ENHANCING SECURITY AND RESILIENCE IN SMART GRIDS THROUGH QUANTUM KEY DISTRIBUTION: CHALLENGES AND OPPORTUNITIES

Manpreet Kaur, Shweta Mishra
E-Mail Id: manpreetk209@gmail.com, shweta@deshbhagatuniversity.in
Department of Computer Science and Application, Desh Bhagat University, Mandi Gobindgarh, Punjab, India

Abstract- Smart grids offer many advantages, but they also come with some risks, especially regarding network security and privacy. This study aims to investigate the privacy and security of existing smart grid systems and to give a cross-section of the latest findings in the field of secure data aggregation and authentication for smart grids. The study focuses on addressing the challenges posed by malicious tampering and unauthorized access to metering data by exploring innovative approaches to ensure the integrity and confidentiality of data through a process termed "secure aggregate" and that the result of secure aggregations is authenticated in a manner that is both scalable and effective using Quantum Key Distribution. A software prototype has been developed to facilitate machine-to-machine authentication because this cryptographic key can be used and machine connections can be verified. This can contribute to the protection of essential infrastructure, the creation of a continuous threat detection feedback system, and the foundations of this technology are essential conditions for increasing the ability of systems to authenticate users.

Keywords: Machine-to-Machine Authentication, Network Security, Privacy, Smart Grids, Secure Data Aggregation, Quantum Key Distribution.

1. INTRODUCTION

Smart grid technology can perform tasks that the conventional grid can do using a sophisticated cyber-physical system and computer intelligence to enable decentralized bidirectional communication, real-time data analysis, and efficient administration. Integrating renewable energy sources, cutting carbon emissions, striking a healthy generation-consumption balance, preventing blackouts, and handling power outages are all goals. Smart grids could have many good effects, but they also come with some risks, especially regarding network security and privacy [1]. Many smart devices and operators collaborate in smart grids to collect real-time information about the system's status. Because of this, advanced metering infrastructure (AMI) is widely implemented throughout smart grids to monitor and control grid behavior. Several IoT solutions are conceptually comparable to smart grids [2]. In this method, the smart meters, often located in the customer's location, collect individual information about the amount of electricity used and then communicate that information to the utility company (i.e., for monitoring and billing purposes) [3]. There would be power waste and financial loss if the supplied meter readings were tampered with maliciously [4].

The smart grid is a potentially new electrical grid paradigm that uses two-way communications between grid organizations to increase transmission flexibility and reliability. Due to the potential for personally identifiable information inference, the privacy of use information monitored by individual smart meters has received considerable attention in the smart grid system. Unauthorized changes to gathered data by enemies with bad intentions would also make it hard to get power to where it needs to go in an effective and reliable way. Due to these threats, it is crucial that the smart grid include measures to ensure the privacy of metering data through a process termed "secure aggregation" and that the result of secure aggregation is authenticated in a manner that is both scalable and effective. This study aims to investigate the privacy and security of existing smart grid systems and to give a cross-section of the most recent findings in the field of secure data aggregation and authentication for smart grids [5].

A Smart Grid (S.G.) allows users and power companies to talk to each other in a two-way, demand-response way with high computing and communication performance. However, this opens the door for users' private information to be shared. Consequently, a new challenge for S.G. is enhancing individual power consumption and distribution efficiency to assure communication dependability while maintaining user privacy. So, they set up a hierarchical communication architecture for power requirement and distribution aggregation (EPPRD) that works well and keeps personal information private. In the system that has been suggested, there is an efficient encryption and authentication method that has been provided to match each specific demand-response scenario better. The authors show how the EPPRD can withstand various security attacks, keep users' data private, and change to meet their needs with a partially true model. Compared to other systems, computing and sending messages takes less time. It does this by doing much research and testing [6].

