International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 07, July-2021

Cryptographic and Key Management Approach for Cybersecurity in Smart Grid

Avradipta Das
[6th] Semester Student in Department of Computer Science and Engineering,
JSS Science and Technology University,
Mysuru, India

***Abstract*:- Power grids are increasingly managed and controlled with the aid of automation initiatives by power utilities by deploying high speed data communication networks. All the constituent electricity organisations are expected to exchange control data for perfect protocol in securing the grids from cascaded failures. Hitherto, it used to be a daunting task in conventional grids to precisely locate and distinguish the root cause of the grid failure from the cascaded effect that it triggers. Unless the data and event loggers are compliant with micro-second response time accuracy the chronology of the events cannot be journaled. Although the utilities stand to gain a lot by deploying ICT interventions along with GPS facilities, in precisely controlling the grid, it simultaneously opens the gates to the unscrupulous hackers to launch attacks, if the so called smart grids are not secured enough from cyber threats. Thus securing an ICT enabled smart Grids throws challenges and assumes paramount importance too, in searching for formidable data security solutions thereof. This is an endeavour to propose a Cryptographic and Key Management Approach for securing Data in the context of prevailing Cyber Security threats and challenges in Smart Grids.**

Keywords: Cybersecurity, Smart Grid, Cryptography, Network

I. INTRODUCTION

Power System is one of the most complex, real time based demanding electrical network. Power is injected into the complex electrical network at various geographical locations (Power Sources) and Power is consumed at numerous demand points (Power Loads). Load Dispatcher does the intricate and spontaneous Power System balancing act to ensure Power Grid health round the clock. The dynamic Power Grid behaviour is required to be dealt with almost instantly when need arises. Assortment of Power Sources makes it all the more difficult to manage. The extent of generation fluctuation over conventional energy sources is too high compared to stable power sources viz., Thermal or Hydel. A typical power grid comprises of Sub Stations and Power Lines built on electrical infrastructure viz., towers, Cables, transformers, breakers, isolators, bays, metering infrastructure, protection infrastructure etc., to provide economy with near-uninterrupted quality power supply. Such a conventional system is predominantly a pure electrical system sans Information and Communication technology (ICT) associated with it. As the Economies are fast developing, had their impact in the form of insatiable hunger electrical power. It is necessary that we make conventional electrical grids into ICT based smart grids, the ones for more reliable and efficient [1] operation. In a developing economy the demand for power outreaches the supply. The demand is not only high but also fluctuating. We could rely on renewable resources like solar energy and wind energy to meet the present need to some extent, but unfortunately, these power sources suffer from the phenomena called intermittency. Shortcomings of the prevailing convention electrical grids are mitigated by transforming them into smart grids. High speed two-way communication backbone used in the conventional grids coupled with computational intelligence converts the system into smarter one.

The power customers are expected to participate in power generation and injection into the supply grid so as to use the available resources in an optimal manner. Huge generation capacity from the customers at large can augment the power shortages faced by the utilities to ensure smooth Load-Curve. They have to change from being passive consumers to being active consumers [1]. Such proactive customers viz., prosumers, can benefit too, in effectively reducing utility bills by installing Roof-Top Solar Panels, EVs etc. This situation is bound open the enterprise network, though to a limited extend is bound to throw Cyber Security challenges. The Metering projects, for instance, include intricate networking strategies include Canopy networking, mesh technologies etc. This can be a source of breach in connectivity. If the Customer end electrical devices, be it domestic or commercial in nature, have to be controlled by the Utilities for Demand-Response purpose or to pass on Time-Of-The-Day benefits to the end customer. These potential sources of Cyber-attacks too. The communication back bone cannot be strictly an intranet. As the customer participation increases by the day the last mile connectivity through internet increases too. Usage of internet to meet the set objectives of the business is a potential threat for the Utilities.

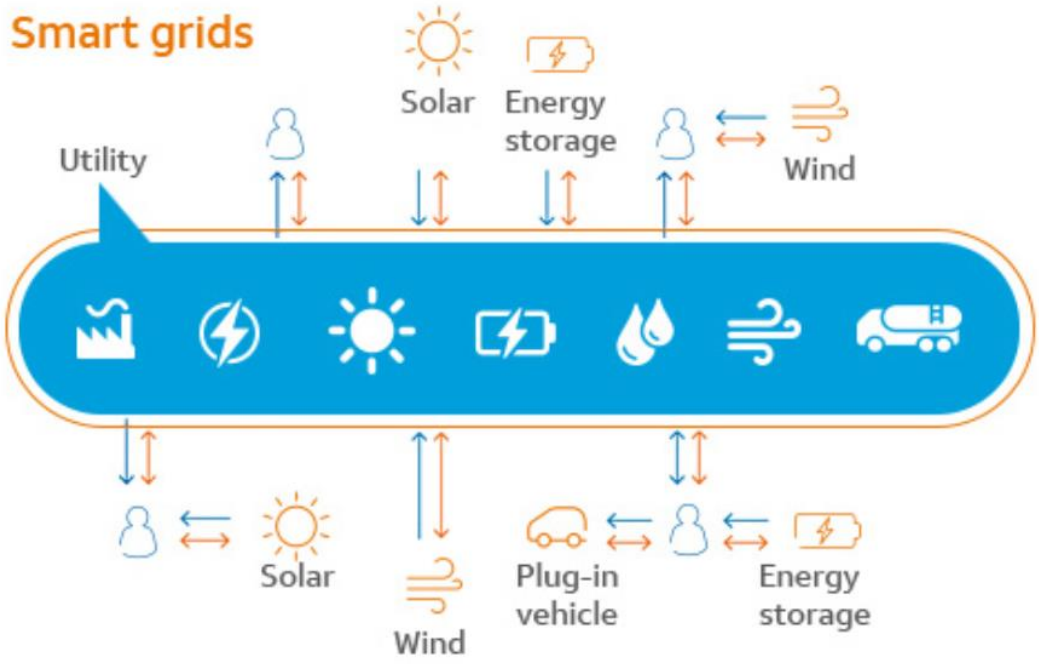
Smart Grids are imminent and without which it would be impossible to manage and control modern ways of power generation, transmission and distribution. Text book protection systems between Transmission and Distribution systems are possible only through smart grids. Renewable Energy Integration is simply not possible without the advent of Smart Grids.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 07, July-2021

