Journal of Green Engineering (JGE)

Volume-10, Issue-12, December 2020

A Study on the Encryption Algorithms in the Metering Infrastructure of Smart Grids

[1]Anita Philips and [2]J. Jayakumar

[1]Ph.D Scholar, Dept. of Electrical & Electronics, Karunya University, Coimbatore Tamil Nadu. India.
E-mail: anucornee@yahoo.com
[2]Professor, Dept. of Electrical & Electronics, Karunya University, Coimbatore Tamil Nadu. India.
E-mail: jayakumar@karunya.edu

Abstract

In this modern day and age, data is arguably the most valuable asset. Specifically, the piece of information which could be transformed into an entity of economic value has a greater need to be protected. During this era of digital upgrading in every domain, the area of electrical energy is not spared either. The conventional electrical grid systems have become smarter with the implementation of smart grid (SG) technologies, along with its own risks and limitations. The prominent challenge here is to discover and apply the correct methods and technologies to safeguard the data that gets accumulated in every node of the SG networks. This paper focuses on the protection of data collected at the Advanced Metering Infrastructure (AMI) of the SGs. The data that becomes available in the smart meters of AMI needs to be encrypted before any communication steps are initialized. Currently, many proven algorithms, and appropriate key management solutions have been suggested to establish end-to-end secure communication for smart grid. Here in this paper, the standard encryption algorithms which are commonly used in AMIs are analysed. Also, the challenges in implementing the encryption algorithms in AMI are investigated with the focus on secure key management. The current standards in implementing the encryption techniques in AMI are also briefly studied.

Journal of Green Engineering, Vol. 10_12, 13150-13176.

Keywords: Smart Grid; Cyber Security; Advanced Metering Infrastructure; Encryption techniques; Key Management Systems; Lightweight KMS Solutions.

1 Introduction

The definition according to European Technology says an SG as a power system that integrates all entities like generators and consumers for the purpose of delivering sustainable and efficient energy supply. The smart grid (SG) system includes automation and controllable power devices in the whole energy value chain from production to consumption. Particularly, the computing and two-way communication capabilities of the SG aids to exchange real-time information between utilities and consumers, thus achieving the desirable balance of energy supply and demand. During this communication life-cycle of SG, when power is transferred from production to user, the utility companies receive information like electricity consumption and the actual energy that is potentially transferred. This data may then be used for forecasting the times of high demand, detect power failure and save excess power thus meeting the energy demands efficiently.

Meanwhile, upgrading the power grid to smarter grid gives rise to new challenges in terms of security which have to be addressed before execution. The rapid advancement of the attacks, especially of the cyber domain is alarming. As the number of threats increases tremendously, according to the Federal Energy Regulatory Commission (FERC) policy, for the operation of the SG, cyber security is essential and the cyber security standards need to be developed at a critically important speed. In the SG, the physical power system is integrated and tightly coupled with the cyber system. Therefore, in the case of any attack in either domain may have an impact on the other domain and lead to potential cascading failures [Black-outs, financial losses etc.].

Advanced Metering Infrastructure (AMI) is essentially the crucial part of SG and aids for the efficiency, sustainability and reliability of the system. Therefore the cyber threats that are possible in the AMI has a huge impact on the reliable and efficient operation of SG. To combat the threats targeting information security in AMI infrastructure, one of the major solutions employed is the encryption algorithms[9],[11-16],[21-26],[29][35][62,63].

According to the definition in [2], a mathematical operation to encrypt the data using an algorithm where the data is transformed to a cipher text with no meaning and employs a key to retain data to the plain text is called an encryption algorithm. The successful operation of the encryption algorithms in terms of computation speed, complexity, and efficient security of data solely depends on the management of cryptographic keys.

Key management is a process that involves key generation, storage, distribution and re-keying if required. Cryptographic key management is a challenging task in the SGs as the system includes a vast number of

components. Many researches are being carried out for the establishment of secure key management solutions [KMS] in the AMI of SGs. Particularly, lightweight KMS solutions are popular in smart meters considering its low memory capacity and to reduce the computational overhead[4]-[7].

This paper aims to present a background knowledge on the implementation of encryption algorithms in the AMI of SGs and the corresponding key management techniques applied.

In Fig 1, the no. of articles reviewed are graphically represented. Out of a total of two hundred and sixteen articles, the most relevant documents related to security issues, encryption and key management in smart grids, fifty of them are selected and reviewed in detail.

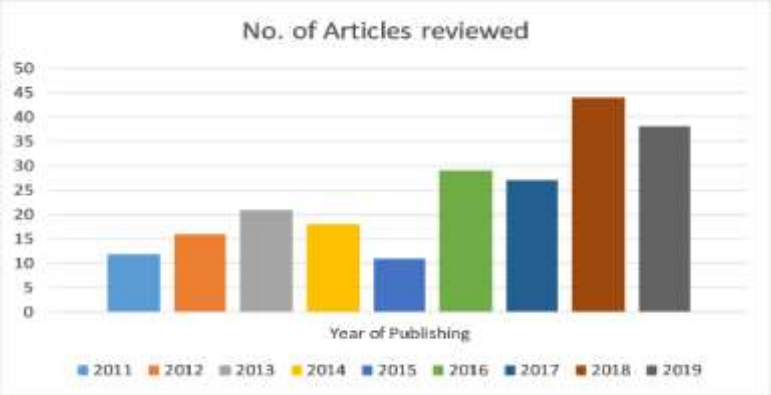

Figure 1 No. of Articles Reviewed

The following sections are organized as: Section 2 describes the background of SG and AMI components, Section 3 presents the outline on the security issues in SG, Section 4 presents an overview of the commonly used encryption algorithms, Section 5 deals with the existing proposed cryptographic solutions and key management solutions applied in AMIs, Section 6 discusses some of the case studies in the field of implementing the encryption algorithms, Section 7 identifies the future scope on researches on new encryption and security solutions in SGs and Section 8 concludes the study.

2 Background

In this section, the framework and standards of SG as stated by National institute of Standards and Technology (NIST) are explained and the components of AMI are discussed. Generally, a framework provides a set of shared principles and practices, and an agreement on standards and protocols. The smart grid framework according to NIST illustrates the conceptual model as shown in Fig.2.

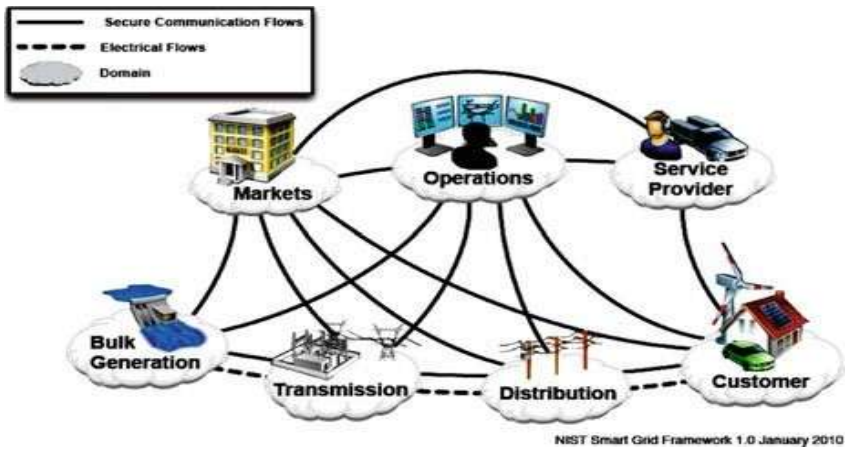

Figure 2 Smart Grid Framework [1]