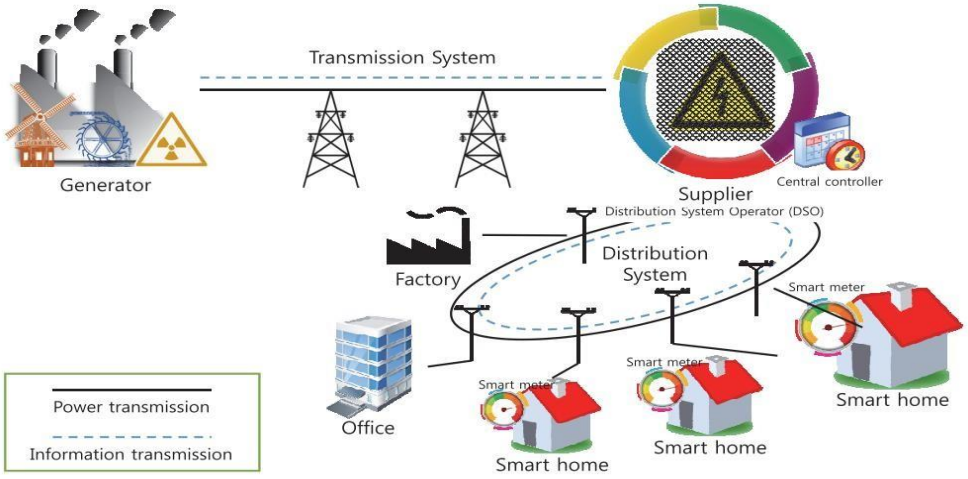

Fig. 1.1 An overview of Smart Grid Architecture [5]

Recent advancements in secure data aggregation and authentication techniques tailored for smart grids. The focus lies on addressing the challenges posed by malicious tampering and unauthorized access to metering data by examining the latest findings in this field. The study aims to contribute to the development of robust and resilient smart grid infrastructures while smart grids offer numerous benefits they also pose security and privacy challenges ensuring the integrity and confidentiality of metering data is crucial for maintaining the effectiveness and reliability of smart grid operations by exploring innovative approaches to secure data aggregation and authentication. This study aims to enhance the security posture of smart grid systems and mitigate potential risks associated with malicious activities. Section 2 contains existing technologies and their limitations. Section 3 will explain our proposed scheme in details with handling various threats, Section 4 will show the analysis and evolution of our scheme. Section 5 will conclude the paper suggests some and future work in this field.

1.1 Smart Grid Security and Existing Work

The administration of data collected by smart meters necessitates the development of a solution that is by applicable privacy requirements. At the same time, this solution should make it possible to use the collected data in the three ways previously described. In addition to this functional need, smart meter data management protocols and solutions should satisfy various security standards.

1.1.1 Confidentiality

During transmission (also known as "data in transit"), storage (also known as "data at rest"), and computing, meter data should not be accessible to anyone or anything that is not allowed (data in use). To achieve cryptographic privacy, it is important to protect the secrecy of data while it is moving, while it is being stored, and while it is being used.

1.1.2 Integrity

The data from the meter should keep their precision and correctness throughout the transmission, storage, and processing stages, and any modifications made to the data should be identifiable.

1.1.3 Authenticity

The data receiver needs to be able to validate the integrity of the information it receives from the meter.

1.1.4 Non-Repudiation

There should be no way for the entity that created the meter data to refute that it was the source of the data. It has connotations of authenticity and genuineness.

1.1.5 Auditability

It must be feasible to validate whether or not the information provided in response to a request (whether it be meter data or a calculation based on meter data) is accurate [7].

2. LITERATURE REVIEW

Singh et al., (2021) [8] propose a privacy-preserving data aggregation technique using deep learning and homomorphic encryption to offset the detrimental effects of a flash burden on prediction model efficacy. The suggested BHDA method demonstrates this with only a modest increase in processing cost.

Guo et al., (2020) [4] suggest that a unique symmetric homomorphic encryption system is the basis for an effective strategy for lightweight aggregation in a smart grid. A concise analysis of our suggested system demonstrates that our proposed scheme is superior in terms of safety and effectiveness.