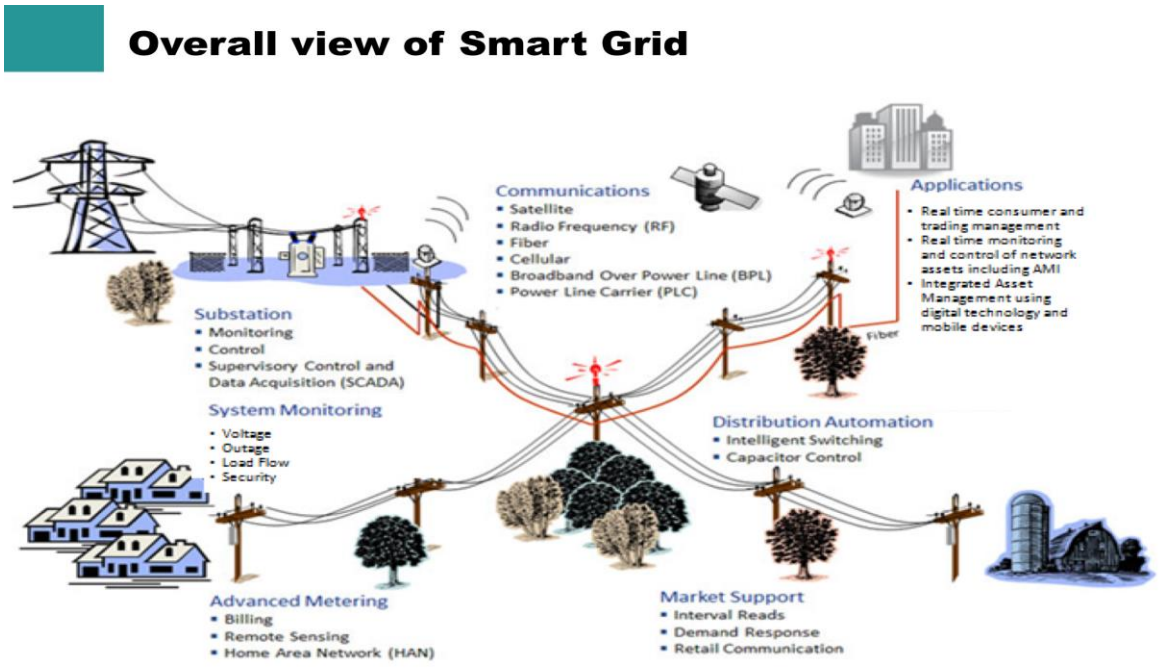
The Cyber Security Solutions have to aim at completely eliminating the possibility of the hacker taking control of the electrical grids under any circumstances. Power being the essential ingredient in any Economy, securing grids from attacks becomes imperative.

Cryptography is an obvious tool in establishing secured end to end communication by comprehensively nullifying Man-In-The-Middle phenomena. National Institute of Standards and Technology (NIST) is a formidable source for cryptographic methods in order to mitigate cyber threats. An endeavour is made to study smart grid security in greater detail in this paper. The goal of this paper is to cover the security challenges related to cyber security, and also study how cryptography and key management are used in order to eliminate cyber-attacks.