The US Department of Energy (DOE) released the metrics for identifying the progress of smart grid implementation which mentions the characteristics to be incorporated in the SG as listed below:

i. Facilitate informed choices to end users
ii. Availability of the option for energy storage.
iii. New markets development.
iv. Enhance the quality of power for the range of applications
v. Optimize utilization of assets and operating efficiency
vi. Predict failures in a self-healing manner
vii. Resilience for physical, cyber threats and natural disasters

The crucial component of the SG network is the AMI as this houses the critical data required for the successful operation of the entire SG network. In [8], the components of AMI are discussed, the smart meters, data accumulators and network components are included in the AMI. The consumer's electricity usage information is transmitted to the meter data management system (MDMS). The AMI comprises of components as shown in Fig.3

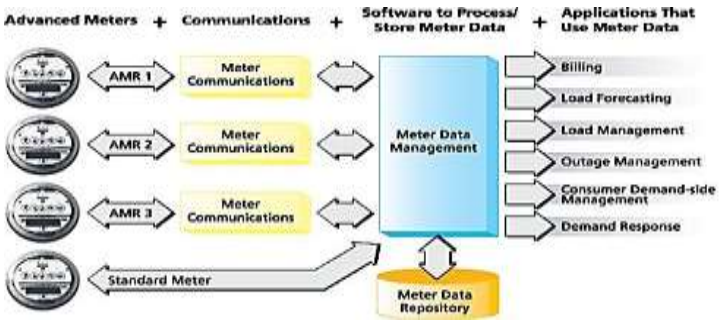

Figure 3 Components of AMI [27]

The AMI of SGs includes access points, smart meters, communication network and meter data management systems (MDMS). The customer information and power usage readings recorded in the smart meters installed in the customer premises are very critical because this usage information transmitted to the control / utility center helps to determine the efficient energy consumption. According to [24], the communications infrastructure in AMI can consist of many communications networks like the Neighborhood, Home and Wide Area Networks. Hence, in AMI many systems and technologies are integrated to provide efficient energy consumption. The main drawback of establishing security in AMI is stated in [25] as low computational ability and limited memory of the smart meters, and the scalability of AMI being a vast network with enormous number of meters.

3 Smart Grid Security Issues

The simple definition of Cyber Security could be stated as a set of techniques to protect systems from digital attacks. Major areas of cyber security could be listed as information security, network security and application security. Here, the information security plays the key role, as most of the business entities are closely tied with various types of data. NIST defines information security as a condition that is established after employing required protective measures which enables a business to carry out its essential operations in spite of the potential threats to its data.

A combination of deterrence, predict and prevent, recovery, early detection, and remedial measures that is to be included in the business's risk management methods are some of the protective measures for information security. Information security comprises of three core principles:

- Confidentiality – Authorization is required for accessing the information.
- Integrity – Modifications can be permitted only for authorized entities. Availability – Availability of the information for authorized personnel at all allowed times.

Together these principles, the "CIA triad," provide secured access to correct data for the authorized entities. Confidentiality, Integrity, and Availability (CIA) ensures the security of information, and it is obvious that breaking "CIA" leads to a sequence of cyber threats.

In [17], the vulnerabilities of the huge heterogeneous SG network such as physical security, user security, intelligent electronic devices, age of power systems, device-to-device communication, increasing no. of stakeholders are discussed. The types of possible attacks are highlighted and an extensive list of security solutions are proposed. The work in [8] highlights the importance of AMI in SG network and the active and passive defenses against the security threats are investigated. Public Key Infrastructure [PKI] for the passive defense and the Intrusion Detection System [IDS] for active defense are studied and the combined defense is suggested to overcome the

limitations of individual defenses.

The security challenges of SG and the possible security solutions are discussed in [18]. The paper in [40] considers the security solutions of SG as a whole system instead of component-wise solutions. The advances in cyber security of SGs are discussed and the shortcomings are identified. System failures, physical threats, targeted attacks and hybrid attacks are investigated. Efficient security recommendations are made for secure information exchange across the SG domain.

In [20], the cyber physical nature of the SG is considered and the attack surfaces are analysed. The attack models and the impacts on cyber and physical domains are studied and the defense strategies are recommended. The work in [39] discusses the security issues found in smart meter systems of SG. The attacks are analysed based on the area of vulnerability namely network, physical hardware and data. The cyber-attacks and their remedial measures in each of these areas are summarized.

4 Standard Cryptographic Algorithms

In general, cryptographic algorithms are the execution of certain set of mathematical operations to achieve the features of information security like entity authentication, data integrity, data confidentiality and authentication. In any general form of cryptographic encryption, the encrypted data transmitted between two entities can be explained as shown in Fig.4.

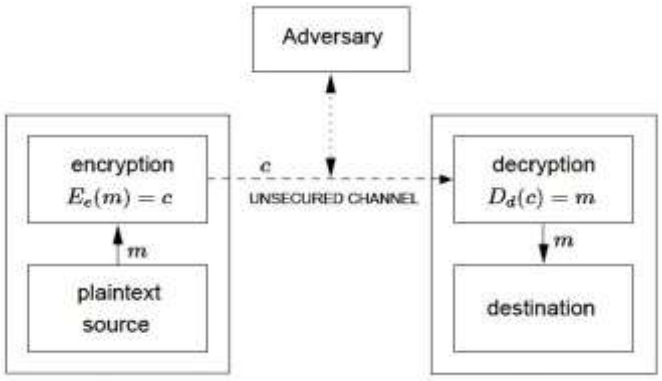

Figure 4 Communication of Two Parties with Encryption [3]

In this model of encryption, without knowing the encryption and decryption key pair (e,d), the adversary gaining access to the communication channel cannot restore the plaintext (m) from the cipher text (c).

The modern encryption techniques are broadly classified based on the no. of cryptographic keys used. The major groups of encryption algorithms are Symmetric, Asymmetric and Hash encryptions. The classification of encryption algorithms can be illustrated as in Fig 5.

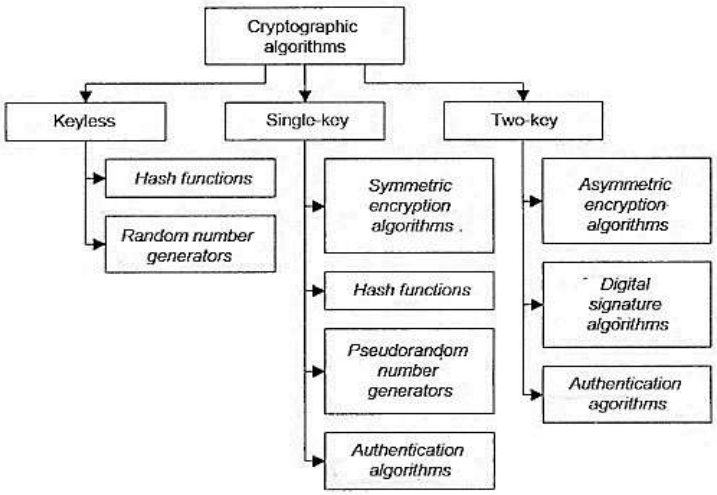

Figure 5 Classification of Encryption Algorithms

Hash encryption algorithm use the hash functions to transform the messages to digests of various lengths. Symmetric encryption uses a shared key between the sender and receiver, whereas asymmetric encryption uses two keys, a public key and a secret key which are linked mathematically. The symmetric encryption technique can be further implemented using Block ciphers or Stream ciphers.

The most widely used symmetric encryption techniques are Data Encryption Standard [DES], Triple DES [3DES] and Advanced Encryption Standard [AES], Blowfish and RC5. Some of the common public key cryptographic algorithms are Rivest-Shamir-Adleman [RSA] and Elliptic Curve Cryptography [ECC] techniques. Some of the characteristics of the algorithms are shown in Table 1.

