IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

SECURE AND PRESERVE PRIVACY FOR CONSUMER AND CONSUMPTION DATA IN ADVANCED METERING INFRASTRUCTURE

Sudha Devi K[1], Dharani Dharan N[2], Jagadeesh M[3], Jeya Pandi M[4], Maibalan K[5]
[1]*Associate professor,* [2] *student,* [3] *student,* [4] *student,* [5] *student*
Department of Computer Science and Engineering,
Paavai Engineering College (Autonomous)
Pachal, Namakkal, Tamil Nadu., India.

Abstract : Smart grids, as integral components of Advanced Metering Infrastructure (AMI), have redefined energy management by providing real-time insights and optimizing consumption. However, this technological advancement is accompanied by critical challenges pertaining to the security and privacy of consumer data. The existing solutions, while attempting to mitigate security concerns, are found to be susceptible to re-identification attacks, communication overhead, and compromise of sensitive consumer information. To overcome these limitations, this project proposes a novel and comprehensive system: GridChain. GridChain integrates state-of-the-art technologies, including hash functions, differential privacy, and blockchain, to fortify the security and privacy framework of AMI. This project harnesses cutting-edge technologies, including hash functions, differential privacy, and blockchain. Hash functions are employed to fortify the protection of sensitive consumer information, ensuring data integrity and confidentiality. The integration of differential privacy techniques introduces controlled noise into smart meter data, preserving individual privacy while allowing meaningful aggregate analysis. The incorporation of blockchain technology establishes a distributed and immutable ledger, recording and verifying smart meter data transactions while preserving consumer privacy. Extensive experiments were carried out to assess our proposal, and the results indicate that our proposal is capable of accurately identifying malicious consumers with acceptable overhead while preserving the privacy of the consumers. The results underscore GridChain's superiority, showcasing enhanced performance, reduced communication overhead, and heightened resistance against re-identification attacks.

Index Terms - Convolutional Neural Networks (CNNs), Scale Invariant Feature Transformation (SIFT), Class Similarity Network (CSN)

INTRODUCTION

A smart grid is an electrical power distribution infrastructure that provides two-way communication between the utility provider and customers. Digital technologies that contribute to smart grid technology include power/current sensors, controls, data centers, and smart meters. "The grid," refers to the electric grid, a network of transmission lines, substations, transformers and more that deliver electricity from the power plant to your home or business. This system allows for monitoring, analysis, control and communication within the supply chain to help improve efficiency, reduce energy consumption and cost, and maximize the transparency and reliability of the energy supply chain. The smart grid was introduced with the aim of overcoming the weaknesses of conventional electrical grids by using smart net meters. Many government institutions around the world have been encouraging the use ofsmart grids for their potential to control and deal with global warming, emergency resilience and energy independence scenarios. A smart grid often also includes the integration of renewable energy sources. These renewable sources, along with a more

decentralized energy supply and bidirectional power flows, can increase the efficiency and sustainability of the power distributed through the grids and reduce the effect of peak power times on the power infrastructure..

OBJECTIVES

The aim of this research is to develop and demonstrate a comprehensive solution called GridChain that enhances privacy and security within the context of Advanced Metering Infrastructure (AMI). GridChain integrates blockchain technology, Differential Privacy, and other mechanisms to safeguard consumer data, protect against privacy breaches, and ensure secure communication, ultimately enabling a responsible and secure modernization of the power grid. • To enhance privacy within Advanced Metering Infrastructure (AMI).

- To strengthen security through the integration of blockchain and PKI.
- To ensure data utility while protecting individual privacy.
- To optimize GridChain for efficient and practical deployment.
- To validate GridChain's effectiveness using real-world smart meter data.
- To compare GridChain with existing solutions to demonstrate its superiority.
- To contribute to the secure modernization of the power grid infrastructure.