II. SMART GRID ARCHITECTURE

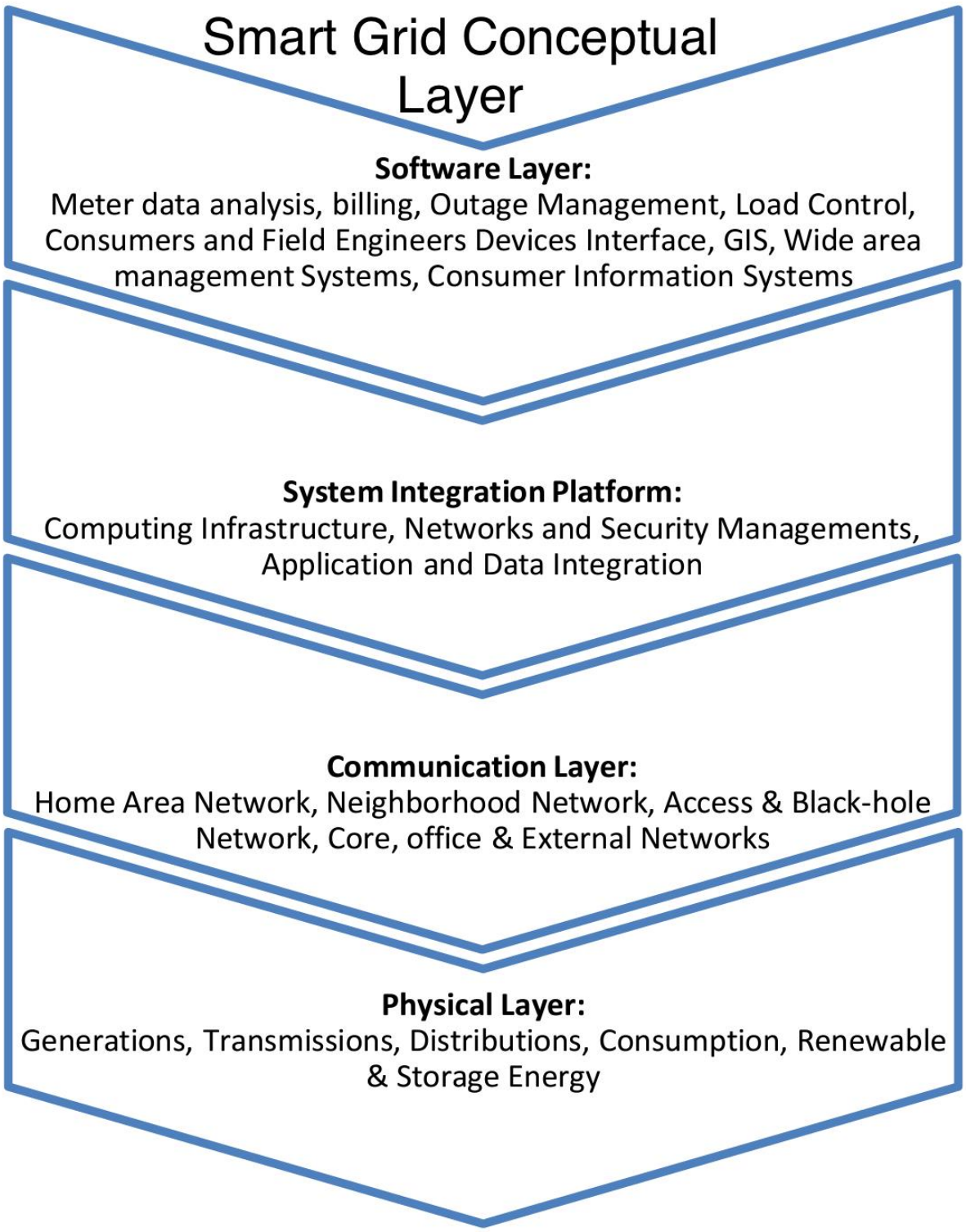


Pic-1 Smart grids



Pic-2 Overall View of Smart Grid

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 07, July-2021



Pic-3 Smart Grid Conceptual Layer

III. SECURITY REQUIREMENTS AND OBJECTIVES OF SMART GRID

Smart Grid is essentially two way ICT applied on conventional electrical grid. The grid parameters have to be necessarily logged in real time using sensory equipment suitably installed at all the control touch points of the conventional electrical grid. As such ICT implementation leads to installation of RTUs, motorised control systems connected to underlying ICT to achieve operational protection to the grid on the fly. Time sensitivity is achieved by time synchronising all the electrical and IT devices through GPS installation. As the high speed communication backbone is quick enough to give near real-time capability to the smart Grid.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 07, July-2021

Smart Grid gathers grid parameters data, status data of control devices, metering data on demand or periodically. In addition the backbone is used to send command-control data by uniquely addressing the electrical devices for desired operation. That is, Supervisory Control and Data Acquisition (SCADA) is truly achieved apart from possessing grid intelligence for possible self-healing like operations. Metering System can furnish Load Survey data and instantaneous data on query to the servers for drawing trending details and conclusions thereof. GIS tools give geographical presentation of the grid apart from grid computing. All the grid components need to be GIS-mapped and loaded in the server for applying the GIS tools.

Thus the two types of smart grid data viz., operational data and grid control data flow through the communication backbone. Control data is particularly vulnerable from the point of view of grid health. Hackers gaining smart grid control can trip the grids irrationally by abusing the control data. This paper focuses on such Cyber threats and proposes strategy/approach to mitigate risks thereof.

The security requirements and objectives in the smart grid are:

- ***Availability***: Denial of Service (DoS) attacks make the resources and system services unavailable. The very purpose of the smart grid is to ensure availability of the information in a timely manner to right people / system automation elements, so that power delivery is not affected because of denial of access to authorised individuals.

- ***Integrity***: Illegitimate users' unauthorised modification of information or system is prevented to maintain integrity. Loss of integrity in smart grid by tampered smart meters, manipulated sensors can cause serious issues in power management.

- ***Confidentiality***: To protect the safety and privacy of the grid participants such as customers, prevention of unauthorised access to grid information is important. Smart grid network has a flow of very sensitive information such as customers power utilisation, behavioural data like sleeping time, availability at home and electronic gadgets utilisation , if accessed by unauthorised attacker can have serious repercussions.

- ***Authentication***: Validating the true identity of the grid participants. A failure in authenticating humans and devices involved can enable an attacker getting undesired access to control devices and private information resulting havocs.
- ***Authorisation***: Access control for providing permission and giving access to a system or information. It is essential to pave way for effective management of information as well as resources considering the wide range of devices used in a smart grid network apart from assortment of legitimate users participate in grid use/operation.

- ***Non-Repudiation***: Assurance that an action performed by a system or user are conclusively established in an undeniable manner. Since valuable resources and information are involved in a smart grid network Non-Repudiation is a major issue.

IV. Security challenges in Smart Grids

Vulnerability of smart grid security is very high because of various threats and challenges. Some of the cyber security challenges in smart grid are addressed below.

