Journal of Electrical Engineering and Automation (EEA) (2020)
Vol.02/ No. 03
Pages: 112-117
https://www.irojournals.com/iroeea
DOI: https://doi.org/10.36548/jeea.2020.3.001

Advanced Metering Infrastructure with Secure Chord Lookup Protocol for IoT Systems

Dr. P. Karrupusamy,
Professor and Head,
Department of Electrical and Electronics Engineering,
Shree Venkateshwara Hi-Tech Engineering College,
Erode, India.
Email: pkarrupusamy@ieee.org

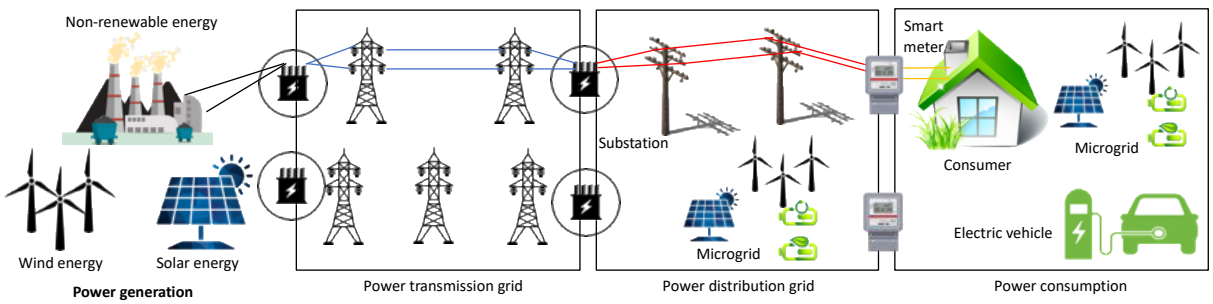
Abstract- The advanced metering infrastructure is enhanced in terms of system storage and latency using a secure chord lookup protocol scheme. Privacy of the subscriber and data security is maintained while reducing the memory consumption and data exchange duration using a protected multi-mode computation algorithm in the proposed model. Internet of things (IoT) based advanced metering networks can be greatly benefitted by this model. The production capacity is increased by 25% using the proposed model as per the simulated results, when compared to the existing systems. There is also over 50% reduction in the average data collection time and 15% reduction in the package delivery ratio. Lightweight authentication based secure mechanism is also provided to improve the safety of the model. When compared to the existing algorithms, the memory requirement and utilization of the proposed model is reduced by half.

Keywords: Data encryption, internet of things, advanced metering infrastructure, secure communication, secure chord lookup protocol, smart meter;

1. Introduction

Scientists and engineers from various industries are focused towards developing optimal communication systems for internet of things (IoT) based smart grid systems that use advanced metering infrastructure [1]. Reduction of environmental pollution and efficient management of subscriber energy demand requires reliable and safe smart grid networks. The measured data must be kept secure while the subscriber privacy has to be maintained in order to overcome the security issues. These factors make it a serious challenge to create security algorithms [2]. The energy distribution centre has to authenticate the encrypted data in these algorithms before performing any further action. It is also essential to separate the actual and malicious information. At the consumer end, smart meters, transmission and distribution systems are deployed along with electronic devices and smart sensors that make the smart grid [3]. Electronic data detection and collection is performed with the help of smart meters and advanced metering infrastructure for obtaining information regarding power consumption in the smart grid networks.