RESEARCH METHODOLOGY

[1] SONG, WEIWEI As a Bidirectional communication in smart grids raises privacy concerns due to the granular flow of energy consumption data. Aggregation methods employed by energy utilities may not fully protect privacy, especially for applications like nonintrusive load monitoring that require disaggregated data. Propose a privacy-preserving scheme for smart grids using a Trusted Execution Environment (TEE) to protect consumer privacy without compromising accuracy. The scheme employs customer-oriented aggregation and prevents false data injection attacks. Utilized to protect the privacy of data collected from smart appliances (SAs). Instead of regular aggregation methods, the scheme employs customeroriented aggregation to provide privacy without sacrificing accuracy A novel scheme proposed to initialize keys, ensuring the encrypted database preserves customer data securely. TEE acts as a trusted key store for cryptographic credentials of SAs and performs security functions during consumer data usage for operational purposes. Linear complexity for decryption operations on TEE, allowing scalability for real-world applications. Utilized for protecting data privacy and performing security functions. The proposed privacypreserving scheme, leveraging TEE and customer-oriented aggregation, outperforms other privacy methods in terms of communication and computation cost. It ensures end-to-end confidentiality without affecting existing smart meter deployment models. Further investigations are planned to improve the model's robustness and scalability.

[2] M. V. VISHNUDAS In their study, Analyzing real-time power data in smart grids while preserving user privacy poses challenges. Existing privacy-preserving data aggregation schemes are limited to stationary users or rely on trusted centers, presenting vulnerabilities. Propose an efficient and robust multidimensional data aggregation scheme for smart grids based on blockchain. Overcome limitations of existing schemes by using a leader election algorithm, verifiable secret sharing homomorphism, and supporting multidimensional data aggregation and fault tolerance. Leader Election Algorithm: Utilize a leader election algorithm in Raft protocol to select a mining node from smart meters for data aggregation. Adopt a dynamically verifiable secret sharing homomorphism scheme for flexible dynamic user management. Leverage blockchain for secure and transparent data aggregation without the need for a trusted authority. Implement multidimensional data aggregation based on the Chinese Remainder Theorem for efficiency. Conduct security analysis to ensure the scheme is IND-CPA secure and meets robust security features. Compare the proposed scheme with other referenced works, assessing computation and communication overhead. The proposed scheme is efficient and robust, utilizing blockchain for transparent and secure data aggregation. A leader election algorithm ensures the selection of a mining node for aggregation. Verifiable secret sharing homomorphism enables flexible dynamic user management. The scheme supports multidimensional data aggregation and fault tolerance. Security analysis demonstrates IND-CPA security and robust security features. Experimental results show lower computation and communication overhead compared to other schemes. Further improvement is suggested for realizing verifiable data aggregation in the future.

[3] ZHENGZHUO HAN In this paper In IoT-enabled smart grid (SG) systems, the smart meter (SM) collects power usage information and transmits it to the central service provider (CSP) over the Internet. This information is vulnerable to security threats, and ensuring the integrity of communication between SMs and CSP is crucial for the smooth operation of the SG system. Present an anonymous and reliable authentication protocol for smart grids (ARAP-SG) to facilitate secure and reliable information exchange between smart meters (SM) and central service providers (CSP) in smart grid systems. The protocol aims to establish a secure channel for communication while preserving the anonymity of both SM and CSP. Authorize CSP and SM to construct a session key (SK) after completing the authentication phase for undecipherable information exchange in the future. Use the random oracle model for security verification of the constructed SK in ARAP-SG. Conduct informal security analysis to demonstrate the protocol's ability to thwart covert security attacks. Employ ROM-based and Scyther-based formal analyses to establish the security of ARAP-SG. Compare ARAP-SG with relevant authentication protocols, showcasing lower computational and communication overheads (25.5-56.76% and 7.69-49.47%, respectively) with improved security properties. ARAP-SG ensures reliable information exchange during the authentication phase while maintaining the anonymity of both CSP and SM. The protocol allows CSP and SM to establish a session key (SK) for secure future information exchange. Formal analyses using the random oracle model and Scyther demonstrate the security of ARAP-SG. Informal security analysis confirms ARAP-SG's capability to withstand various security threats. Comparative analysis shows that ARAP-SG requires fewer resources with improved security functionalities compared to relevant authentication protocols. The protocol allows the construction of a session key (SK) for future secure exchanges. Security analyses, including formal assessments and comparisons with other protocols, validate ARAP-SG's effectiveness in providing security with reduced computational and communication overheads.