Table 1 Characteristics of Encryption Algorithms

Feature / Algorithm	Hash	Symmetric	Asymmetric
No. of Keys	0	1	2
NIST recommended Key length	256 bits	128 bits	2048 bits
Commonly used	SHA	AES	RSA
Key Management/Sharing	N/A	Big issue	Easy & Secure
Effect of Key compromise	N/A	Loss of both sender & receiver	Only loss for owner of Asymmetric key
Speed	Fast	Fast	Relatively slow
Complexity	Medium	Medium	High
Examples	SHA-224, SHA-256, SHA-384 or SHA-512	AES, Blowfish, Serpent, Twofish, 3DES, and RC4	RSA, DSA, ECC, Diffie-Hellman

4.1 Hash Based Encryption Algorithms

A hash function is defined as an algorithm where large data of random size is transformed into small data of fixed size. This transformed data is called the digest or hash value. The hash functions operate in a one-way manner and do not require any key. In this method of one-way operation, it is not possible to re-generate the input from a certain digest. The hash functions are generally used for message and source integrity services, generation and verification of digital signatures, key generation in key-establishment techniques and pseudorandom number generation. A general process flow of a hash encryption algorithm is shown in Fig 6.

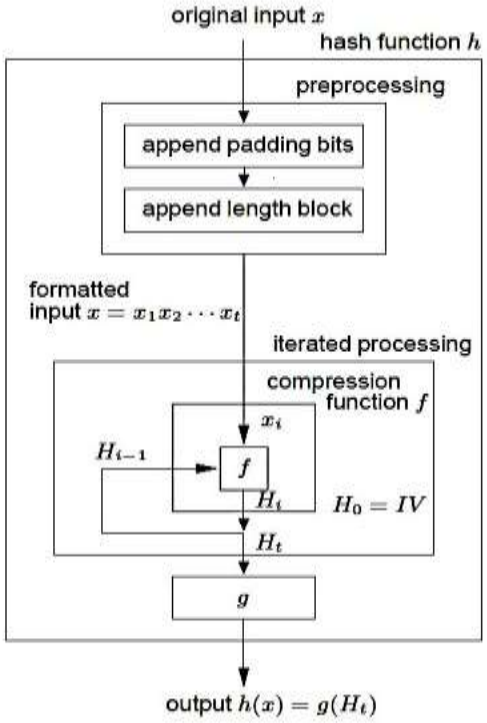

Figure 6 Hash function [3]

4.2 Symmetric Algorithms

Generally, the symmetric algorithms are employed to establish data encryption and data integrity due to its proven performance efficiency whereas the public key cryptography facilitates repudiation through signatures and key management. Some of the symmetric block cipher algorithms are discussed below. In the DES algorithm, [28] describes that there are two permutations and sixteen Feistel rounds. Fig 7 shows the elements of DES cipher at the encryption site.

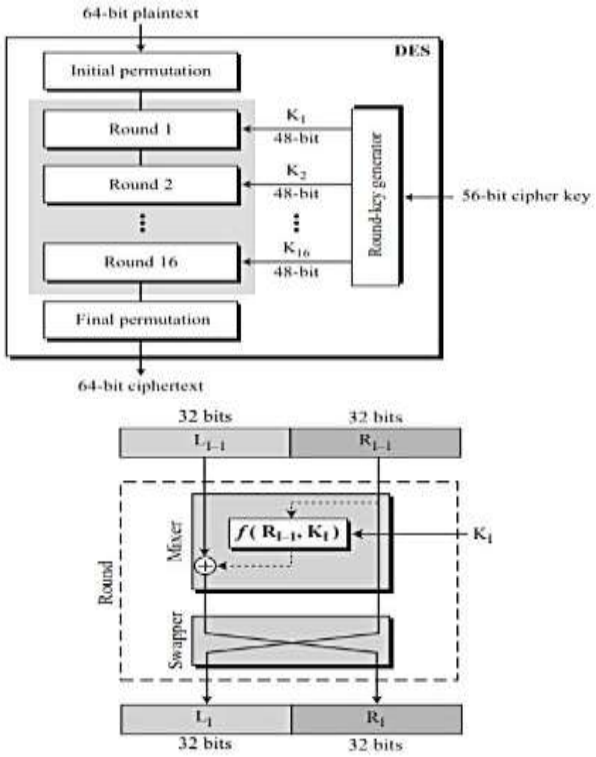

Figure 7 DES Encryption and a Typical DES round [28]

There are 16 rounds in DES. A typical round in DES algorithm is also shown in Fig. 7.

The DES key size is extended in 3DES algorithm and the DES algorithm is run thrice, with three 56-bit keys as explained below:

- Using key 1, the plaintext is encrypted.
- Using key 2, the encrypted key is decrypted.
- Using key 3, the decrypted content from above step is again encrypted.

In the three-key method the text is encrypted three times in succession, thus providing more security. The 3DES structure is illustrated in Fig 8.

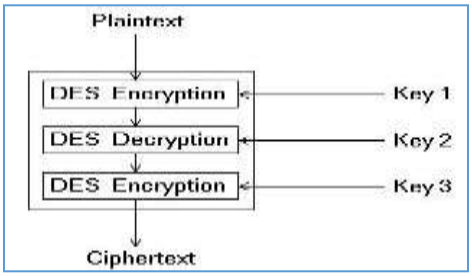

Figure 8 3DES Structure

Another such symmetric block cipher algorithm explained in [22], the AES encryption algorithm has proven to be more secure, fast and efficient in the AMI node of SGs due to its robust security and encryption/decryption speed. The AES structure is shown in Fig 9.

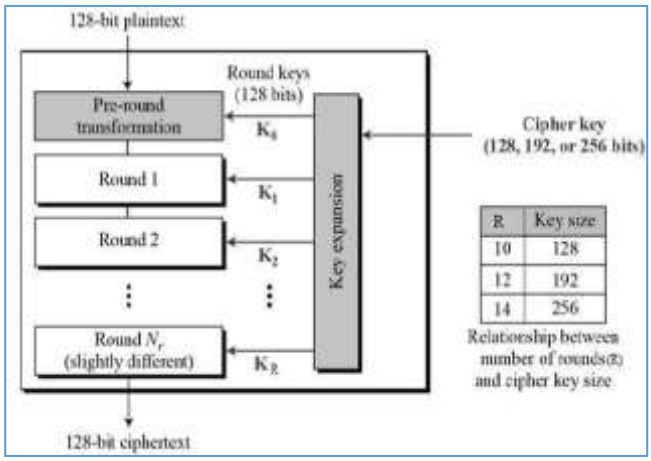

Figure 9 AES Encryption [10]

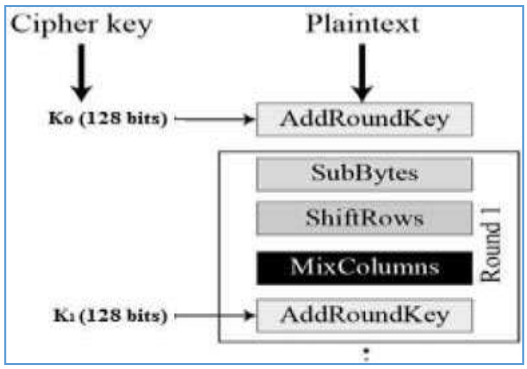

Figure 10 First Round [10]

A typical round of the encryption process which has four sub processes is shown in detail in Fig.10. The AES algorithm provides a complete security solution against Brute-Force attacks.

4.3 Asymmetric Algorithms

Some of the common public key cryptographic algorithms are Rivest-Shamir-Adleman [RSA] and Elliptic Curve Cryptography [ECC] techniques. The RSA (Rivest-Shamir-Adleman) algorithm is a common asymmetric

public key encryption algorithm where large integers are used. There is a single round of encryption and uses two different keys as explained in [61]. The RSA process flow is described in Fig 11.