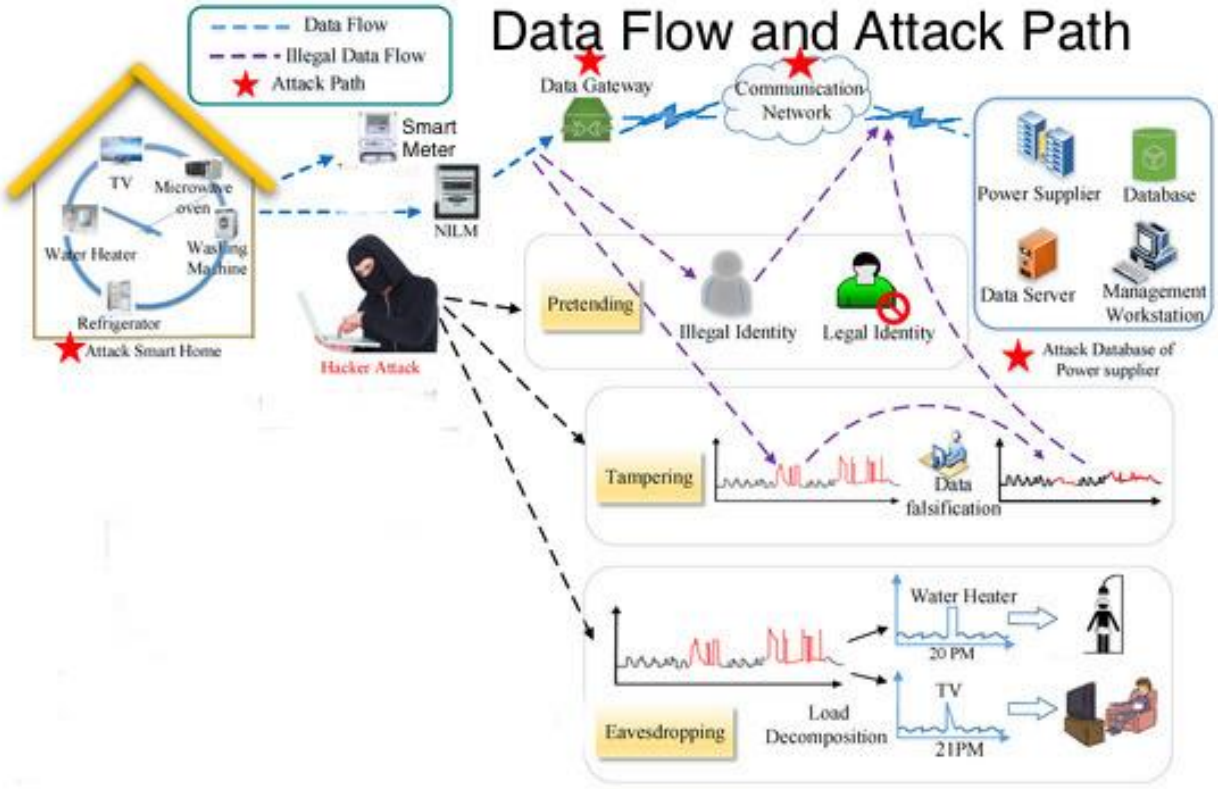
Connectivity*:* Because of number of devices and interoperability among these the communication network in smart grid is complex and sophisticated. Environment being a decentralised one, high level of protection against vulnerabilities and attacks is needed. Attacks can cause blackouts, infrastructural damages and increase frequency as well as duration of power interruption apart from potential safety hazards, as the attackers are likely gain control of the system [14].

Trust*:* Due to questionable trustworthiness of the customers at large in a participative smart grid, the design decisions are highly affected in the light of huge number of nodes connected in the smart grid network. Consumers may resort to deliberate violation of agreements, procedures and policies like tampering the smart meter for falsifying consumption data.

Privacy of Customers*:* Like any other public systems, it is essential to maintain privacy of the customers' data in smart grid which need to be well protected and preserved. Smart meters in Advanced Metering Infrastructure (AMI) while collecting various essential power consumption information of the customers, these can compromise the privacy of the customers' data leading to severe penal provisions. The information collected at Service provider end can lead to behavioral analysis of the customer household like availability of people in the house, when householders are travelling, sleeping time and timing of use of electronic gadgets and other appliances in the house. These can be used by many like criminals for robbery, marketers for selling products and terrorists for attacks. In order to maintain customer-privacy data must be securely transmitted, stored and access must be secured and authenticated [15]. Even within the utility data access needs to be layered and confined to role based access mechanism.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 07, July-2021

Software Vulnerabilities: Software is vulnerable to many threats including malware. Supervisory control and data acquisition (SCADA) system components being general purpose technology, introduces the hazard of malicious and malware updates. Also general purpose systems often have many vulnerabilities which are patched from time to time to update the system. But such patching is very expensive and causes increased amount of downtime in time critical system like smart grid [14].



Pic-4 Data Flow and Attack Path [25]

V. SMART GRID SECURITY SOLUTIONS

The sheer enormity of the smart grids having ICT-enabled, emphasises how critical it is to secure it firmly from Cyber-attacks. Thus it takes center stage focus by both Industry experts and academicians. As the smart grid itself described as journey, the associated Cyber Security also takes cycles of refinement and strengthening. As such there is no assurance of cent per cent security. The Key aspects and methods that address Cyber Security are detailed hereunder.

A. Network Security

With Denial of Service (DoS) attack by the intruders, the intended services of the server are stalled. DoS attack detection and mitigation thereof, by following established techniques forms part of the solution strategy [16].

B. Data Security

Quite often smart grid networks are secured by protecting data and authenticating objects. Encrypted data using cryptography methods and algorithms are used to secure communication, protect user data and authenticate user access to prevent attack against data integrity.

