An Efficient Technique for Smart Grid Communications using IBE-ECIES

Rishi Kushwah, Sini Shibu

Abstract— Smart Grid Communication is one of the best technique used for transmission of data from sender to receiver. But during the transmission of data security is important such that the data is secure against various attacks in the grid communication. Although in the existing work various parameters are implemented for grid communication with Dynamic Encryption technique [1] but the technique implemented needs further enhancements regarding encryption and security of such data. Hence an efficient technique is implemented for the security of data in grid communication using identity based encryption with elliptic curve integrated encryption scheme. The proposed scheme provides security against various attacks and provides less storage.

Index Terms— IBE, ECIES, Smart Grids, DSE, DER, DG.

1 INTRODUCTION

Smart grid implies network of computers and power infrastructure to manage the energy usage and analyze the usage by monitoring them. Energy producer in an area receives information from devices called collector devices [13]. The information is the usage information managed by operational centers of the producer. The usage information or the readings are shared with the help of internet or dial-up line. The billing and utilities are performed based on this reading. The device used for this purpose is termed as smart meter installed at each customer site. The meter is computerized capable of processor, communication and non-volatile storage.

Smart meters are capable of multiple software controls comprising of auto cut-off, alarms in case of problems etc. the meters can be interfaced with smart devices to control them. The control of the energy usage can easily be maintained, monitored and deployed through smart meters. These smart meters are applied over smart grid. Smart grid features these abilities to support customer energy usage. With the help of smart grid the economic condition of the customer and the grid can also be analyzed and enhanced. Energy farms can generate energy using various sources like solar panels, methane generators, wind mills and turbines etc. the excess energy then can be sell back to utility there by reducing the energy cost [13]. With the help of smart grid such type of cost elimination methods can be applied at larger level. Customers are able to manage their electrical energy consumption and making it effective [3]. The load data that depicts the details of energy consumption by customer is stored and collected in smart meters. Smart meters are capable of storing data related to customer, energy provider, billing details etc. This private data needs to be preserved from security vulnerabilities resulting in security of smart grid. The data may be in form of personal information daily activities, individual behaviors, etc. needs to be adopted for privacy preservation [8].This data is transferred through wireless communications to energy provider for analysis. The data is shared from different customers containing privacy information. This data need to be applied with some sort of security technique like key cryptography etc. for prevention from illegal use [2].

A smart grid is a modern electrical grid that uses information and communication technology to gather and act on informational data. For e.g. information about the behaviors of suppliers and consumers to improve the efficiency, reliability, economics, and sustainability of the production and distribution of energy. The transmission of this data by wired or wireless communication should be secured. Security features are the additional capabilities evolving in smart grid apart from substation and distribution automation. Smart grids with the help of smart devices are able to heal from various problems by themselves like blackouts etc. but for security of the smart grids a whole functional setup needs to be deployed [5]. Due to limitations some security techniques may not apply on Smart Grid wireless communication. The limitations are:

Low cost- for being cost effective smart devices used in smart grid compromises from storage, computational power and memory thereby limiting towards security algorithms etc.

Low-bandwidth: The communication channels in lower distribution and consumption grids are designed to transmit short message and require only low bandwidth.

Easy-maintenance: The wireless networks in SG should be flexible and easy to manage. It is impossible to hire multiple engineers to manage user’s encryption key sand change of battery.

The old conventional electric grids are needed to be upgraded for efficiency and reliability to prevent blackouts [12]. For upgradation dependency on distributed intelligence and broadband communication is of major importance resulting in concern for security. Security is a primary concern in Smart Grid due to transmission of pricing information and control actions via information network. The attacks may be in form of eavesdropping, information tampering and malicious control command which may harm Smart Grid operations. Unethical customers may modify their meter readings to change electric charge consumption. Users or hacker scan extract the behaviors of household consumption by eavesdropping communications of smart meters in smart grids. They may even try to disrupt the grids functioning and shut it down temporarily resulting in great loss for energy provider and other customers.

Some security can be applied with the help of wired communication using optical fiber for communication but wired communication is not feasible in home network to monitor devices with different interface and also while monitoring multiple parameters in grid wired system architecture is costly and complicated.