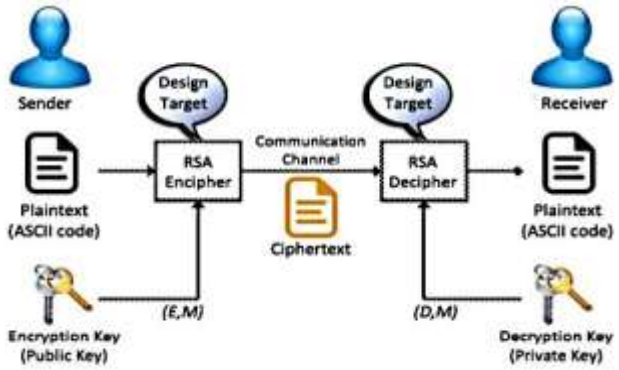

Figure 11 RSA Algorithm Structure

Another widely used public key cryptography algorithm is the Elliptic Curve Cryptography [ECC]. It is based on elliptic curves over finite fields structures. The elliptic curve representation can be shown as in Fig. 12

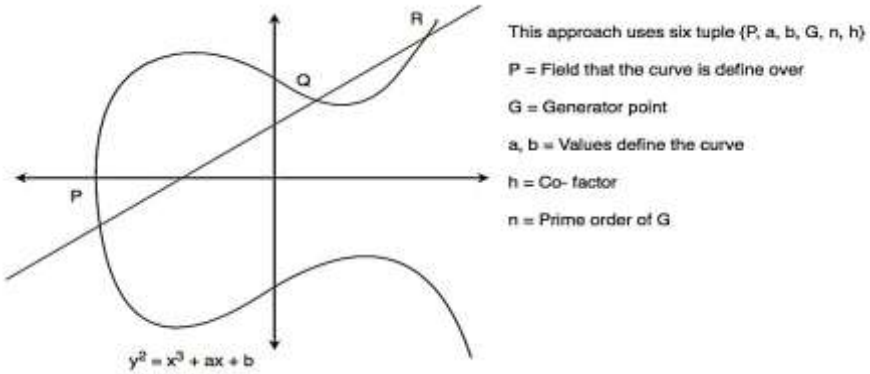

Figure 12 Elliptic Curve Representation

5 Encryption Algorithms for Smart Grids

5.1 Existing Encryption Methods Proposed for AMI

For secure transmission of data between the smart meter and utilities require the implementation of encryption techniques. Most importantly, the primary task is to identify the most effective encryption algorithm to be employed for smart meter data. To achieve efficient information security, symmetric block ciphers are preferred in the AMIs. In block ciphers, the plaintext bit stream is grouped into blocks of fixed size and for each block, the same cryptographic key is to generate the cipher text.

The authors in [46] recommend the use of Spritz encryption to protect consumer data. This method is based on the RC4 (Rivest Cipher 4) encryption which is usually implemented in the Open Smart Grid Protocol (OSGP) standard. To overcome the weakness of RC4 algorithm, the spritz method is proposed to be used which is a stream cipher algorithm and works similar to RC4-like algorithm and developed to overcome the weak design in RC4 to achieve total security. The performance of the proposed solution shows significant improvement. In this technique, the brute force attacks on small keys are efficiently avoided.

A different approach is discussed in the document [47], wherein extended Chebyshev chaotic maps are used in an anonymous password authenticated key exchange protocol. This method proves to overcome the vulnerabilities found in [48] which introduced a two-phase authentication and key agreement scheme for isolated smart meters, particularly the desynchronization attacks and forward insecurity. This protocol works in three stages like initialization, authentication and password change.

In [49], the authors propose an order preserving encryption [OPE] technique in which the ciphertext space maintains the order of numerical data. Considering the scenario where computations are to carried out jointly by individual meters and suppliers, this solution recommends smart meters to transmit the periodical metering data to the utility using the privacy preserving method. Hence, in this method, after their encryption the order of plaintext values are preserved. Here, the privacy preserving unique statistics scheme (PPUS) is employed for the smart meters.

A hybrid encryption solution is found in [50], where both the asymmetric and symmetric key encryptions are incorporated to establish security in smart metering networks. Advanced Encryption Scheme (AES) and Elliptic Curve Integrated Encryption Scheme (ECIES) are the two methods chosen in this solution and a precomputation procedure is presented to improve speed and to overcome the computational overhead of ECIES. Here, Hybrid Cryptosystem [HC] concept is used which is a method of encryption that together employs the strong security of public key encryption and the productivity of symmetric encryption. The two subsystems of HC are data encapsulation which uses symmetric encryption algorithms and key encapsulation which uses public key algorithms. The AMI messages are encrypted using AES 128 system and the arbitrary key is encrypted using ECIES. To improve the efficiency of the proposed protocol, a precomputation parameter is used the precomputed values are frequently updated which are then used to produce the cryptographic keys. In this proposed solution, the computation, communication and storage overheads are proved to be reduced along with the security requirements.

Similarly, the authors in [52] have proposed the combined usage of AES and RSA algorithms for generating session keys. The hash based message authentication code is also used for message integrity. The method works in

three phases - initialization, authentication and message transmission. Here mutual authentication is provided and the MiM attacks and forward secrecy issues are handled.

A scalable key management scheme is proposed in [51], in which Physically Unclonable Function [PUF] based approach is used for authentication of metering units and key management. The PUF devices resist spoofing attacks by using a hardware based strong authentication mechanism. The master key is not stored and hence the PUF based secret key generation mechanism protects strongly against key leakage. Along with this, a broadcast key management scheme [BGKM] is used to assign a secret to each smart meter to generate the group key. By using BGKM, the actual private key can be obtained by combining the individual private key with a public information. Here, the solution is completely scalable as the number of smart meters can be increased without any effect on the old meters.

A method to preserve the privacy of the consumer, in the midst of the compromised substation and some attacked smart meters is proposed in [53] wherein the consumption data from the members of a group are homomorphically aggregated. The conversion of plaintext into ciphertext that can be analyzed and worked on as similar to its original form is called homomorphic encryption. In this proposed solution, the consumption messages which are masked with random values are sent by the smart meters using a shared group public key and individual private key are homomorphically aggregated and encrypted. Later the ciphertexts when returned to the smart meters are partially decrypted and sent to the utilities for further computations. Hence the relationship between the customers and their respective energy consumption values are not transparent, thereby preserving the privacy.

An additive homomorphic encryption is used by the authors in [54] and a privacy-friendly architecture is proposed. Each smart meter's data is encrypted in shares using the public key and sends the cipher to the utility. Subsequently, the utility homomorphically aggregates all the data encrypted under the public key and sends back to the meters. The received cipher text is decrypted by each meter. The results are sent for computation, where the all received results are summed to get the aggregated energy consumption.

A similar method of homomorphic encryption using factor problem is employed in [55], which suggests accumulating homomorphically the consumption of the members in a particular domain, thus preserving customer's privacy. Here, the electricity reading is masked them with a random value and then it is encrypted. This method requires communication with the utilities, but not among the smart meters.

In [56], a privacy-preserving electricity billing method is recommended in which the data quality is not compromised. The functional encryption is used in this proposed solution. Here, the smart meter encrypts the consumption data and transmits to the utility which a restricted decryption key is present with which the weighted sum can be obtained and cannot

directly recover the consumption information. The separate consumption details of each time unit is hidden from the utility provider, thus this method efficiently solves the privacy issues.