While encrypting both Public Key and Symmetric Key encryption are very effective to secure smart grids. It is established that public key is far easier to implement when it comes to key management and more secured even though symmetric key needs less computing capabilities. However, because of different computational capabilities of varied devices from sensors, PC, Mobile phones to controllers in the smart grid network, both symmetric and public key methods are used. Selection of the type of encryption to be used in different parts of smart grid network depends upon criticality, time constraints and computational capability.

For authentication, the requirements to be met [14] are high efficiency, tolerance to faults and attacks and multicast support etc. Among these requirements support for multicast, compared to unicast/broadcast, is one of the most important requirement in smart grid. Because smart grid network involves power generation, transmission, distribution, monitoring and control, multicast provides the means for smart delivery of mass messages like those needing delivery of power to certain targeted load or fast operation of a circuit breaker.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 07, July-2021

Multicast applications authentication can be done using one of the following methods:

Secret-info asymmetry:
Each transmitter with the use of a specific key gets authenticated at each receiver. Through multicast the transmitter sends a message created with appended authentication keys of all receivers. However this increases the overhead of the system. As the size of the network grows, the throughput keeps on decreasing due to increasing number of keys required, as the authentication data is considered as redundant data.

Time asymmetry:
First the transmitter sends message and then creates authentication temporary keys which are sent once received by the receivers. This makes the keys if sniffed by attacker unusable.

Hybrid asymmetry:
In this both the above two methods are used to create different temporary keys for every transmission.

C. Key Management
Key management is vital for encryption and authentication for securing a system. There are two categories in this as mentioned below.

Public Key Infrastructure (PKI): Using this technology security is ensured for establishing any communication by verifying true identity of the party by receiving a certificate from the certifying authority (CA).

Symmetric Key Management: It is used in symmetric cryptography which consists of key generation, key distribution, key storage and key update. This has advantage of speed and efficiency.

However, because of the complexity and criticality of smart grid and the differences in computing capabilities of smart grid components, new approaches were proposed to the key management issue [6]. The first step is to identify smart grid key requirements which include:

- Secure management: To provide confidentiality and integrity.
- Scalability: Since smart grid network is huge and large, number of objects that share keys and the distance they cover has to be taken care by the key management.
- Efficiency: Computation , storage, response time and communication
- Evolve-ability: Since the smart grid network consists of new cutting-edge technologies like IoT as well as legacy systems like SCADA, Key management protocols have to accommodate existing devices, as well as to evolve to accommodate emerging technologies.

D. Network Security Protocols
Smart grid security depends upon design and implementation of secured network protocol and architecture. Some of the existing smart grid systems use internet based protocols for secure communication like IPSec and TLS. Since classical data network requirements differ majorly from smart grid network needs , many smart grids use protocols and standards which are appropriate and relevant like protocols used for communication between sensors and RTUs. On the other hand communication of data from sensors to application layer are done using Data Aggregators which need a set of protocols considering security requirements and overheads.
Smart grid networks are built using one of the following two architectures for security [6]:

- *Trust computing-based architecture*: Where the task of authenticating objects is distributed throughout the system, and all objects participate in authenticating each other by assigning trust levels.

- *Role-based network architecture*: Where a network is divided to sub-domains and each domain has a number of devices that take on certain roles and privileges.

E. Compliance Checks
To ensure whether configurations of each component in the system are meeting highest level of secure mitigation and protection standards or not compliance checks are done continuously using vulnerability analysis using automated tools like penetration and SQL injection tools. This is important for the fact that a fault in one component can cause huge security breach which in turn can create severe damage to infrastructure and can be life threatening at the same time.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 07, July-2021

VI. CRYPTOGRAPHIC AND KEY MANAGEMENT BASED SOLUTION

General Design Considerations

(i) Selection of cryptographic technique should be such that the design is robust and the algorithm is free of f laws.

(ii) Entropy issue can be resolved by seeding a deterministic random bit generator (RBG) before distribution or use a key derivation function which comes with the device.

(iii) Use of cryptographic modules that is used to protect the cryptographic algorithm. We need to upgrade these modules timely, since smart grid equipment would be used for around twenty years and also replacing them would be a costlier affair.

(iv) Failure in encryption systems may occur due to implementation errors, compositional failures, insecure algorithms, or insecure protocols. These categories should be taken into consideration while designing.

(v) Since a random number generator is an integral part of the security system, its failures would result in a compromise of cryptographic algorithm or protocol.

(vi)There must be alternatives for authentication and authorisation procedures in case we cannot connect to another system.

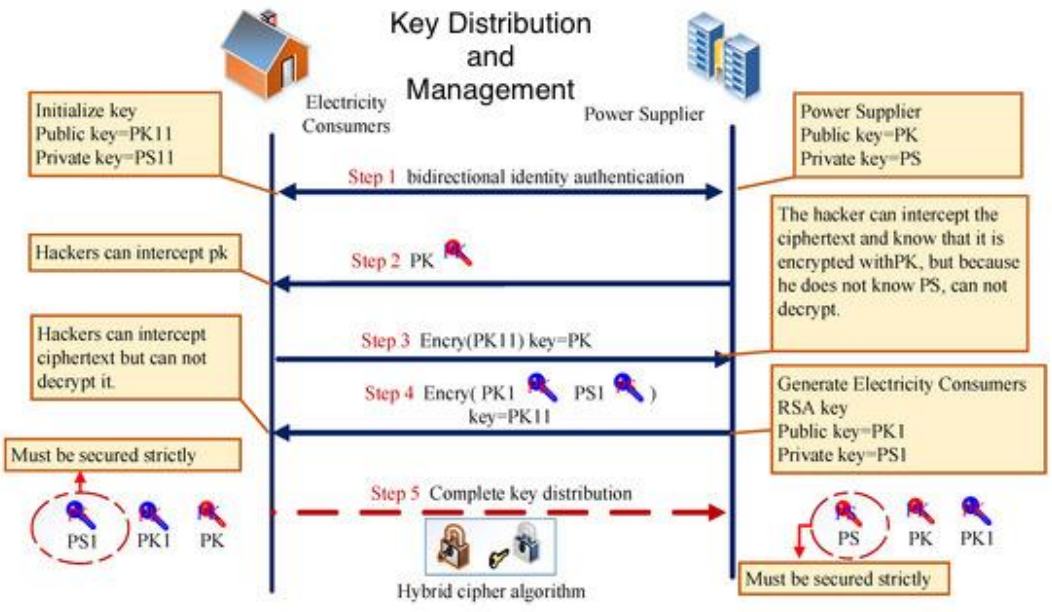
(vii) Availability must always be there since dropping or refusal to re-establish a connection may affect the critical communication.