[4] WEIXUN ZHOU In this paper, In smart power grid systems, the real-time sharing of electricity data offers numerous benefits, but security and privacy challenges arise due to the potential inclusion of private and sensitive information. Achieving a balance between data utilization, data privacy, and user privacy is crucial. Propose a framework for secure data sharing in smart grid systems, addressing privacy concerns and ensuring data security. The focus is on leveraging privacy-preserving multi-authority attribute-based encryption (MA-ABE) using the inner product encryption (IPE) technique. Inner Product Encryption (IPE): The proposed scheme utilizes IPE, where the access policy and attribute set are made fuzzy by converting them into two vectors. Successful data access is contingent on the orthogonality of these vectors. The scheme allows threshold access policies to involve only attribute name indexes, preserving sensitive attribute values and ensuring attribute privacy. To enhance efficiency, a testing phase is introduced before data recovery, preventing unnecessary operations. The security of the proposed scheme relies on the decisional bilinear k-Linear assumption, reducing the need for strong assumptions. Inner Product Encryption (IPE): Utilized to make access policies and attribute sets fuzzy, ensuring successful data access only when two vectors are orthogonal. The proposed framework addresses privacy-preserving data sharing and data security challenges in smart grid systems. The use of IPE and the orthogonal vectors criterion enhances the security and privacy of shared data. The scheme's security is based on the decisional bilinear k-Linear assumption, contributing to its robustness. Performance analysis indicates that the proposed approach outperforms known schemes in terms of efficiency. Performance analysis indicates the superiority of the proposed approach compared to known schemes.

PROBLEM DEFINITION

The problem addressed by the project revolves around the inherent challenges in ensuring the security and privacy of consumer data within the Advanced Metering Infrastructure (AMI). Two primary issues are identified:

- Firmware Hacking and Billing Fraud: Malicious consumers attempt to compromise the integrity of smart meters by hacking into them and altering the firmware. This unauthorized manipulation allows them toreport false electricity consumption readings to the energy provider, leading to reduced bills. The potential economic losses for the power grid and the risk of incorrect decision-making in energy management necessitate robust security measures.
- Privacy Breaches and Re-Identification Attacks: Attackers may attempt to acquire the consumption readings of fellow consumers to deduce sensitive information about them. This unauthorized access poses a threat to consumer privacy. Traditional methods, including hardware tamper-proof modules, face limitations in preventing these attacks due to cost constraints and challenges in guaranteeing full trust. These identified problems underscore the urgency of implementing a comprehensive solution to safeguard consumer information, prevent fraudulent activities, and preserve privacy within the AMI. The proposed Grid Chain project aims to address these challenges by incorporating advanced security measures, including hash functions, differential privacy techniques, noise generation mechanisms, Public Key Infrastructure (PKI), and blockchain technology. The goal is to create a resilient and privacy-preserving infrastructure that ensures the integrity of smart meter data while allowing for secure and efficient grid management.

OVERVIEW OF THE PROJECT

The project presents a solution to address critical challenges within the Advanced Metering Infrastructure (AMI). The project aims to enhance the security, integrity, and privacy of consumer and consumption data in smart grids. The following key components and objectives provide an overview of the project: Security and Privacy Preservation:

- Utilization of hash functions to protect sensitive consumer information,including consumer IDs and locations.
- Integration of differential privacy techniques to inject controlled noise intosmart meter data, ensuring privacy preservation while maintaining utility in aggregate analysis.
- Implementation of noise generation mechanisms, such as Laplace or Gaussian noise, to safeguard consumption data against re-identificationattacks. Digital Identity Management:
- Deployment of Public Key Infrastructure (PKI) to manage digital identities securely and establish secure communication channels amongnetwork participants. Blockchain Technology Integration:
- Adoption of a distributed and immutable blockchain ledger for recordingand verifying smart meter data transactions.
- Preservation of consumer privacy through the transparency and securityprovided by the blockchain. User Interfaces:
- Development of user interfaces catering to both EU Admins and Consumers.
- EU Admin Interface with features for grid monitoring, consumer management, analytics tools, and user access controls.
- Consumer Interface offering a personalized dashboard for real-time consumption data, account management, bill payments, energy efficiencytips, and privacy controls.

SYSTEM TESTING

Introduction:

Grid Chain is a sophisticated software solution designed to enhance the security and privacy of consumer and consumption data in the context of Advanced Metering Infrastructure (AMI). This software testing report outlines the various testing phases conducted to ensure the reliability, security, and effectiveness of Grid Chain.

Testing Objectives: The primary objectives of software testing for GridChain Include.

