PRIVACY-PRESERVING ELECTRICITY THEFT DETECTION BASED ON BLOCK-CHAIN

TIRUMALA SITARAM,

PG STUDENT ,DEPT OF MCA

MR. NAGA SRINIVASA RAO

Asst. Prof, Dept of MCA

SREE KONASEEMA BHANOJI RAMARS P.G. COLLEGE (AMALAPURAM)

Abstract- In most electricity theft detection schemes, consumers' power consumption data is directly input into the detection center. Although it is valid in detecting the theft of consumers, the privacy of all consumers is at risk unless the detection center is assumed to be trusted. In fact, it is impractical. Moreover, existing schemes may result in some security problems, such as the collusion attack due to the presence of a trusted third party, and malicious data tampering caused by the system operator (SO) being attacked. Aiming at the problems above, we propose a block-chain based privacy-preserving electricity theft detection scheme without a third party. Specifically, the proposed scheme uses an improved functional encryption scheme to enable electricity theft detection and load monitoring while preserving consumers' privacy; distributed storage of consumers' data with block-chain to resolve security problems such as data tampering, etc. Meanwhile, we build a Hash code model to perform higher accuracy for electricity theft detection. The proposed scheme is evaluated in a real environment, and the results show that it is more accurate in electricity theft detection within acceptable communication and computational overhead. Our system analysis demonstrates that the proposed scheme can resist various security attacks and preserve consumers' privacy.

Keywords: . ITS-G5, C-V2X, LTE, 5G and, in the future, 6G)

I. INTRODUCTION

SMART grid (SG) is an advanced grid integrating smart technology, which uses smart meters (SMs) to collect, analyze and process fine-grained power consumption data from consumers to manage energy effectively [1]. While the smart grid brings convenience, it also brings serious challenges [2]. For one thing, the communication of the smart grid is exposed to potential malicious attacks, such as data tampering attack and false data injection. If these malicious attacks cannot be resisted, the smart grid will be unable to operate normally [3]. For another thing, electricity theft has become a wide spread phenomenon in the smart grid. Annual economic losses due to electricity theft are estimated to be about 170 million dollars in the United Kingdom [4] and 6 billion dollars in the United States [5]. Meanwhile, electricity theft can also seriously affect energy management and endanger the normal operation of the smart grid [6].

Since the smart grid has access to consumers' fine-grained power consumption data, the traditional machine learning model [7] and deep learning model [8] based on big data have achieved good performance. However, directly giving fine-grained power consumption data of consumers to the SO raises serious privacy issues [9]. Meanwhile, as the security and privacy of data are becoming more and more concerned, related laws and regulations have been proposed, such as the General Data Protection Regulations (GDPR) in Europe, and the utilities' disregard for privacy aspects could lead to strong consumer objection and significant curtailment of service deployment [10]. Therefore, there is an urgent demand for a privacy-preserving electricity theft detection scheme.

i i RELATED WORK

A literature survey on "Sec-Health," a blockchain-based protocol for securing health records, would involve reviewing existing research, publications, and projects related to blockchain technology in healthcare data management. Here's a general outline of what such a survey might cover:

1. Introduction to Blockchain in Healthcare:

Provide an overview of how blockchain technology is being explored and utilized in the healthcare sector to address security, privacy, and interoperability challenges.

2. Existing Solutions and Protocols:

Survey the existing blockchain-based solutions and protocols designed for securinghealth records. This may include systems implemented in various healthcare settings, such as hospitals, clinics, and research institutions.

3. Key Challenges and Limitations:

Discuss the challenges and limitations faced by current blockchain-based healthcare systems, such as scalability issues, regulatory concerns, interoperability barriers, and the need for efficient consensus mechanisms.

4. Proposed Solutions and Innovations:

Highlight recent research papers, projects, and proposals that aim to enhance the security, privacy, and usability of blockchain-based healthcare systems. This could include novel consensus algorithms, privacy-preserving techniques, interoperability standards, and governance models.

5. Case Studies and Use Cases:

Examine real-world case studies and use cases of blockchain technology being applied in healthcare settings. Analyze the benefits, drawbacks, and lessons learned from these implementations.

6. Evaluation and Comparative Analysis:

Provide a critical evaluation and comparative analysis of different blockchain-based protocols for securing health records. Compare their technical features, performance metrics, security guarantees, and adoption challenges.

7. Future Directions and Research Opportunities:

Identify emerging trends, potential areas for improvement, and future research directions in the field of blockchain-based healthcare systems. Discuss how advancements in

blockchain technology, such as sharding, zero-knowledge proofs, and federated learning, could beleveraged to address existing limitations.

Summarize the key findings from the literature survey and highlight the importance ofcontinued research and development in blockchain-based protocols for securing health records.

By conducting a comprehensive literature survey, researchers and practitioners can gain valuable insights into the current state-of-the-art, identify gaps in knowledge, and inform the design and implementation of innovative solutions for securing health records using blockchain technology.

III METHODOLOGY

Admin

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such as Login, View All User, View All Datasets, View All Electricity Theft Detection By Block chain, View Electricity Theft Detection Type Results, View Consumer Age Results, View Gender Type Results.

View and Authorize Users

In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

User

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like Register and Login, View Profile, Encrypt and Upload Datasets, Find Electricity Theft Detection Type Results, Find Electricity Theft Detection Type By Hash code,

IV PROPOSE SYSTEM & IMPLEMENTATION

The system proposed Sec-Health, a protocol that secures health records by addressing all of their properties. In essence, Sec-Health is composed of a set of schemes, based on decentralized approaches (e.g., blockchain and InterPlanetary File System [10]) and cryptographic primitives (e.g., Ciphertext-Policy Attribute-based Encryption [11] and public key encryption), which allow records to be stored and shared securely. Sec-Health fills the gap of the literature that lacks integrated approaches which fulfill all health records properties. It overcomes the security problems of proposals based on centralized servers and presents advantages over other decentralized solutions by covering not only the most addressed properties of health records (confidentiality, access control, and integrity), but also more challenging ones (e.g., emergency access, access revocation, and anonymity).