(viii) The algorithms and key lengths should be such that the desired security strength is attained.
(ix) In order to maintain security of the keying materials and authentication data, we must protect it from unauthorised access or any device tampering. Physical security is required for this purpose.

Key Management

We use certificates that have validity, that is, certificates that have not expired. If this certificate is issued to a device, that is, no longer reliable, either lost or stolen, then the certificate can be revoked. A certificate revocation list is used for this purpose. A device that uses the information in a certificate is called relying party (RP). RP has a checklist that must be considered when accepting a certificate. The points that need to be checked are as follows

i. if the certificate was issued by a trusted CA,
ii. if certificate is still valid and not expired,
iii. certificate should be in an authoritative CRL,
iv. verification of the certificate subject and policy for which certificate is being used.



Pic-5 Key Distribution and Management [25]

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 07, July-2021

VII. APPLICABLE ALGORITHMS

i. Symmetric Key

Advanced encryption standards (AESs), triple data encryption algorithm (TDEA), or triple data encryption standard (TDES).

ii. Asymmetric Key

Digital signature standard (DSS), digital signature algorithm (DSA), RSA digital signature algorithm (RSA), elliptic curve digital signature algorithm (ECDSA).

iii. Hash Standard

Secure Hash Algorithm (SHA) and Message Digest Algorithm

iv.Key Management

SP800-108 KDF's

v. Deterministic Random Number Generators

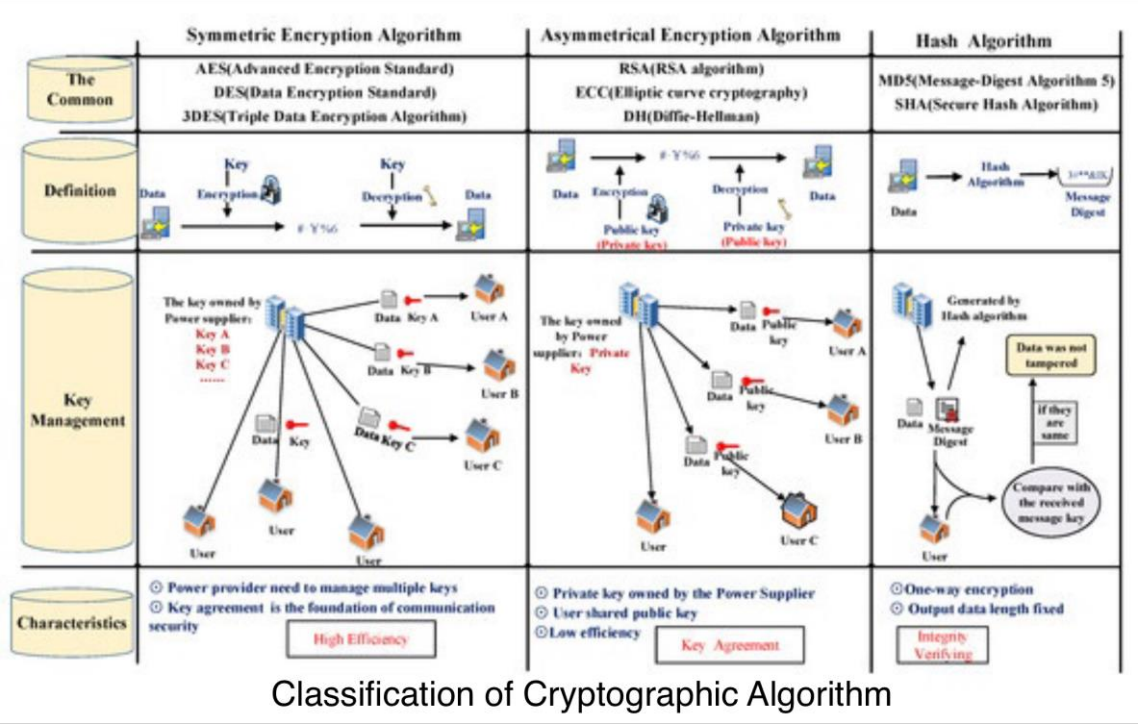
FIPS 186–2 APPENDIX 3.1 RNG, FIPS 186–2 APPENDIX 3.2 RNG, ANSI X9.31-1998 APPENDIX A2.4 RNG, ANSI X9.62-1998 ANNEX A.4 RNG, and ANSI X9.31 APPENDIX A.24 RNG using TDES and AES RNG,SP800-90 RNG.

vi.Symmetric Key Establishment Techniques

FIPS 140–2 1G D.2.