2 LITERATURE SURVEY

T. Liu et. al.[1] stated that information network in smart grid introduced many security problems. Although wireless communication in smart grids are cheaper, easier to deploy, shared and mobile but are vulnerable to security threats. They defined the concept of dynamic secret applied over wireless communication in smart grids for designing encryption schemes. They obtained their results by applying ZigBee protocol for wireless communication over a smart grid. The dynamic secret based encryption scheme (DSE) designed by them showed that transmission and packet loss was unpredictable and inevitable and the dynamic encryption key cannot be tracked. They reduced the complexity of scheme by retransmitting sequence to update dynamic encryption key which led to protection from eavesdropping. They developed a system to monitor the performance of DSE. The scheme proposed by them uses light weight encryption method and dynamically generates during normal communication [1].

C.Bekara et.al. [4] Presented that smart meters are essential for real time balance between energy consumption and its production. They remarked that metering infrastructure collects, stores, analyze and provide metering data from smart meters to the authorized center and also carries commands, requests, messages and software updates from the authorized center to the smart meters thus it requires security for deployment and functioning of smart grid. They provide some features to secure these meters by authentication, confidentiality, integrity services and by preserving the privacy of the customer equipped with smart meter to keep metering data, energy consumption data, billing data safe. They proposed ID based authentication protocol providing source authentication, non-repudiation services and data integrity. They provided authentication to prevent data modification and impersonation and key establishment to preserve customer’s privacy [4].

W. Wanget. al.[6] provided that smart grid are integration of high speed and reliable data communication networks managing power system. They proposed survey on communication architectures, network compositions, functions, technologies and challenges in power systems. They surveyed to find research problems in communication networks of smart grid. They observed their results as energy suppliers and customers located differently the proposed communication network assume a hybrid structure connecting all the suppliers and customers. They removed communication delay by correct message delivery in required time window by communication network. Communication reliability and security provisioned with the delay constraint and communication network panned effectively for performance in energy management [6].

Z. Md. Fadlullahet. al.[7]remarked that AMI of smart grid presented Machine 2 Machine market. They gave the idea that smart meters do not require human interference in analyzing power requirements and energy distribution. They proposed that different M2M gateways are required at different places for smart grid communication network. They described the infrastructure of smart grid and technologies to enable smart grid area communication. They used ZigBee protocol for M2M communication in smart grid environment. The described M2M communication in the smart grid takes place within the considered area network and the communications between other are network is for data forwarding. They presented a technique to improve the performance of the ZigBee based M2M communications in Smart Grid by incorporating intelligence in the smart meter [7].

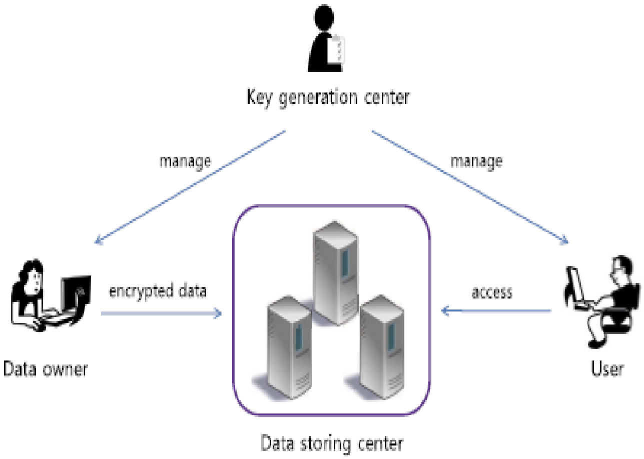
S. McLaughlin et.al. [9] Presented that AMI has brought revolution to electrical grids Intelligent AMI or smart meters report real time usage data for efficient energy generation its use. They stated that new devices vendors and device suppliers are being introduced into grids without understanding the security problems they may bring. They proposed archetypal attack tree approach for penetration testing of vendor’s technology class implementation. They proposed the strategy of grafting archetypal attack trees modeling broad adversary goals and attack vectors to vendor-specific concrete attack trees. These grafted trees are then evaluated and used for penetration testing for denial of energy fraud and service manipulation of energy usage data, spoofing meters and extracting sensitive data. They investigated technique that ensures security analysis and more consistent coverage of potential attacker goals and methods although government has provided guidelines for design and maintenance of AMI infrastructure security [9].