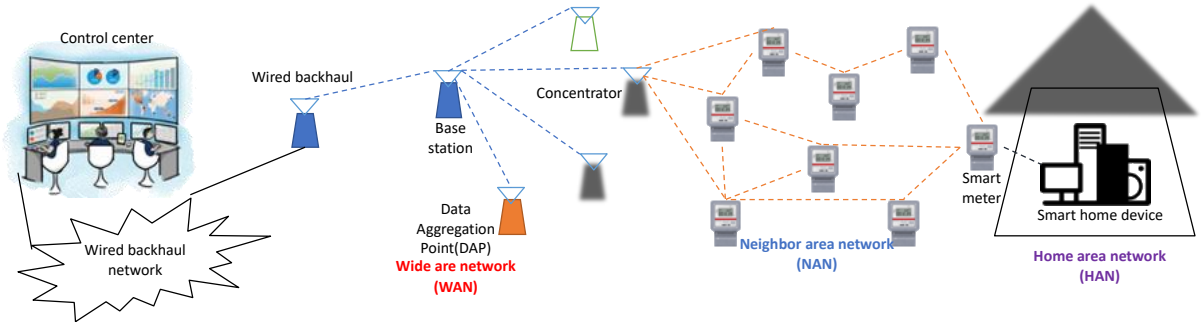
A smart grid infrastructure and the communication network is represented in figure 1. The electrical distribution infrastructure and communication infrastructure are to be separated from each other in smart grids [4]. Smart grids are a combination of the hardware, software parts along with the relationship among them. The current, voltage and consumption related consumer information is obtained in this structure. A two-way communication is established by the network that can monitor, read, process and configure information, control the meter from a remote environment and analyse the gathered data. These processes are all automated in the system [5].



(a) Distributed Electrical Infrastructure

ISSN: 2582-3051 (online)
Submitted: 15.12.2020
Accepted: 12.01.2021
Published: 19.01.2021

Journal of Electrical Engineering and Automation (EEA) (2020)
Vol.02/ No. 03
Pages: 112-117
https://www.irojournals.com/iroeea
DOI: https://doi.org/10.36548/jeea.2020.3.001



(b) Communication Infrastructure

Figure 1. Smart grid network infrastructure

2. Literature Review

A reliable and stable two-way communication is established between the manufacturer and consumer with the help of advanced metering infrastructure in smart grids such that the consumer privacy is maintained [6]. Existing data from the network can be obtained in a secure and private manner to overcome certain concerns of the consumers. Mathematical calculations can be performed using a Fully Homomorphic Encryption (FHE) technique for enabling secure data collection process. Data encryption is performed at the source and transmitted to the destination. This data is collected using various methods. FHE and Partially Homomorphic Encryption (PHE) schemes can be used for encryption and increase in security of these networks [7]. A complete or approximation encryption can be performed on the data first and calculation on the data can be done using Secure Multiparty Computation method. Various distributed power centres and computational solutions are discussed here. In advanced metering infrastructure, data collection may be performed using partially approximation method (PAM) due to its features like security, expansion of smaller messages and aggregation [8].

The aggregation process is executed in the cloud space between the gateway, receiver and transmitter in advanced metering infrastructure using these algorithms [9]. Generally aggregation is performed on the output gateway by most software. Advanced encryption and Paillier (Pai) cryptosystems are used in the terminal for performing end to end data acquisition. Elliptic Curve Digital Signature Algorithm (ECDSA) had been proposed by the FHE in the year 2009. This enabled achieving a full encryption solution. Encrypted text and large scale encryption schemes are produced using this technology when compared to other networks [10]. However, excessive noise created by the encryption may cause difficulties in implementation in certain places. The encryption and decryption keys are available similar to that of the FHE system in Smart-Vercauteren (SV) scheme. Decryption and multiplication features are also available. Data encryption is performed with the help of public and private keys provided by this scheme [11]. Small text size and key modes are proposed to be used in the FHE scheme. This scheme helps in an estimated data security maintenance. However, during rebuilding process, the package size is not considered. Smart grid data acquisition with the help of secure multitasking protocols are found in limited literature only [12].