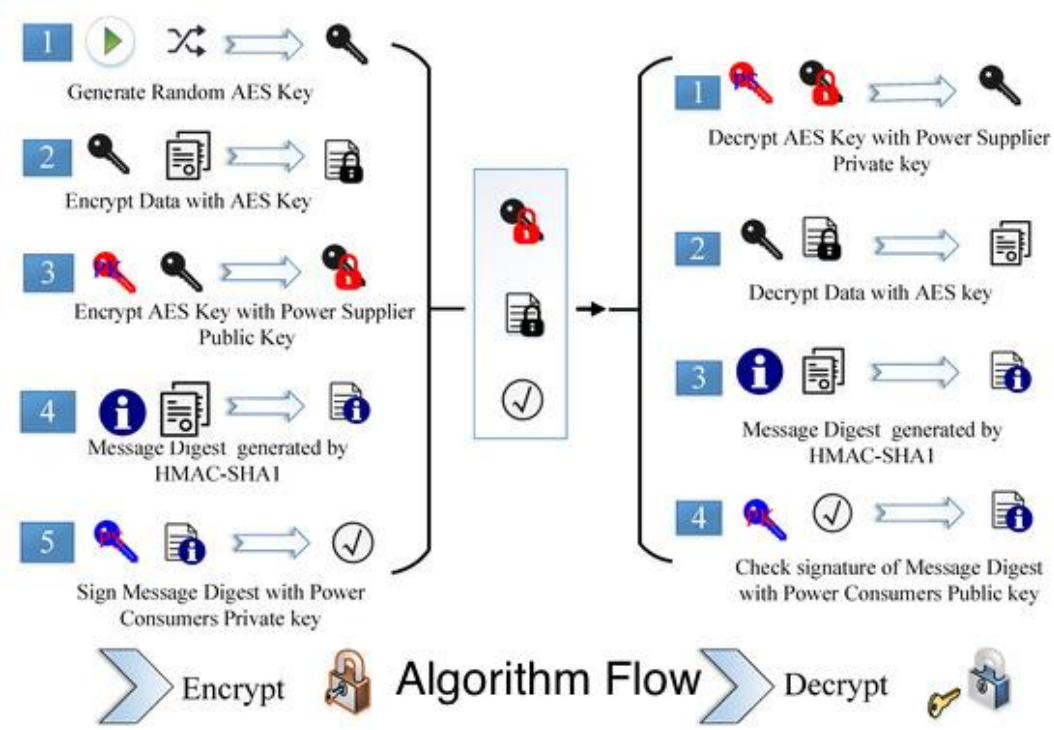
vii. Asymmetric Key Establishment Techniques

SP 800–56 A, SP 800–56 B, a

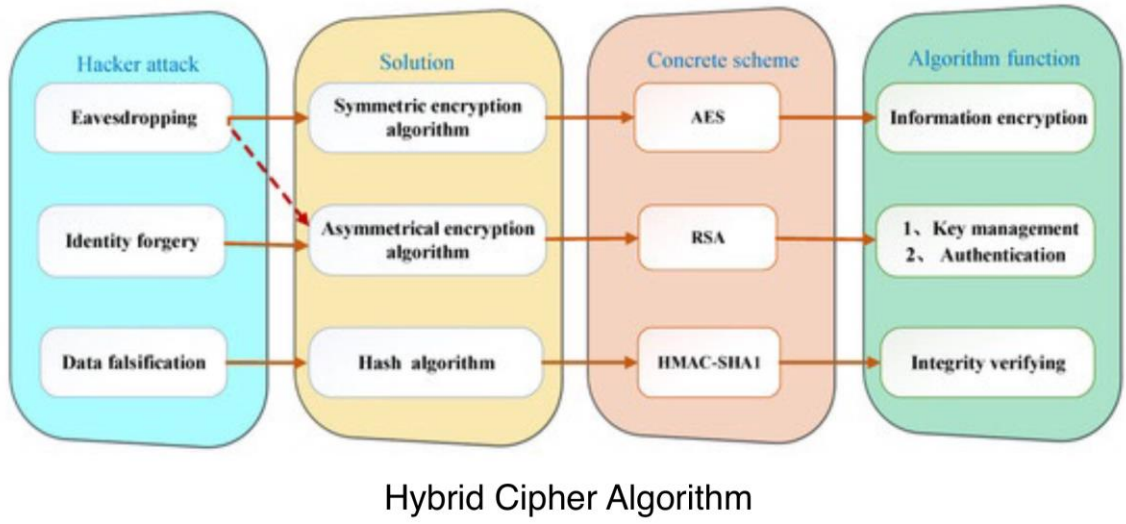


Pic-6 Classification of Cryptographic Algorithm [25]

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 07, July-2021



Pic-7 Algorithm Flow [25]



Pic-8 Hybrid Cipher Algorithm [25]

VIII. CONCLUSION

Numerous Smart grid centric cyber Security threats are focussed in this paper. Smart grid is a long drawn journey and is quite a complex concept. But a strategic of such a smart grid implementation through prioritisation and phasing is bound to deliver expected results. Cyber Security threats are both potential and real in the context of Smart Grid and the same have to be dealt with, in a comprehensive manner. Thus Cyber Security becomes integral part of DataCom network based smart Grids. Water-tight handshaking between otherwise independent electrical systems of different utilities is a daunting task. Further such devices increase along with increase in power demand, Suitable smart grid architecture in the context of the Cyber Security is detailed

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 07, July-2021

in one of the sections. Cryptographic and Key management techniques are also discussed in detail to mitigate the inherent Cyber Security threats. Constraints and limitations in Cryptography technique are covered along with possible mitigation approaches. Consumer data privacy is equally important security angle which is not covered in this paper. An effective Smart Grid can be realised by comprehensively treating every possible Cyber Security risk.