- Evaluate the functionality and performance of privacy-preserving features.
- Ensure the robustness of security measures, including hash functions, differential privacy, and noise generation.

- Verify the proper integration and functionality of Public Key Infrastructure (PKI) and Blockchain components.
- Assess the system's resilience to potential vulnerabilities and attacks. Testing Phases:
- Unit Testing: Conducted testing at the individual component level to ensure each module functions as intended. Verified the correctness of hash functions, noise generation mechanisms, and differential privacy algorithms.
- Integration Testing: Tested the interactions between different modules to ensure seamless integration. Verified the integration of PKI and Blockchain components with other system elements.

System Testing: Evaluated the overall functionality and performance of GridChain. Teste
d end-to-end scenarios, including data transmission, noise injection, and blockchain ledger verification.

- Security Testing: 30 Conducted penetration testing to identify and address potential security vulnerabilities. Verified the effectiveness of security measures in preventing unauthorized access and data breaches.

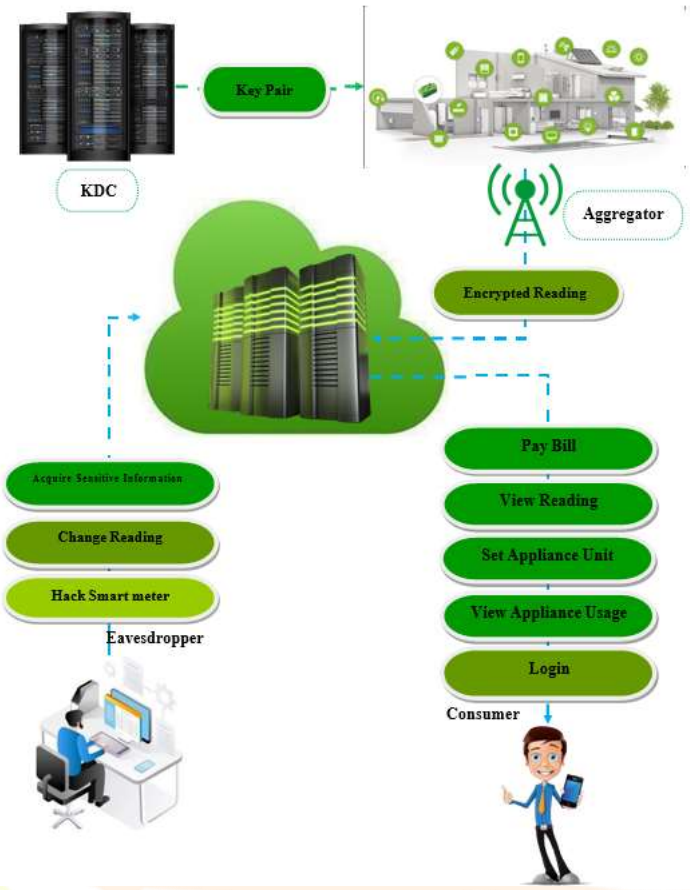
Performance Testing: Assessed the system's performance under normal and peak load conditions. Verified response times, resource utilization, and system scalability. Testing Tools: Various testing tools were employed, including:

- JUnit: For unit testing of individual components.
- Selenium: For automated testing of user interfaces.
- OWASP ZAP: For security testing and identifying potential vulnerabilities.
- LoadRunner: For performance testing under various load conditions.