Guan et al., (2019) [10] proposed that the EFFECT strategy in a smart grid is an efficient, adaptable, and privacy-

preserving aggregation and authentication technique. The authors compare it to current techniques to further prove the efficacy of the suggested strategy in terms of low computing complexity and communication overhead.
Liu et al., (2019) [11] presented a smart grid model that makes use of fog computing and then uses it to inform the design of a privacy-preserving, highly effective communication. The results of our experiments show that our approach is effective, requiring few resources for both computation and communication.
Romdhane et al., (2019) [12] presented a homomorphic encryption-based safe and private data aggregation system. Extensive testing and analysis prove that our suggested approach is secure and protects users' personal information.
Shen et al., (2017) [13] propose an anonymized power usage data cube-aggregation technique. Finally, our research demonstrates that the suggested method is cost-effective in terms of computing and transmission.
Customers and utilities can improve their ability to monitor and control the amount of energy they consume with the help of information and communication technology, which is enabled by smart grid technologies. It is anticipated that the electric grid's reliability, efficiency, and long-term viability will all improve as a result. This will be accomplished through the utilization of more sophisticated monitoring and control systems. Because modern communications networks are used, criminals have the potential to target the power system and obtain vital information. A software prototype was developed to facilitate machine-to-machine authentication. Because of this, cryptographic keys could be used, and machine-to-machine connections could be verified. This example demonstrates how to use QKD to strengthen the protection afforded to infrastructure. This can contribute to the protection of vital infrastructure. Building a loop threat detection feedback system as the foundation of this technique is a crucial prerequisite for increasing a system's capability to authenticate users. This system will serve as the cornerstone of this technique [14].

3. PROPOSED TECHNOLOGY

3.1 Quantum Key Distribution (QKD)

A technology known as quantum cryptography employs quantum physics to ensure the safety of the deployment of symmetrical encryption keys. QKD is a moniker that more accurately describes quantum cryptography. The different QKD techniques are designed to assure that any effort by an unauthorized person to view the broadcast photons could disturb the communication if the eavesdropper succeeds in observing the photons.