A dynamic programming algorithm, DNA-based authentication solution is proposed in [57] where the DNA-based key generation algorithm and the key based random permutation [KBRP] algorithms are used for authentication. Here, the exchange of different groups of data between the smart meters and server is possible without data leakage to any intermediate adversary. There is no requirement for the exchange of cryptographic keys between the entities.

In [58], a sigcryption scheme namely Ciphertext-Policy Attribute Based Encryption [CP ABSC] is proposed. Here a message can be signcrypted utilizing the access rights which is defined in the message. The ciphertext can be designcrypted only when the attributes specified in the data access rights are provided. In smart grids, this method is proved to be very efficient in establishing security in multicast and broadcast message communications.

5.2 Key Management Solutions in AMI

The traditional and general security solutions applicable to hardware devices, network elements and software applications are no longer able to provide comprehensive readymade alternatives to secure the systems. As the scalability of the system increases, component-wise security solutions are essential for end-to-end security. Likewise, a single key management infrastructure is not feasible for use in all the components of the SG. Suitable KMS solutions are to be identified for every component to derive and distribute the encryption keys. [23]

In [43], the authors have proposed a framework for key management based on key graph and are utilized for unicast, broadcast and multicast transmission modes. The performance is arguably better with less computational overhead and forward / backward securities ensured. A similar approach is suggested in [42] with a multi group key graph technique applied for different modes of communications and proved to have low communication and storage overhead.

A key agreement scheme is proposed in [19] and the session key is secured under the Canetti-Krawczyk CK adversary model with reduced computation overhead. A hybrid key management scheme is suggested in [41] for different modes of communications in which the method of One way function tree [OFT] is used. The computations are majorly carried out in the utility servers keeping the smart meter burden-free.

In [44], a two level encryption method based on two partially trusted simple servers is proposed. Data encryption and node authentication are achieved with enhanced data security. An identity based key establishment

protocol based on elliptic curves [ECC] is proposed in [45] to establish resilience for well-known attacks.

The most critical part in encryption is the key management. The best approach is to be identified and designed. Generally, in key management the keys are classified as follows:

- Session keys - one-time keys generated for every new message.
- Public keys - used in asymmetric encryption.
- Private keys - used as shared keys in symmetric encryption and also used as the additional key in asymmetric encryption.
- Passphrase-based keys - used for protecting private keys.

In [32], Lili Yan, Yan Chang and Shibin Zhang propose a lightweight authentication and key agreement scheme to provide mutual authentication and key agreement without a trust third party. The scheme works in four stages like Registration, Authentication, regeneration of keys and multicast key generation. The session key is generated in the key agreement phase and refreshed in a short-term or long-term process.

Key management schemes are proposed in [33] where multi-group key graph structure is used for individual and batch rekeying to support different modes of communications. Security analysis assures strong forward and backward secrecy and the batch keying schemes prevent out-of-sync problem.

As in [34], a lightweight authentication protocol is proposed for the two-way device authentication of the Supervisory node [SN] and control node [CN] in SGs by Qianqian Wu, Meihong Li. This scheme is based on the shared security key which is embedded in the device chip and random number to authenticate the identity of SN and CN. In this method, third party services and certificates are avoided, and a symmetric cryptographic algorithm and hash operation are adopted. A comparison of the various proposed encryption and key management technologies for the metering infrastructure of SGs are listed in a tabular format in Table 2.

Table 2 Comparison of Existing Encryption / Key Management Solutions for AMI

Contributed by	Encryption / KMS Technique	Description	Advantages
Lincoln Kamau Kiarie Et al. [2019]	Spritz Encryption	RC4 like stream cipher algorithm	Effective against Brute Force attacks
Dariush Abbasinezhad-Mood and Morteza Nikooghadam [2018]	Chaotic maps	Two-phase authentication and key agreement scheme with extended Chebyshev chaotic maps	Protects isolated smart meters from desynchronization attacks and forward insecurity.

Iraklis Leontiadis, Refik Molva, Melek O¨nen [204]	Order Preserving Encryption	Order of plaintext value is preserved after encryption	Protects consumer privacy efficiently
Samer Khasawneh & Michel Kadoch [2017]	Hybrid encryption with Elliptic Curve Integrated Encryption Scheme (ECIES) and Advanced Encryption Scheme (AES)	Data encapsulation with symmetric and key encapsulation with public key encryption	Additional security with recomputation value for updating keys
Mahmood K, Chaudhry Et al. [2016]	Combined usage of AES and RSA algorithms	Hash based message authentication code used for message integrity	MiM attacks and forward secrecy issues mitigated.
Nabeel M, Ding X, Et al. [2015]	Physically Unclonable Function [PUF] based approach	Hardware based authentication mechanism, broadcast key management scheme [BGKM]	Key leakage and spoofing attacks handled, solution is highly scalable
N. Busom, Et al. [2015]	Homomorphic encryption	Data masked with random values and usage of shared group public key and individual private keys.	Complete preserving of consumer privacy, as data is homomorphically aggregated and encrypted.
Garcia F and Jacobs B [2011]	Additive homomorphic encryption	Shared group public key and individual private keys with homomorphic aggregation and encryption	Consumer privacy preserved efficiently.
Jalaja Valisireddy and Anjaneyulu [2018]	Homomorphic encryption using factor problem	Data masked with random value, homomorphically accumulated and encrypted using factor problem method	Consumer privacy preserved fficiently
Jong-Hyuk Im, Et al. [2019]	Functional encryption	Restricted decryption key provided to utility to receive weighted sum of data	Consumer privacy issues handled

Shakir M. Hussain, Et al. [2017]	DNA based encryption	Key based random permutation [KBRP] algorithms used for key generation	No exchange of keys required, effective key management.
Chunqiang Hu, Jiguo Yu, Et al. [2018]	Ciphertext-Policy Attribute Based Encryption	Access rights specified in the message itself	Very efficient for security in broadcast communications.
Imtiaz Parvez, Arif I. Sarwat, My T. Thai, Anurag K. Srivastava [2017]	Two level encryption	Two partially trusted simple servers for data encryption and node authentication	Improved data security
Mourad Benmalek, Et al. [2018]	Rekeying using multi-group key graph structure	Individual and batch rekeying for unicast, multicast and broadcast communications	Forward and backward insecurities well handled.

5.3 Key Protection Issues

Protecting the cryptographic keys can be efficiently done by defining and enforcing proper key management policies. A higher level of authorisation in the key management process for release or recovering of the key should be included in the key management policy. Individual key usage policy must be applied for every key to define which device, group of devices, or types of application can request it, and the type of operations like encrypt, decrypt or sign that device or application can perform. In this way, it is ensured that the secure keys are constantly protected. According to 'Recommendation for Key Management- part 2', published by NIST [30], the segregated roles in the key management are

- Separation of duties - divides critical functions among different staff to enable the option of not giving enough privilege to one individual.
- Dual Knowledge - two or more persons operating in concert to protect sensitive cryptographic key information.
- Split Control - the combined value of an encryption key or paraphrase key is unknown to anyone.

In [31], rekeying is defined as in the encrypted storage, the method of updating the existing key to a new value. Here, the old key is thus retired and the new key is used for all further encryptions. Also, [31] focuses on Access Revocation, wherein if the entity no longer stays in the group, the access privileges are to be removed for that entity to ensure data security. The encryption key life-cycle is illustrated in Fig 13.

