alexandria Eng. J.*, 2020, doi: 10.1016/j.aej.2020.09.008.

[50] H. Nicanfar, P. Jokar, K. Beznosov, and V. C. M. Leung, "Efficient authentication and key management mechanisms for smart grid communications," *IEEE Syst. J.*, vol. 8, no. 2, pp. 629–640, 2014, doi: 10.1109/JSYST.2013.2260942.