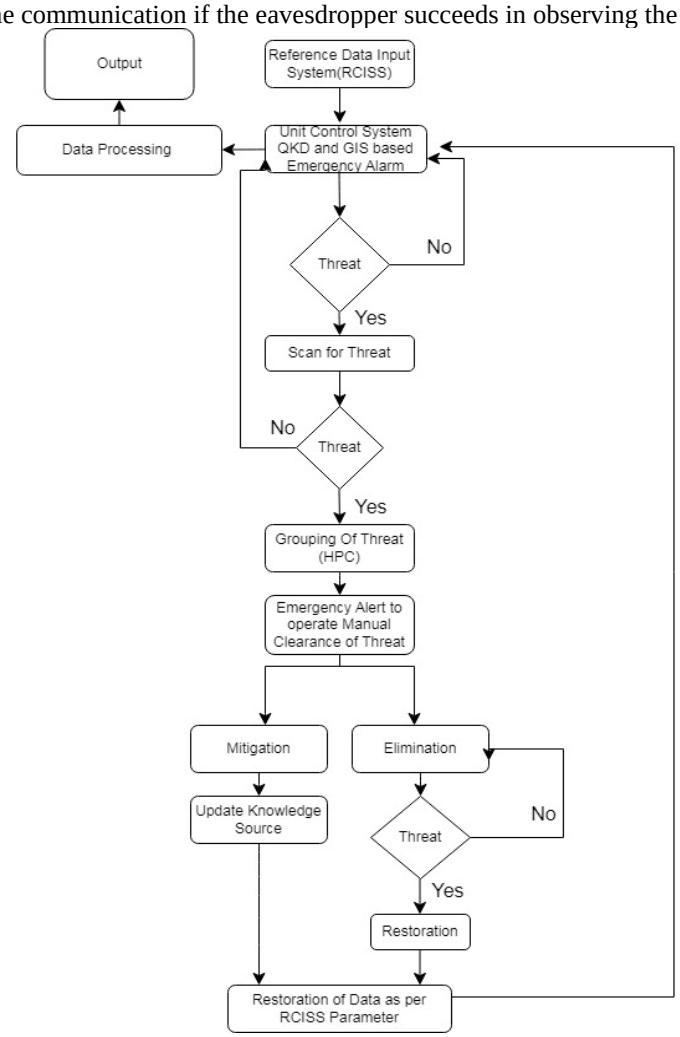

Fig. 3.1 Block Diagram Authentication Approach

$$Q = 2 \times \left\lfloor A + \frac{\log\left\lceil \frac{Q}{2} \right\rceil}{\log 2} + S\frac{Q}{2} + L \right\rfloor$$

Whereas Q is denoted as the Raw Key, A is denoted as the length of the final key, S is denoted as the percentage of the raw key, and L is denoted as the number of bits leaked during the key reconciliation phase [15].

The defined block diagram mentioned in Figure 3.1, depicts the complete layout of defining conditions mechanism to analyze the system perfectly and the layering of conditions suitably fulfill the desired result completely. The grid mechanism applied in the process shows the complete feedback mechanism to analyze and nullify the threading order to contain a proper authentication process.

The Algorithm is mentioned here-

1. The stage that is responsible for the output data is the stage that clears threats and provides feedback. This stage also provides data for additional analysis and reference input for the Reference Control and Support System (RCISS).
2. After being cross-checked by the RCISS, sensors, or GIS-based system with the control and support system unit to determine whether there is a threat, the alert that was generated from the input data was delivered to the reference input. Based on the quantum key distribution (QKD) technique, it transmits data at the central processing stage, which could be compared to a control center. This comparison is appropriate. At this point, the necessary features required from the data are extracted, classified, identified, and grouped in preparation for an effective system clearance and restoration.
3. After fulfilling the necessary parameters in the above steps, the system follows a feedback mechanism to detect thread if no thread is found then the data moves to processing format for responsive output.
4. If any thread is found, the threat must be scanned before again sending to the feedback condition if any threat is found in the system. This possible condition defines the working module of the smart grid layout design for this privacy-preserving approach technique.
5. After any threat is produced again, the processing mechanism of the smart grid moves to the grouping stage where the sorting or grouping of threads concerning the processor is used. The processor mainly used for the sorting mechanism is a high-performance computing resource (HPC) to interpret live sensors in real time. Based on the condition of prediction analysis which is faster than real-time.
6. After grouping any unwanted threats group emergency alert sends to the operating manual clearance of threat to analyze if the threat can nullify without being into the failure condition and if the threat can nullify then only moves to the next condition only.
7. After manually clearing the unnecessary condition or threat that ably to nullify moved into two conditions-
   (a) Mitigation- the resilience condition applied if the power of thread to distort the system is very low and it cannot harm efficiently than the generalized source of data in this condition moved to this condition to process and send to another processing step.
   (b) Loop again applied to neglect high order thread and only small deviation containing thread allows passing to restoration condition then proceed to another applied condition.
8. After processing all the internal background processing of any leak or thread that occurred in a process and applying the conditions of the smart grid mechanism perfectly then the output data source arrived matched to the input applied RCISS(Reference Control and Support System) condition to match the authentication of the system in a privacy-preserving aggregation approach perfectly and again follows a feedback loop mechanism to match the authentication level to sends its result to unit control processing condition to preserve the system correctly. The output value is processed again in the block. If any thread again occurs, then the system is processed again completely.

4. SECURITY ANALYSIS

In this section we analyze the security properties of our proposed scheme. The analysis will focus on how this scheme can address the security requirements. The Above Algorithm resolves following security issues-

4.1 User Authentication

Proposed scheme ensures that only legitimate parties participate in secure communication preventing unauthorized access to sensitive information

4.2 Data Integrity

QKD provides unconditionally secure communication it leverages quantum phenomena to create keys that are inherently resistant to eavesdropping or interception it enhances data integrity by protecting against classical attacks

4.3 Denial of Service

QKD protocols are designed to handle dos attacks by detecting fake users and ensuring secure communication channels while risks exist practical implementations mitigate these vulnerabilities making QKD a promising technology for secure communication.