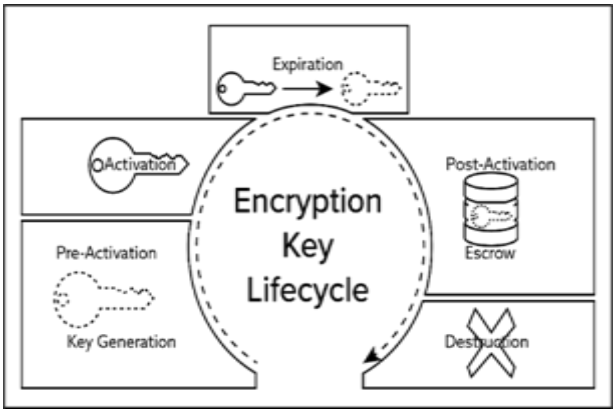

Figure 13 Encryption Key Life-Cycle [38]

The cryptographic key management system [CKMS] security policy as found in [30] emphasizes that every cryptographic key needs to be replaced as it reaches its limit of lifetime. Hence, it is important that the expired keys be updated by rekeying to enable continued protection of encrypted data with new keys.

5.4 Standards Implementing Encryption in AMI

The way that encryption algorithm is implemented is crucially important in the AMI setup of the SGs. If the encryption is poorly tested or subjected to insufficient review, there may still be vulnerabilities and opportunities arise for adversaries to gain access of the data or break the encryption. Hence, it is important that the encryption solutions meet the current standards during implementation.

As a general standard, encryption algorithms must satisfy the standards mentioned in NIST publications, with effect from the date of implementation. According to NIST publications, the algorithms from an approved list can only be implemented by the cryptographic modules. These approved algorithms widely includes the standards for all types of encryptions like symmetric, asymmetric, hash and message authentication modules. The algorithm requirement states that set defined as "AES-compatible" or "partially AES-compatible" must be met by the ciphers [36].

The accredited Cryptographic and Security Testing (CST) laboratories are used to test the cryptographic modules. As in [37], to test the cryptographic modules, these institutions use different strategies like Derived Test Requirements (DTR), Implementation Guidance (IG) and applicable Cryptographic Module Validation Program (CMVP) programmatic guidance.

The comprehensive standards for the implementation of encryption algorithms are found in the various NIST publications.

6 Case Studies

Two types of real world large scale implementations of encryption techniques are discussed here, the ATOS cryptoserver solution which uses hardware cryptographic computations and an application level encryption using THALES SafeNet ProtectApp.

6.1 ATOS Worldline Cryptoserver

According to the case study reported by Atos, the information technology service provider company has a successful data encryption solution delivered to the energy provider Enexis of Netherlands [59].

With the implementation of smart meters in 7 million households, the consumers are provided with informed choices of energy usage and the utility company with accurate consumption data to enable efficient energy delivery. The implementation was delayed due to security concerns, in particular, to those related to data confidentiality. Enexis being one of the largest energy utility provider, in order to influence most customers, provided the utmost privacy and security to user data in collaboration with Atos. Hence, a hardware based crytoserver solution is developed, wherein the Cryptographic operations happen only inside the Hardware Security Modules [HSMs]. The data collection by Enexis uses the DLMS/COSEM Protocol-based data acquisition system. Here, security for data collection is achieved via a cryptographic system that uses cryptographic keys for encoding and decoding the data, while ensuring that non-authorised access is made virtually impossible.

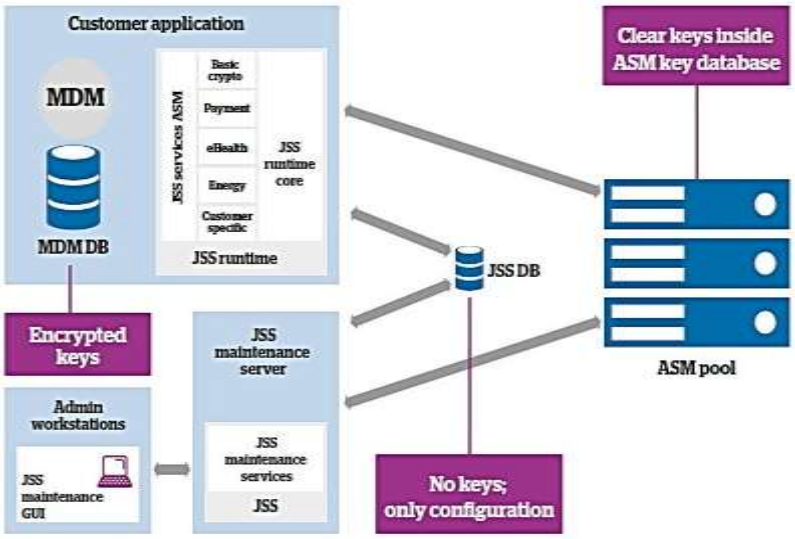

Figure 14 Interaction between Cyrtoserver and Core Processes [59]

The encryption process is explained in Fig. 14. The encrypted data is stored in the MDM database and sent to the ASM server pool which comprises the HSMs with embedded encryption keys, enabling the encrypted data from customers to be turned into data that can be used within core applications to determine the amount of energy consumption, payment data and other necessary information for managing the business.

In this solution, data in transit is always unreadable to the outside world. It becomes a plaintext message only when decrypted within the HSMs. No cryptographic keys or security operations are ever visible to the main servers or the core applications, themselves. This Cryptoserver project proved to be one of the earliest, largest, scalable and successful smart meter implementations that is fully based on accepted international standards.

6.2 Thales SafeNet ProtectApp

Application level data encryption provides data protection at earlier stages of information lifecycle, controlling the risk of data exposure. SafeNet ProtectApp from Thales [60] provides the data encryption solution in which the data is encrypted immediately after generation, and is securely transmitted throughout the lifecycle irrespective of data iterations.

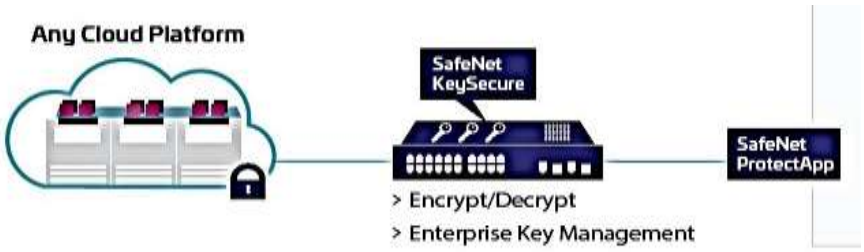

Figure 15 SafeNet ProtectApp Process Flow

Along with it, SafeNet KeySecure provides a scalable and centralized key and policy management. This solution has in-built capabilities of re-keying and cryptographic functions like encryption, decryption, digital signing and verification and authentication. The process flow is explained in Fig. 15. The data and encryption keys are fully controlled and owned always with all with security requirements achieved. Comprehensive logging and auditing capabilities are also available in this interface with which encrypted data and keys can be accessed for addressing the internal policies.

7 Future Directions

The ultimate goal of utility providers in the smart grid networks is to eliminate the vulnerabilities which may lead to data leak and information

theft from the customer's premises. Particularly, in the energy industry dealing with hundreds of millions of monetary transactions, the collection of incorrect consumption data may lead to heavy losses. To achieve complete security of data, various methods and security solutions need to be employed at different points of the network, the most important solution being encryption techniques. As many standard encryption methodologies are in use, the emerging trend predicts the use of the latest, much more sophisticated algorithms.

Quantum cryptography combines the quantum mechanics with cryptographic operations to establish the highest level of data security. Using the quantum mechanics, the key distribution issues can also be greatly solved with the quantum key distribution [QKD] feature. Application of quantum cryptography for securing smart meters can be an interesting and upcoming research direction.

Another emerging technology of Blockchains can be employed in smart metering systems as a means to safeguard the smart meters from cyber-attacks. Here, single points of failure can be avoided, so in the case of an individual smart meter being hacked, the propagating failures can be eliminated. In such a distributed network, an attacker would have to hack each single device to obtain each single key. Adoption of blockchain technology in the smart meter market can be a very effective solution for cyber security issues in the smart grid and a developing area for research.