3. Proposed Work

In this paper, privacy and security is maintained with secure protocol and architecture for data acquisition and decryption. Along with text encryption, homomorphic operation is also performed by this scheme with the help of a secure chord lookup protocol. Privacy preserving method is used for performing arithmetic operation and data aggregation using a secure multiparty computation (SMPC). Schemes with lesser computational complexity must be maintained for data measurement and protection of consumer data security [13]. The distortion from the acquired data should also be prevented. Data should also not be compromised. The processing time should be reduced along with the data storage memory while verifying, receiving or transferring information. System overhead, consumption of excess memory and time are the common drawbacks of most authentication plans. Implementation of a lightweight authentication model helps in overcoming these issues. A transmission data plan is provided exclusive of authentication. Here, validation of data is done and comparison with the initial data is performed [14]. The encryption complexities are eliminated while communication, memory and time overhead is improved in the encrypted data. During the process of data exchange, the public and private keys are created by the lightweight authentication scheme.

ISSN: 2582-3051 (online)
Submitted: 15.12.2020
Accepted: 12.01.2021
Published: 19.01.2021

Journal of Electrical Engineering and Automation (EEA) (2020)
Vol.02/ No. 03
Pages: 112-117
https://www.irojournals.com/iroeea
DOI: https://doi.org/10.36548/jeea.2020.3.001

Figure 2 provides the block diagram of the proposed protocol. When confirmation is obtained by two interconnectors, data exchange is done in a secure manner. Finger tables and hash process of the cuckoo filter obtains the acquired data in the first step. A ring protocol acts as a power distribution centre from which the measured data is transmitted to the consumers in the second step [15]. Data from the loop structure is removed and returned to the cuckoo filter in the third stage. Data from the centre of the cuckoo filter is compared with the destination filter. The outputs are found to be identical in both filters. This proves that data accuracy and integrity is maintained without any changes. The source has to return the request source if there is any output mismatch. The ring protocol involves a network comprising of consistent hashing, keys and nodes. Acceptable performance, proven accuracy and simplicity are the three major factors that distinguish ring protocol from the other existing protocols [16].