ACKNOWLEDGEMENT

I would like to thank Dr. Prasant K. Pattnaik (Professor, School of Computer Engineering, KIIT Deemed University, Bhubaneswar), Dr. D. Tukaram (Ex Professor , Department of Electrical Engineering, Indian Institute Of Science , Bangalore), Mr. Anant Rao (Ex Chief General Manager, Odisha Power Transmission Corporation Ltd.), Dr. A.K,Ojha (Associate Professor Indian Institute of Technology , Bhubaneswar) and Mr. Debashis Dash (Industry Leader Energy and Utility, IBM) for their guidance , help and inspiration for this paper.

REFERENCES

[1] NIST, Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security. http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf
[2] R. Apel, "Smart Grid Architecture Model: Methodology and Practical Application," in Workshop of Electrical Power Control Centers, 2013.
[3] H. Brown, S. Suryanarayanan, S. Natarajan, and S. Rajopadhye, "Improving Reliability of Islanded Distribution Systems With Distributed Renewable Energy Resources," IEEE Trans. on Smart Grid, 3(4), pp. 2028–2038, 2012.
[4] M. Miller, M. Johns, E. Sortomme, and S. Venkata, S. "Advanced integration of distributed energy resources" in Power and Energy Society General Meeting, pp. 1-2, July 2012.
[5] R. Morales Gonzalez, B. Asare-Bediako, J. Cobben, W. Kling, G. Scharrenberg, and D. Dijkstra, "Distributed energy resources for a zero-energy neighborhood," in 3rd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies, pp.1-8, 2012.
[6] W. Wang and Z. Lu, "Cyber Security in the Smart Grid: Survey and challenges," Computer Networks, 57(7), pp. 1344-1371, 2013.
[7] W. Wang, "A survey on the communication architectures in smart grid," Computer Networks, vol. 55, no. 15, pp. 3604-3629, 2011.
[8] G. F. Reed, P. A. Philip, A. Barchowsky and C. J. Lippert, "Sample survey of smart grid approaches and technology gap analysis," in Innovative Smart Grid Technologies Conference Europe, 2010.
[9] G. Garner, "Designing Last Mile Communications Infrastructures for Intelligent Utility Networks (Smart Grid)," IBM Intelligent Utility Network (IUN) Communication Services, 2010.
[10] Claudio Lima, "An Architecture for the Smart Grid," in IEEE P2030 Smart Grid Comm. Architecture SG1 ETSI Workshop, pp. 1-27, 2011.
[11] H. Naidua and K. Thanushkodib, "Recent Trends in SCADA Power Distribution Automation Systems," in Bangladesh Journal of Scientific and Industrial Research, 45(3), pp. 205-218, 2010.
[12] A. Rezai, P. Keshavarzi, and Z. Moravej, "Secure SCADA communication by using a modified key management scheme," ISA Transactions, 52(4), pp. 517-524, July 2013.
[13] E. Knapp and R. Samani, "Security Models for SCADA, ICS, and Smart Grid," in Applied Cyber Security and the Smart Grid, ch. 5, 2013.
[14] M. B. Line, I. A. Tondel and M. G. Jaatun, "Cyber security challenges in Smart Grids," in 2nd IEEE PES International Conference and Exhibition , Innovative Smart Grid Technologies (ISGT Europe), Manchester, 2011.
[15] H. Khurana, M. Hadley, L. Ning and D. A. Frincke, "Smart grid security issues," IEEE Security & Privacy, 7(1), pp. 81-85, 2010.
[16] NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3, Nat'l Institute of Standards and Technology, 2014.
[17] J.-H. Jun, D. Lee, C.-W. Ahn and S.-H. Kim, "DDoS Attack Detection Using Flow Entropy and Packet Sampling on Huge Networks," in the 13th International Conference on Networks, Nice, 2014.
[18] G. Meng and N. Wang, "A Network Intrusion Detection Method Based on Improved K-Means Algorithm," Advanced Science and Technology Letters, 53(1), pp. 429-433, 2014.
[19] S. Shin, S. Lee, H. Kim and S. Kim, "Advanced probabilistic approach for network intrusion forecasting and detection," Expert Systems with Applications, 40(1), pp. 315-322, 2013.
[20] D. Lin, "Network Intrusion Detection and Mitigation against Denial of Service Attack," WPE-II Report, Univ.of Pennsylvania, Apr. 2013.
[21] W. Xu, W. Trappe, Y. Zhang and T. Wood, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," in 6th ACM Int'l Symposium on Mobile Ad Hoc Networking and Computing, 2005.
[22] C. Popper, M. Strasser and S. Capkun, "Anti-Jamming Broadcast Communication using Uncoordinated Spread Spectrum Techniques," IEEE J. on Selected Areas in Comm., 28(5), pp. 703-715, 2010.
[23] E. K. Lee, M. Gerla and S. Y. Oh, "Physical Layer Security in Wireless Smart grid," IEEE Comm. Magazine, 50(8), pp. 46-52, 2012.
[24] M. Kammerstetter, "Architecture-Driven SMART GRID Security Management," in ACM Workshop on Information Hiding and Multimedia Security, 2014.
[25] Ruijue Feng , Zhidong Wang , Zhifeng Li , Haixia Ma , Ruiyuan Chen , Zhengbin Pu , Ziqiu Chen and Xianyu Zeng , "A Hybrid Cryptography Scheme for NILM Data Security", Published in MDPI on 10th July 2020.

-oOo-