4.4 Threat Analysis

Threat analysis at each looping algorithm and ensure completely handling any kind of attack. It is expected that the reliability efficiency and long-term viability of the electricity grid will improve as a result, because criminals using modern communication networks have the potential to target the electricity system and obtain essential information. A software prototype has been developed to facilitate machine-to-machine authentication because of this cryptographic key that can be used and machine-to-machine connections can be verified. This example shows how to use QKD to strengthen the protection of infrastructure. This can contribute to the protection of essential infrastructure, the creation of a continuous threat detection feedback system, and the foundations of this technology are essential conditions for increasing the ability of systems to authenticate users.

CONCLUSION AND FUTURE WORK

This paper first introduces the smart grid technology its different components and how the are connected to each other then it highlights various threat issues associated with sg communication and various previous schemes that tries to handle these threats then we proposed a new scheme that handles the security threats like data confidentiality data integrity service failure data aggregation and authentication with different looping mechanisms to handle the threat with QKD protocol through the block diagram the author tries to explain the threat handling mechanism the proposed system tries to assure unconditional secure communication with use of quantum key that blocks the unauthorized access to the transmission of any information between two parties as future work QKD is theoretically secure practical implementations can be vulnerable to side-channel attacks designing and handling of QKD protocols are vulnerable due to its high complexity the whole QKD depends on photon generator which can leads to incorrect information due to imperfection of the device in practical.

REFERENCES

[1] Alaba, Fadele Ayotunde, et al. "Internet of Things security: A survey." Journal of Network and Computer Applications 88 (2017): 10-28.

[2] Agarkar, Aarti, and Himanshu Agrawal. "A review and vision on authentication and privacy preservation schemes in smart grid network." Security and Privacy 2.2 (2019): e62

[3] Nabeel, M., Kerr, S., Ding, X., & Bertino, E. “Authentication and key management for advanced metering infrastructures utilizing physically unclonable functions.” IEEE Third International Conference on Smart Grid Communications (SmartGridComm) (2012) :324-329.

[4] Guo, Fei, Zhenfu Cao, Zhusen Liu, and Nanyuan Cao. "A Privacy-Preserving Aggregation and Authentication Scheme Towards Mobile Users in Smart Grid." Journalof Shanghai Jiaotong University (Science) 25 (2020): 37-43.

[5] Koo, Dongyoung, Youngjoo Shin, and Junbeom Hur. "Privacy-preserving aggregation and authentication of multi-source smart meters in a smart grid system." Applied Sciences 7, no. 10 (2017): 1007.

[6] Zhang, Lei, and Jing Zhang. "EPPRD: an efficient privacy-preserving power requirementand distribution aggregation scheme for a smart grid." Sensors 17, no. 8 (2017): 1814.

[7] Asghar, Muhammad Rizwan, György Dán, Daniele Miorandi, and Imrich Chlamtac. "Smart meter data privacy: A survey." IEEE Communications Surveys & Tutorials 19, no. 4 (2017): 2820-2835.

[8] Singh, Parminder, Mehedi Masud, M. Shamim Hossain, and Avinash Kaur. "Blockchain and homomorphic encryption-based privacy-preserving data aggregation model in smart grid." Computers & Electrical Engineering 93 (2021): 107209.

[9] R. Jangid; J.k Maherchandani; R.R. Joshi and B.D Vairagi, “Development of Advance Energy Management Strategy for Standalone Hybrid Wind & PV System Considering Rural Application”, IEEE 2nd International Conference on Smart Systems and Inventive Technology, Organized by Francis Xavier Engineering College during November 27-29, 2019 at Tirunelveli, India.

[10] Guo, Cheng, Xueru Jiang, Kim-Kwang Raymond Choo, Xinyu Tang, and Jing Zhang. "Lightweight privacy-preserving data aggregation with batch verification for smart grid." Future Generation Computer Systems 112 (2020): 512-523.