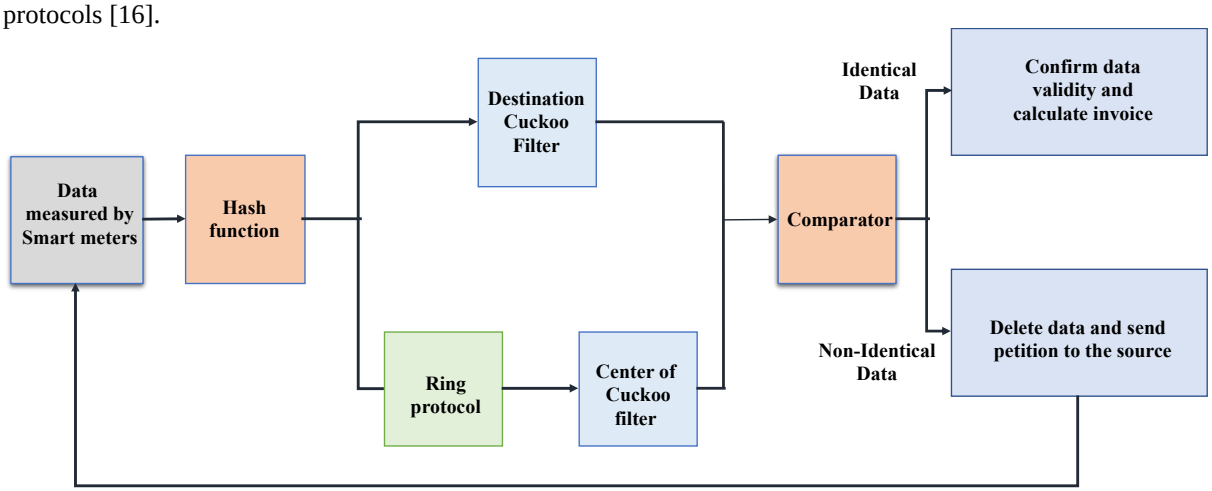


Figure 2: Proposed secure protocol model

4. Results and Discussion

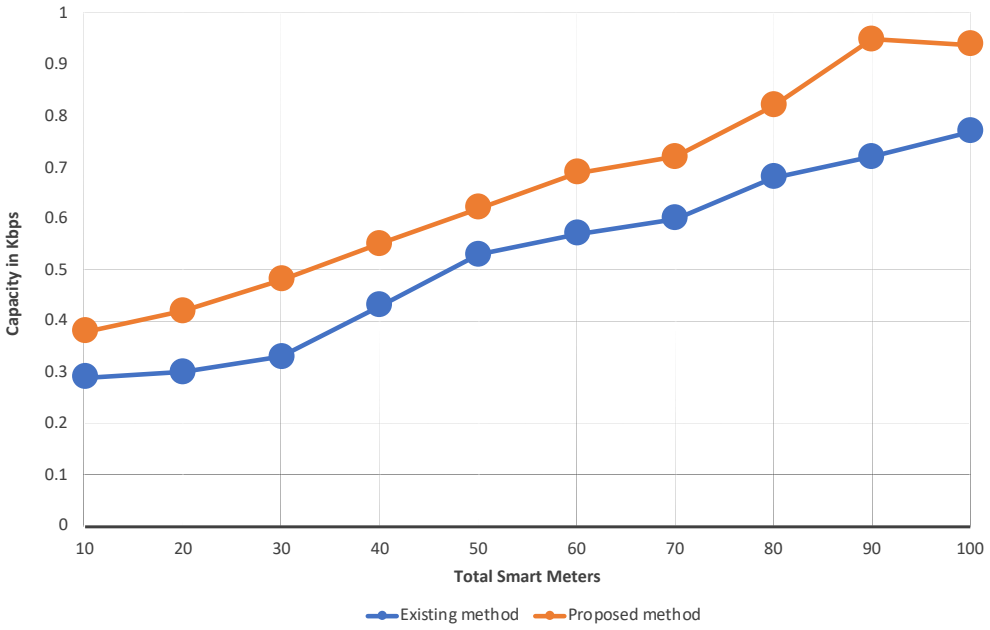


Figure 3: Production capacity comparison between existing and proposed system model

Packet delivery ratio, meantime completion time and production capacity are the major parameters that measure the performance of the proposed design. The number of meters is increased during simulation for achieving a real sample. The output capacity represents the total data received per second at each gateway during simulation. The loop structure annotation layer helps in centralized searching and reconstruction of data in the proposed scheme by which the data transmission and reception process has been improved drastically. Figure 3 represents a capacity comparison between the proposed system model and the existing system. It is evident that

ISSN: 2582-3051 (online)
Submitted: 15.12.2020
Accepted: 12.01.2021
Published: 19.01.2021

Journal of Electrical Engineering and Automation (EEA) (2020)
Vol.02/ No. 03
Pages: 112-117
https://www.irojournals.com/iroeea
DOI: https://doi.org/10.36548/jeea.2020.3.001

with the increase in number of smart meters, the production capacity can be increased by an approximate of 25%. MATLAB software is used for simulation of the proposed model system. Over a duration of 120 seconds, a maximum of 100 smart meters are used for the proposed simulation over 5 iterations. The meter size values are assumed to be between 1 to 100. For ease of computation and measuring the speed value, 3 hashes are considered with the length of cuckoo filter fixed at 100.

Data collection time involves the average time period to acquire all readings from all available smart meters in the data collection centre. Hash and loop structures are used instead of complex computation and cryptography. This helps in reduction of data collection time by eliminating wastage of computational time to a large extent. Figure 4 represents the average time for data acquisition compared across the existing and proposed techniques. It is deduced that the proposed system takes 50% lesser time to acquire all the information when compared to the existing model.