8 Conclusion

The heterogeneous nature of smart grid networks gives rise to many challenges in implementing the end-to-end security solutions. In particular, the cryptographic techniques used for information security of AMI data of SG's are very efficient as well as challenging to implement. From the analysis of existing literature, it is observed that multiple symmetric and asymmetric encryption algorithms are available, and the usage and application decides the best one to be applied. In this paper, the symmetric block cipher algorithms are analysed in detail, namely DES, 3DES and AES algorithms. It is observed from many exiting works that in AMI of SGs, the 128 bit AES symmetric algorithm is efficient in smart meters and is used for communication between smart meters and data accumulators because of its adequate security solutions. This is also because, in future, AES block sizes can even be stretched beyond 128,192 and 256 bit lengths for superior long-term security against brute force attacks aimed at metering infrastructure.

Moreover, it is also observed that, in terms of light weight memory capabilities of smart metering devices, the symmetric block ciphers like AES are best suitable for AMI of SGs, along with its computational speed when compared to the public key algorithms. The main challenges faced while implementing the encryption algorithms are identified as key management

issues and key protection policies. Lightweight KMS solutions are most suited for the metering infrastructure of SGs because of their low-memory and low-computational overheads. The successful implementation of encryption algorithms is achievable through the standards specified by NIST guidelines.

References

[1] "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0", Report number: (NIST-SP-1108r3), National Institute of Standards and Technology, 2014.

[2] Available online : https://www.webopedia.com/TERM/E/encryption_algorithm.html

[3] Alfred, J. Menezes., Paul, C. Van, Oorschot., Scott, A. Vanstone., "A Handbook of Applied Cryptography", Jaypee medical; 1st edition ,1996.

[4] Gurpreet, Singh., Supriya, Kinger., "A study of encryption algorithms for Information security", International Journal of Computer Applications, Vol.67, no.19, pp.33-38, 2013.

[5] William Stallimgs, Cryptography and Network Security, Principles and Practices, 2007, Available online : http://uru.ac.in/uruonlinelibrary/Cyber_Security/Cryptography_and_Network_Security.pdf

[6] Rajdeep, Bhanot., Rahul, Hans., "A Review and Comparative Analysis of Various Encryption Algorithms", International Journal of Security and Its Applications, Vol.9, no.4, pp.289-306, 2015.

[7] Sanket, Desai., Rabei, Alhadad., Naveen, Chilamkurti., Abdun, Mahmood., "A survey of privacy preserving schemes in IoE enabled Smart Grid Advanced Metering Infrastructure", Cluster Computing, Vol.22, pp.43–69, 2019.

[8] Jing, Xu, Zhilei,Yao., "Advanced Metering Infrastructure Security Issues and its Solution: A Review", International Journal of Innovative Research in Computer and Communication Engineering, Vol.3, no.11, pp.11501-11507, 2015.

[9] Ajay Kumar, Alpana Agarwal, "Research Issues Related to Cryptography Algorithms and Key Generation for Smart Grid: A Survey", 7th India International Conference on Power Electronics(IICPE), 2016.

[10]Available online : https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm

[11] Available online : https://www.comparitech.com/blog /information-security/what-is-aes-encryption/

[12] Jose, Manuel, Ortega., "Mastering Python for Network and Security", Packt, Publishing, 2018.

[13] Philani, Khumalo., et al., "A Secured Smart Grid Network for Advanced Metering Infrastructure", Smart Grid conference, 2016

[14] Muhammad, Faheem, Mushtaq., Sapiee, Jamel., Abdulkadir, Hassan. Disina., Zahraddeen, A. Pindar., Nur, Shafinaz, Ahmad, Shakir, Mustafa, Mat, Deris., "A Survey on the Cryptographic Encryption Algorithms", International Journal of Advanced Computer Science and Applications, Vol.8, no.11, pp.333-344, 2017.

[15] S. Ahmad., K. M. R. Alam., H. Rahman., S. Tamura., "A comparison between symmetric and asymmetric key encryption algorithm based decryption mixnets", IEEE International Conference on Networking Systems and Security, 2015.

[16] "Smart Grid Cryptographic Key Management", Scalable cryptographic key management to secure data and communications for millions of smart devices in the energy sector, 2012. Available online : https://www.energy.gov/sites/prod/files/2017/04/f34/Sypris_Smart%20Grid%20Cryptographic%20Key%20Management_FactSheet.pdf

[17] Fadi, Aloul., A. R. Al-Ali., Rami, Al-Dalky., Mamoun, Al-Mardini., Wassim, El-Hajj., "Smart Grid Security: Threats, Vulnerabilities and Solutions", International Journal of Smart Grid and Clean Energy, Vol.1, no.1, pp.1-6, 2012.

[18] Vandana, Milind, Rohokale., Ramjee, Prasad., "Cyber Security for Smart Grid - The Backbone of Social Economy", Journal of Cyber Security Mobility, Vol.5, no.1, pp. 55–76, 2016.

[19] Vanga, Odelu., Ashok, Kumar, Das., Mohammad, Wazid., Mauro, Conti., "Provably Secure Authenticated Key Agreement Scheme for Smart Grid", IEEE Transactions on Smart Grid, Vol.9, no.3, pp.1900-1910, 2018.

[20] Longfei, Wei., Luis, Puche, Rondon., Amir, Moghadasi., Arif, I. Sarwat., "Review of Cyber-Physical Attacks and Counter Defense Mechanisms for Advanced Metering Infrastructure in Smart Grid", IEEE/PES Transmission and Distribution Conference and Exposition (T&D) , 2018.

[21] Sajjad, Hussain., Raja, Omman, Zafar., "Key Management Scheme and Cryptography in Smart Grid Elements", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 8, August 2015.

[22] Joan, Daemen., Vincent, Rijmen., "The Design of Rijndael", AES -The Advanced Encryption Standard, Information Security and Cryptography book series, 2001.

[23] Bashar, Alohali., Kashif, Kifayat., Qi, Shi., William, Hurst., "A Survey on Cryptography Key Management Schemes for Smart Grid", Journal of Computer Sciences and Applications, Vol.3, no.3A, pp.27-39, 2015.

[24] Nabeel, Mohamed., Zage, John., Kerr, Sam., Bertino, Elisa., Athula, Kulatunga., et al., "Cryptographic Key Management for Smart Power Grids", Cyber Center Technical Reports ,2012, Available online : https://www.embedded.com/cryptographic-key-management-for-smart-power-grids/

[25] Imtiaz, Parvez., Arif, I. Sarwat., My, T. Thai., Anurag, K. Srivastava., "A Novel Key Management and Data Encryption Method for Metering Infrastructure of Smart Grid", arXiv:1709.08505v1 [cs.MA] 2017.

[26] Xin, Zhou., Xiaofei, Tang., "Research and Implementation of RSA Algorithm for Encryption and Decryption", 6th International Forum on Strategic Technology, 2011.

[27] Available online : https://electricenergyonline.com/energy/magazine/ 297/article/Conquering-Advanced-Metering-Cost-and-Risk.htm

[28]Available online : https://academic.csuohio.edu/yuc/security/ Chapter_06_Data_Encription_Standard.pdf

[29] H. R. Nemati., L. Yang., "Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering", Information Science Reference, 2011.

[30] Elaine Barker William C. Barker, "Recommendation for Key Management: Part 2 – Best Practices for Key Management Organizations", NIST Special Publication 2019.

[31] Jingwei, Li., Chuan, Qin., Patrick, P. C. Lee., Jin. Li., "Rekeying for Encrypted Deduplication Storage", 46th Annual IEEE International Conference on Dependable Systems and Networks, 2016.