F.Rahimi et.al.[10] remarked that Demand response (DR), distributed energy storage (DES) and distributed generation (DG) are important part of smart grid referred as distributed energy resources (DER) and sometimes these resources are also referred as virtual power plant. They represented that DR resources are important elements for reliable and economic operation of the transmission system. They explored main industry drivers of smart grid and the facets of DER under the smart grid architecture and then concentrated on DR summarizing the existing and evolving programs and the product markets they can participate and concluded by addressing some of the challenges and potential solutions for implementation of DR [10].

G. N. Ericsson et.al. [11] Provoked that for effective electricity transmission in critical information infrastructure, cyber security and power system communications are essential. Power control systems with “openness” are vulnerable to cyber security threats. The proposed cyber security issues and highlighted access points in substation important for smart grid solutions. They gave a perspective of tying PSC and cyber security. They also described development of isolated islands of automation to integrated computer environment. They evident for the use of smart meters and introduction of wind power require smart grid system [11].

3 PROPOSED METHODOLOGY

Here CP-ABE attribute based data sharing technique is used which solves key escrow problem and proxy encryption. It provides an efficient technique of attribute based encryption which prevents from various attacks. Cost ineffective and chances of security is less.



Here in the Proposed work contains data owner, User, Data Storing center and key generation center. The data to be send is encrypted using the attribute policies to the data storing center which can be accessed by the user only after authenticated by the key generation center.

Although the various attribute based key generation are implemented which provides security from various attacks in the network and also the chances of overhead cost reduces, but further enhancements can be done related to the security of these attribute based policies.

The algorithm contains the following phases:

1. The sender generates an automated message and generates an identity string using message to be send.
2. The sender generates public key and private key from the identity and encrypts the message and makes tupple which contains identity and encrypted data and send to storage panel.
3. The owner when access the data needs to be authenticated at the storage panel using identity and password that is generated by the sender.
4. The owner after authenticates access the data based on identity and decrypts the message from the storage panel.

4 RESULT ANALYSIS

The table shown below is the analysis of number of keys generated depends on the number of packets and time taken to generate those keys. The analysis shows that the keys generate are same as the number of packets sends.

No. of Packets	Keys Generated	Time in ms
100	100	12.64
200	200	18.43
300	300	25.83
400	400	34.98
500	500	41.34
600	600	49.57
700	700	55.83
800	800	62.29
900	900	68.49
1000	1000	73.57

Table 1. Result Analysis of Proposed Work

The figure shown below is the total storage required for the 'n' number of packets to be sending.

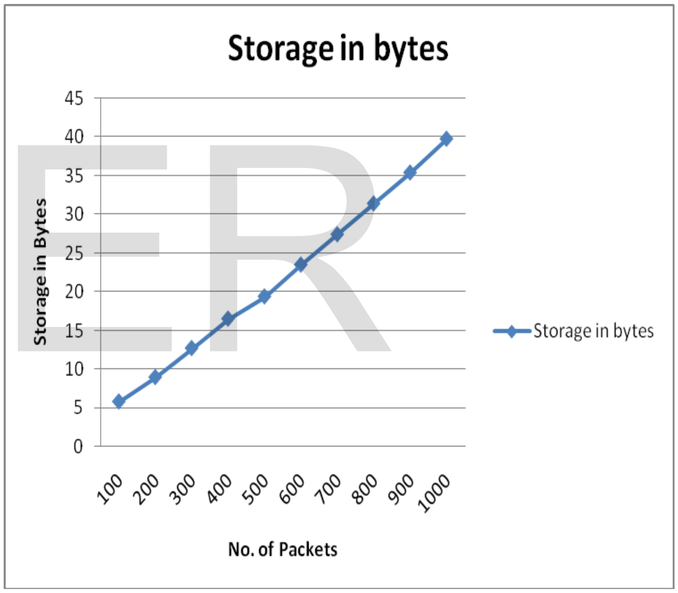


Figure 1. Storage required in Prposed Work

The table shown below is the storage in bytes versus the numner of packets to be send. The storage in bytes can be calculated using the storage required to store keys.