Test Cases Test Case ID: TC001 Input: Validate Hash Function Expected Result: Hashed output for a given input matchesthe expected hash value. Actual Result: Passed Pass: Yes Test Case ID: TC002 Input:**Evaluate Differential Privacy Expected Result**: Differential privacy techniquessuccessfully inject controlled noise into smart meter data. 31 Actual Result: Passed Pass: Yes Test Case ID: TC003 Input: Test Noise GenerationMechanism (Laplace Noise) Expected Result: Laplace noise added to consumption data ensures re-identification resistance. Actual Result: Passed Pass: Yes Test Case ID: TC004 Input: Validate Noise Generation Mechanism (Gaussian Noise) Expected Result: Gaussian noise implementation safeguardssensitive consumption data. Actual Result: Passed Pass: Yes Test Case ID: TC005 Input: Verify PKIIntegration **Expected Result**: PKIsecurely manages digital identities and communication channels. Actual Result: Passed 32 Pass: Yes Test Case ID: TC006 Input: TestBlockchain Ledger Integrity Expected Result:Blockchain ledger records and verifiessmart meter data while preserving privacy. Actual Result: Passed Pass: Yes Test Case ID: TC007 Input: Conduct PenetrationTesting Expected Result: No unauthorized accessis granted, and potential vulnerabilities are identified and addressed. Actual Result: Passed Pass: Yes Test Case ID: TC008 Input: PerformanceTesting under Peak Load Expected Result: System maintains performance metrics underpeak load conditions. 33 Actual Result: Passed Pass: Yes Test Case ID: TC009 Input: Check for Security Vulnerabilities Expected Result: No security vulnerabilities are detected. Actual Result: Passed Pass: Yes Test Case ID: TC010 Input: ValidateEnd-to-End Scenario Expected Result: Complete end-to-end scenarios, ensuring data transmission, noise injection,and blockchain ledger verification function correctly. Actual Result: Passed Pass: Yes Test Results: All testing phases were successful, with GridChain demonstrating robust functionality, effective privacy preservation, and strong security measures.

SYSTEM ARCHITECTURE

A system architecture or systems architecture is the conceptual model that defines the structure, behaviour, and more views of a system. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviours of the system. System architecture can comprise system components, the externally visible properties of those components, the relationships (e.g. the behaviour) between them. It can provide a plan from which products can be procured, and systems developed, that will work together to implement the overall system. There have been efforts to formalize languages to describe system architecture; collectively these are called architecture description languages (ADLs).



CONCLUSION

The rise of smart grids in power distribution has ushered in remarkable efficiency but also posed challenges in ensuring the security and privacy of consumer data within Advanced Metering Infrastructure (AMI). The "GridChain" project was conceived as a solution to these concerns, employing innovative technologies like hash functions, differential privacy, and blockchain. By utilizing hash functions, sensitive consumer information is safeguarded, and differential privacy techniques inject controlled noise into smart meter data, mitigating privacy breaches. The integration of PKI and a distributed blockchain ledger further fortify the system against re-identification attacks while reducing communication overhead. Achieving superior performance compared to predecessors, the project instils confidence in consumers, fostering trust in smart grid technologies and providing a reliable platform for energy providers. In essence, "GridChain" not only addresses current security and privacy challenges but also paves the way for a secure and privacy-preserving future in smart grid systems. The tangible benefits of the "GridChain" project extend beyond its technical advancements. It instils confidence in consumers regarding the security of their data, fostering trust in smart grid technologies. For energy providers and administrators, the solution offers a reliable and efficient platform for managing consumption data while adhering to stringent privacy standards.

I. ACKNOWLEDGMENT

We are grateful to Mrs. K.Sudha Devi, Assosiate Professor, CSE Department, Paavai Engineering College(Autonomous) for mentoring us to present this paper successfully

REFERENCES

[1] Alsharif, M. Nabil, S. Tonyali, H. Mohammed, M. Mahmoud, and K. Akkaya, ‘‘Epic: Efficient privacy-preserving scheme with etoe data integrity and authenticity for ami networks,’’ IEEE Internet of Things Journal, vol. 6, no. 2, pp. 3309–3321, 2019.
[2] B. M. Yakubu, M. I. Khan, A. Khan, A. Anjum, M. H. Syed and S. Rehman, "A privacy-enabled blockchain-based smart marketplace", Appl. Sci., vol. 13, no. 5, pp. 2914, Feb. 2023.

[3] H. Fan, Y. Liu, and Z. Zeng, ‘‘Decentralized privacy-preserving data aggregation scheme for smart grid based on blockchain,’’ Sensors, vol. 20, no. 18, p. 5282, 2020

[4Mohammadali and M. S. Haghighi, ‘‘A privacy-preserving homomorphic scheme with multiple dimensions and fault tolerance for metering data aggregation in smart grid,’’ IEEE Transactions on Smart Grid, vol. 12, no. 6, pp. 5212–5220, 2021.

[5] N. Ravi, A. Scaglione, S. Kadam, R. Gentz, S. Peisert, B. Lunghino, E. Levijarvi, and A. Shumavon, ‘‘Differentially private k-means clustering applied to meter data analysis and synthesis,’’ IEEE Transactions on Smart Grid, vol. 13, no. 6, pp. 4801– 4814, 2022.