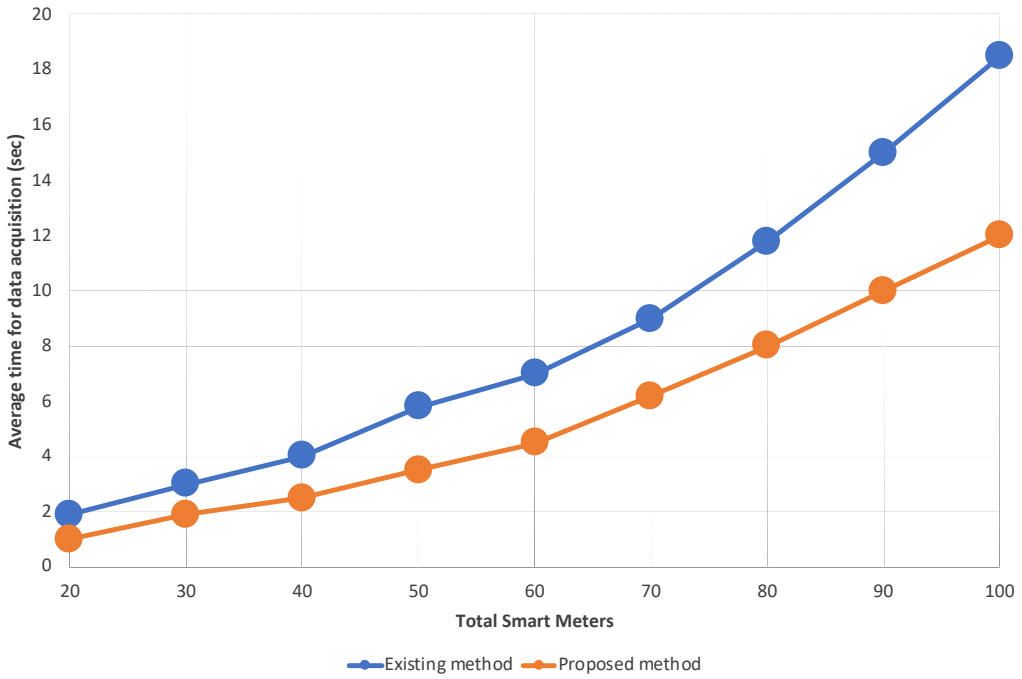


Figure 4 : Average data collection time comparison between the existing and proposed system model

A key is generated during the process which helps the meter in obtaining accurate data from the connecting meter from the corresponding building meter. This enables secure data exchange and communication. Secure connection can be established between two building meters using the public key used for encryption of the home meter data. The home meter is confirmed and authenticated if the appropriate data is received by the building meter. Cross authentication scheme can be provided by the proposed method between the building and home meters. A secure shared key can hence be provided by the lightweight authentication solution. There is no compromising in the cross-verification process if any unsuitable action takes place in the building or home meter security. Hence the security of rest of the keys is not affected by the connection between building and home keys. This provides better confidentiality through the lightweight authentication scheme.

ISSN: 2582-3051 (online)
Submitted: 15.12.2020
Accepted: 12.01.2021
Published: 19.01.2021

Journal of Electrical Engineering and Automation (EEA) (2020)
Vol.02/ No. 03
Pages: 112-117
https://www.irojournals.com/iroeea
DOI: https://doi.org/10.36548/jeea.2020.3.001

Figure 5: Communication overhead of lightweight authentication scheme

When compared to the existing scheme, the lightweight authentication model consumes substantially lesser memory. When the building meter concurrently receives large volume of data, the performance of the system can be improved. The impact on average communication overhead caused by the total number of meters is also analysed. The comparison between the existing and proposed schemes is as represented in figure 5. Over a duration of 60 to 90 seconds, there is an increase in the average communication overhead when the number of smart meters are increased. The total smart meters are increased from 2 to 30 for monitoring the response of lightweight authentication scheme in terms of communication overhead. It is noted that after certain value, the communication overhead remains constant despite increasing the number of smart meters using the proposed scheme.