[11] Guan, Zhitao, Yue Zhang, Liehuang Zhu, Longfei Wu, and Shui Yu. "EFFECT: An efficient flexible privacy-preserving data aggregation scheme with authentication in smart grid." Science China Information Sciences 62, no. 3 (2019): 1-14.

[12] Liu, Jia-Nan, Jian Weng, Anjia Yang, Yizhao Chen, and Xiaodong Lin. "Enabling efficient and privacy-preserving aggregation communication and function query for fog computing-based smart grid." IEEE Transactions on Smart Grid 11, no. 1 (2019): 247-257.

[13] Romdhane, Rihem Ben, Hamza Hammami, Mohamed Hamdi, and Tai-Hoon Kim. "A novel approach for privacy-preserving data aggregation in smart grid." In 2019 15th International Wireless Communications

& Mobile Computing Conference (IWCMC), pp. 1060-1066. IEEE, 2019.
[14] H. Kumawat and R. Jangid, “Using AI Techniques to Improve the Power Quality of Standalone Hybrid Renewable Energy Systems”, Crafting a Sustainable Future Through Education and Sustainable Development, IGI Global, Pages 219-228, 2023.
[15] H. Kumawat; R. Jangid, “Performance and Investigation of Two Drive Train Interfaced Permanent Magnet Synchronous Generator for Wind Energy Conversion System”, Journal of Emerging Technologies and Innovative Research, ISSN:2349-5162, Volume 7, Issue 1, January 2020.
[16] R. Jangid et. al., “Smart Household Demand Response Scheduling with Renewable Energy Resources”, IEEE Third International Conference on Intelligent Computing and Control System, Organized by Vaigai College of Engineering during May 15-17, 2019 at Madurai, India.
[17] S. Kumar; R. Jangid and K. Parikh “Comparative Performance Analysis of Adaptive Neuro-Fuzzy Inference System (ANFIS) & ANN Algorithms Based MPPT Energy Harvesting in Solar PV System.” International Journal of Technical Research and Science, vol. 8, Issue 3, March 2023.
[18] S. Sharma; R. Jangid and K. Parikh “Development of Intelligent Control Strategy for Power Quality Improvement of Hybrid RES Using AI Technique” International Journal of Technical Research and Science, vol. VIII, Issue II, Feb. 2023.
[19] L. Jhala et al., “Development of Control Strategy for Power Management in Hybrid Renewable Energy System” International Journal of Technical Research and Science, vol. VI, Issue XII, Dec. 2021.
[20] P. S. Rajpurohit, et al., “Design of DE Optimized PI and PID Controller for Speed Control of DC Drives” International Journal of Research in Engineering, Science and Management, Volume-2, Issue-6, June-2019.
[21] N. Dhakre, et al., “Optimal Synchronization of PSS and Statcom Based Controller Using De Algorithm” International Journal for Research in Applied Science & Engineering Technology, Volume-5, Issue-XI, Nov.-2017.
[22] P. Megha, et al., “Flow Analysis of Transmission System Incorporating STATCOM” International Journal of Inventive Engineering and Sciences, Volume-3, Issue-1, Dec.-2014.
[23] D. Trivedi, et al., “Optimization of Voltage Stability of Transmission line using UPQC” International Journal of Engineering Research & Technology, Volume-4, Issue-2, Feb.-2015.
[24] Shen, Hua, Mingwu Zhang, and Jian Shen. "Efficient privacy-preserving cube-data aggregation scheme for smart grids." IEEE Transactions on Information Forensics and Security 12, no. 6 (2017): 1369-1381.
[25] Alshowkan, Muneer, Philip G. Evans, Michael Starke, Duncan Earl, and Nicholas A. Peters. "Authentication of smart grid communications using quantum key distribution." Scientific reports 12, no. 1 (2022): 1-13.
[26] Yulianti, Lenny Putri, and Kridanto Surendro. "Implementation of Quantum Annealing: A Systematic Review." IEEE Access (2022).