[32] Lili, Yan., Yan, Chang., Shibin, Zhang., "A lightweight authentication and key agreement scheme for smart grid", International Journal of Distributed Sensor Networks , Vol.13, no.2, 2017.

[33] Mourad, Benmalek., Yacine, Challal., Abdelouahid, Derhab., Abdelmadjid, Bouabdallah., "VerSAMI: Versatile and Scalable key management for Smart Grid AMI systems", Computer Networks, Vol.131,pp. 161-179, 2018.

[34] Qianqian, Wu., Meihong, Li., "A Lightweight Authentication Protocol for Smart Grid", IOP Conf. Series: Earth and Environmental Science, Vol. 234, 2019.

[35] FIPS 140-2, "Security Requirements for Cryptographic Modules", Information Technology Laboratory , National Institute of Standards and Technology, 2001.

[36] "Ciphers in Use in the Internet - Internet Research Task Force", D. McGrew, Chinese Academy of Science, 2012, Available online: https://tools.ietf.org/id/draft-irtf-cfrg-cipher-catalog-01.html

[37] Derived Test Requirements for FIPS PUB 140-2, "Security Requirements for Cryptographic Modules", Computer Security Division Information Technology Laboratory, National Institute of Standards and Technology, 2011.

[38] Available online :https://info.townsendsecurity.com/ definitive-guide-to-encryption-key-management-fundamentals

[39] Fatemeh, Halim., Salman, Yussof., Mohd. Ezanee, Rusli,, "Cyber Security Issues in Smart Meter and Their Solutions", IJCSNS International Journal of Computer Science and Network Security, Vol.18 no.3,pp.99-109, 2018

[40] Lindah, Kotut., Luay, A. Wahsheh., "Survey of Cyber Security Challenges and Solutions in Smart Grids", Cybersecurity Symposium,IEEE, 2016.

[41] Nithin, George., Nithin, S., Sasi, K. Kottayil., "Hybrid Key Management Scheme For Secure AMI Communication", 6th International Conference On Advances In Computing & Communications ICACC, Vol.93, pp.862-869, 2016.

[42] Mourad, Benmalek., Yacine, Challal., Abdelmadjid, Bouabdallah., "Scalable multi-group key management for Advanced Metering Infrastructure", International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing , 2015.

[43] Nian, Liu., Jinshan, Chen., Lin, Zhu., Jianhua, Zhang., Yanling, He., "A Key Management Scheme for Secure Communications of Advanced Metering Infrastructure in Smart Grid", IEEE Transactions on Industrial Electronics, Vol.60, no.10, pp.4746-4756, 2013.

[44] Imtiaz, Parvez., Arif, I. Sarwat , A., MY.T. Thai., Anurag K. Srivastava, "A Novel Key Management and Data Encryption Method for Metering Infrastructure of Grid", IEEE Transactions On Industrial Electronics, Vol. 60, No. 10,2013.

[45] Amin, Mohammadali., Mohammad, Sayad, Haghighi., Mohammad, Hesam, Tadayon., Alireza, Mohammadi, Nodooshan., "A Novel Identity-based Key Establishment Method for Advanced Metering Infrastructure in Smart Grid", IEEE Transactions on Smart Grid, Vol.9, no.4, pp.2834-2842, 2016.

[46] Lincoln, Kamau, Kiarie., Philip, Kibet, Langat., Christopher, Maina, Muriithi., "Application of Spritz Encryption in Smart Meters to Protect Consumer Data", Journal of Computer Networks and Communications, Vol. 2019, 2019.

[47] Dariush, Abbasinezhad-Mood., Morteza, Nikooghadam., "Efficient Anonymous Password-Authenticated Key Exchange Protocol to Read Isolated Smart Meters by Utilization of Extended Chebyshev Chaotic Maps", IEEE Transactions on Industrial Informatics, Vol.14, no.11, pp.4815-4828, 2018.

[48] K. Sha., N. Alatrash., Z. Wang., "A secure and efficient framework to read isolated smart grid devices", IEEE Trans. Smart Grid, Vol.8, no.6, pp.2519–2531, 2017.

[49] Iraklis, Leontiadis., Refik, Molva., Melek, O¨nen., "Privacy Preserving Statistics in the Smart Grid", 34th International Conference on Distributed Computing Systems Workshops, 2014.

[50] Samer Khasawneh & Michel Kadoch, “Hybrid Cryptography Algorithm with Precomputation for Advanced Metering Infrastructure Networks”, Mobile Networks and Applications, Vol.23, pp.982-993, 2018
[51] Nabeel, M., Ding, X., Seo, S. H., Bertino, E., “Scalable end-to-end security for advanced metering infrastructures”, Information Systems, Vol.53, pp.213–223, 2015.
[52] Mahmood. K,, Chaudhry, S. A., Naqvi, H., Shon, T., Ahmad, H.F., “A lightweight message authentication scheme for smart grid communications in power sector”, Computers and Electrical Engineering, Vol.52, pp.114–124, 2016.
[53] N. Busom., R. Petrlic., F. Seb´e., C. Sorge., M. Valls., “Efficient smart metering based on homomorphic Encryption”, Computer Communications, Vol.82, pp.95-101, 2015.
[54] Garcia, F. and Jacobs, B., “Privacy friendly energy metering via homomorphic encryption”, International Workshop on security and Trust Management, pp.226-238, 2011.
[55] Jalaja, Valisireddy., Anjaneyulu, G.S.G.N., “Adept smart meters using homomorphic encryption based on factor problem over groups”, Information and Learning Science, Vol.119, no.4, 2018.
[56] Jong-Hyuk, Im., Hee-Yong, Kwon., Seong-Yun, Jeon., Mun-Kyu, Lee., “Privacy-Preserving Electricity Billing System Using Functional Encryption”, Energies, Vol.12, 2019.
[57] Shakir M. Hussain, Hussein Al-Bahadili, Hadi Al-Saadi, “A DNA-Based Smart Meter Authentication Scheme”, 2nd International Conference on the Applications of Information Technology in Developing Renewable Energy Processes & Systems (IT-DREPS),2017.
[58] Chunqiang, Hu., Jiguo, Yu., Xiuzhen, Cheng., Zhi, Tian., Kemal, Akkaya., Limin, Sun., “An attribute based signcryption scheme to secure multicast communications in smart grids”, American Institute of Mathematical Sciences, Vol.1, no.1, pp.77-100, 2018.
[59] “Security for smart meters in a fast-changing energy marketplace”, Enexis / Atos, 2014.
[60] SafeNet ProtectApp Application-level encryption and key management, Thales GH. v11 2019.
[61] Hüseyin, Bodur., Resul, Kara., “Secure SMS Encryption Using RSA Encryption Algorithm on Android Message Application”, 3rd International Symposium on Innovative Technologies in Engineering and Science, 2016.
[62] Tianqi, Zhou., Jian, Shen., Xiong, Li., Chen, Wang., Jun, Shen., “Quantum Cryptography for the Future Internet and the Security Analysis”, Hindawi Security and Communication Networks, Vol. 2018, 2018
[63] Claudia, Pop., Marcel, Antal., Tudor, Cioara., Ionut, Anghel., David, Sera., Ioan, Salomie., Giuseppe, Raveduto., Denisa, Ziu., Vincenzo, Croce., Massimo, Bertoncini., “Blockchain-Based Scalable and Tamper-Evident Solution for Registering Energy Data”, Sensors, Vol.19, no.14, 2019.

Biographies

Anita Philips, Ph.D Scholar, Dept. of Electrical & Electronics, Karunya University, Coimbatore Tamil Nadu. India.

J. Jayakumar, Professor, Dept. of Electrical & Electronics, Karunya University, Coimbatore Tamil Nadu. India.