5. Conclusion

This paper proposes an IoT based advanced metering infrastructure with secure chord lookup protocol. Finger table based scrambling scheme is used rather than complete and estimated homomorphic encryption schemes in the proposed model. Cuckoo filter is used for storing the numbers based on the finger table positions and compared with another filter in its parallel path. The outputs of both filters are compared and the bill is extracted if they are found to be identical. If there is a mismatch, the receiver requests the transmitter to resend the bill information. Latency, capacity and other output parameters of the system are improved while complete security is maintained during data transfer using this model.

References

[1] Cebe, M., & Akkaya, K. (2019). Efficient certificate revocation management schemes for IoT-based advanced metering infrastructures in smart cities. Ad Hoc Networks, 92, 101801.

[2] Cebe, M., & Akkaya, K. (2017, November). Utilizing Advanced Metering Infrastructure to Build a Public Key Infrastructure for Electric Vehicles. In Proceedings of the 6th ACM Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications (pp. 91-98).

[3] Panchanathan, P., & Kumar, E. R. Secure Route Discovery Protocol with Enhanced Backtracking Technique for MANET.

[4] Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2019). LSB: A Lightweight Scalable Blockchain for IoT security and anonymity. Journal of Parallel and Distributed Computing, 134, 180-197.

[5] Marzal, S., González-Medina, R., Salas-Puente, R., Figueres, E., & Garcerá, G. (2017). A novel locality algorithm and peer-to-peer communication infrastructure for optimizing network performance in smart microgrids. Energies, 10(9), 1275.

ISSN: 2582-3051 (online)
Submitted: 15.12.2020
Accepted: 12.01.2021
Published: 19.01.2021

Journal of Electrical Engineering and Automation (EEA) (2020)
Vol.02/ No. 03
Pages: 112-117
https://www.irojournals.com/iroeea
DOI: https://doi.org/10.36548/jeea.2020.3.001

[6] Shit, R. C., Sharma, S., Puthal, D., & Zomaya, A. Y. (2018). Location of Things (LoT): A review and taxonomy of sensors localization in IoT infrastructure. IEEE Communications Surveys & Tutorials, 20(3), 2028-2061.

[7] Cebe, M., & Akkaya, K. (2017, October). Efficient management of certificate revocation lists in smart grid advanced metering infrastructure. In 2017 IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS) (pp. 313-317). IEEE.

[8] Xu, Q., Aung, K. M. M., Zhu, Y., & Yong, K. L. (2018). A blockchain-based storage system for data analytics in the internet of things. In New Advances in the Internet of Things (pp. 119-138). Springer, Cham.

[9] Kimani, K., Oduol, V., & Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. International Journal of Critical Infrastructure Protection, 25, 36-49.

[10] Chin, W. L., Li, W., & Chen, H. H. (2017). Energy big data security threats in IoT-based smart grid communications. IEEE Communications Magazine, 55(10), 70-75.

[11] Barman, B. K., Yadav, S. N., Kumar, S., & Gope, S. (2018, June). IOT based smart energy meter for efficient energy utilization in smart grid. In 2018 2nd International Conference on Power, Energy and Environment: Towards Smart Technology (ICEPE) (pp. 1-5). IEEE.

[12] Muralidhara, S., Hegde, N., & Rekha, P. M. (2020). An internet of things-based smart energy meter for monitoring device-level consumption of energy. Computers & Electrical Engineering, 87, 106772.

[13] Smys, S. (2020). A Survey on Internet of Things (IoT) based Smart Systems. Journal of ISMAC, 2(04), 181-189.

[14] Mugunthan, S., & Vijayakumar, T. (2019). Review on IoT based smart grid architecture implementations. j Electric Eng Autom, 1(1), 12-20.

[15] Bhalaji, N. (2020). EL DAPP–An Electrıcıty Meter Trackıng Decentralızed Applıcatıon. Journal of Electronics, 2(01), 49-71.

[16] Nirmal, D. (2020). Artificial Intelligence Based Distribution System Management and Control. Journal of Electronics, 2(02), 137-47.

ISSN: 2582-3051 (online)
Submitted: 15.12.2020
Accepted: 12.01.2021
Published: 19.01.2021