No. of Packets	Storage in bytes
100	5.7823
200	8.9345
300	12.6843
400	16.4855
500	19.3648
600	23.4685
700	27.3845
800	31.3749

900	35.3783
1000	39.7394

Table 2. Storage in bytes versus keys generated

The table shown below is the attack prevention by the proposed methodology from various attacks in the network grid communication.

S. No.	Attack Type	Security
1	Replay Attack	Yes
2	Identity Disclosure Attack	Yes
3	DOS attack	Yes
4	DDOS attack	Yes
5	Password Impersonation	Yes
6	Online dictionary	Yes
7	Offline dictionary	Yes

Table 3. Prevention from various attacks

5 CONCLUSION

The proposed technique implemented here provides less storage as shown in the analysis above. The technique also provides security against various attacks such as DOS attack, replay attack, identity disclosure attack. The Data communication in Smart Grid devices provides less packet loss ratio as compared to the other existing technique used for communication in grids.

REFERENCES

[1]Ting Liu, YangLiu,YashanMao,YaoSun,XiaohongGuan, Weibo Gong and ShengXiao "A Dynamic Secret-Based Encryption Scheme for Smart Grid Wireless Communication" IEEE-2013, IEEE Transactions on Smart Grid.

[2]Cheng-Kang Chu, Sherman S. M. Chow, Wen-GueyTzeng, Jianying Zhou and Robert H. Deng "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage", 2013

[3]Guoming Tang, Kui Wu, Jian Pei, Jiuyang Tang, Jingsheng Lei "Is My Electricity Bill Accurate? A Model-Driven Approach to Corrupted Load Data Identification" 2013

[4]ChakibBekara, Thomas Luckenbach and KheiraBekara "A Privacy Preserving and Secure Authentication Protocol for the Advanced Metering Infrastructure with Non-Repudiation Service", The Second International Conference on Smart Grids, Green Communications and IT Energy-aware Technologies, ISBN: 978-1-61208-189-2 , IARIA 2012.

[5]FaribaAalamifar "Viability of Powerline Communication for Smart Grid Realization", 2012

[6]Wenye Wang, Yi Xu, and MohitKhanna "A survey on the communication architectures in smart grid" Elsevier-2011, Science Direct Elsevier Pvt. Ltd.

[7]Zubair Md. Fadlullah, Mostafa M. Fouda, Nei Kato, Akira Takeuchi, Noboru Iwasaki and Yousuke Nozaki "Toward Intelligent Machine -to-Machine Communications in Smart Grid," IEEE Communications Magazine, vol. 49, no. 4, pp. 60-65, IEEE-2011.

[8]Depeng Li, ZeyarAung, SrinivasSampalli, John Williams and Abel Sanchez "Privacy Preservation for Smart Grid Multicast via Hybrid Group Key Scheme". 2011

[9]Stephen McLaughlin, Dmitry Podkuiko, Sergei Miadzvezhanka, Adam Delozier and Patrick McDaniel "Multi-vendor Penetration Testing in the Advanced Metering Infrastructure", ACSAC '10, ACM 978-1-4503-0133-6/10/12, ACM-2010.

[10]FarrokhRahimiand Ali Ipakchi "Demand Response as a Market Resource Under the Smart Grid Paradigm", IEEE Transactions on Smart Grid, Vol. 1, No. 1, IEEE- June 2010.

[11]Göran N. Ericsson "Cyber Security and Power System Communication—Essential Parts of a Smart Grid Infrastructure" IEEE Transactions on Power Delivery, Vol. 25, No. 3, IEEE- July 2010

[12]Anthony R. Metke and Randy L. Ekl "Security Technology for Smart Grid Networks", IEEE Transactions on Smart Grid, IEEE- June 2010.

[13]Patrick McDaniel and Sean W. Smith "Security and Privacy Challenges in the Smart Grid", Secure Systems, IEEE Computer and Reliability Societies, IEEE-2009.