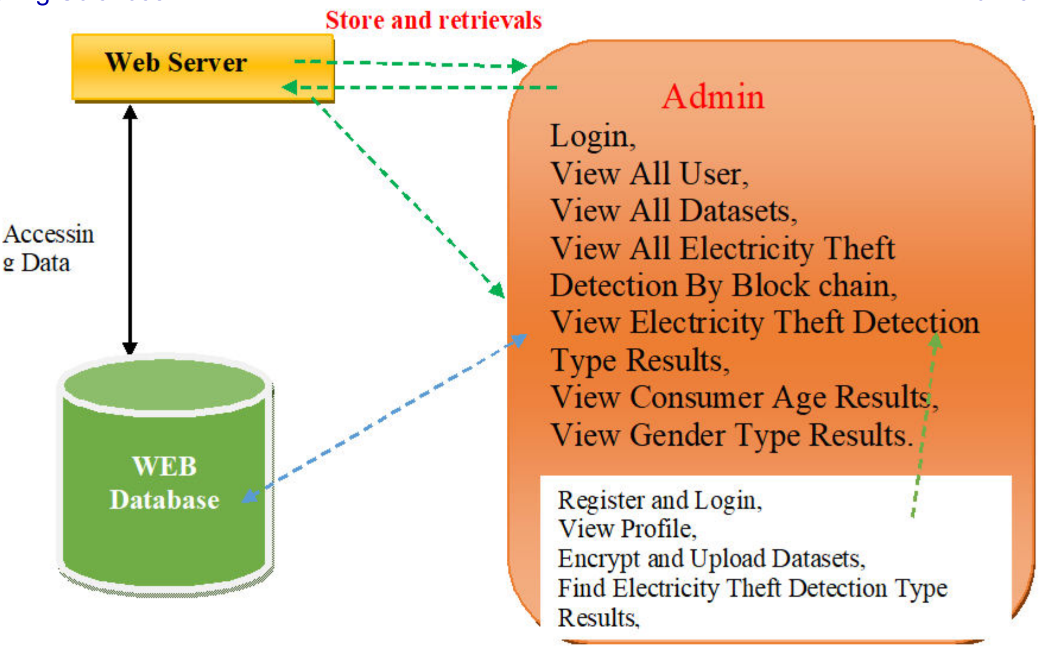
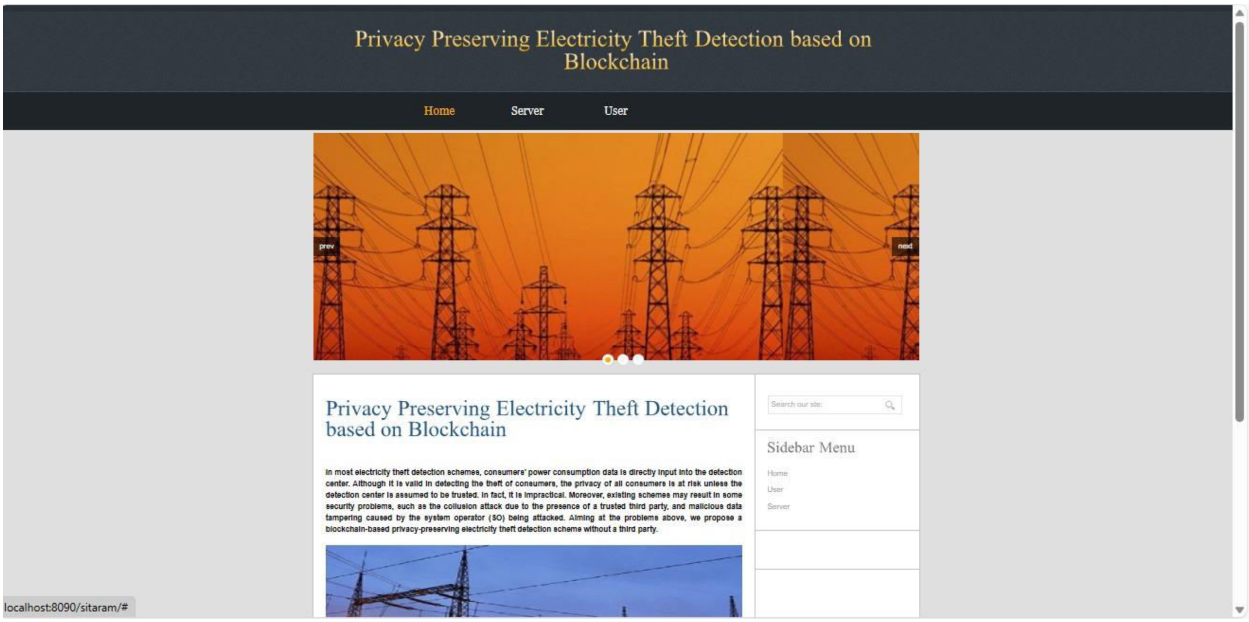

Store and retrievals
Web Server
Accessin
g Data
WEB
Database
Admin
Login,
View All User,
View All Datasets,
View All Electricity Theft
Detection By Block chain,
View Electricity Theft Detection
Type Results,
View Consumer Age Results,
View Gender Type Results.
Register and Login,
View Profile,
Encrypt and Upload Datasets,
Find Electricity Theft Detection Type
Results,

Figure 1: Proposed system architecture

V RESULT ANALYSIS

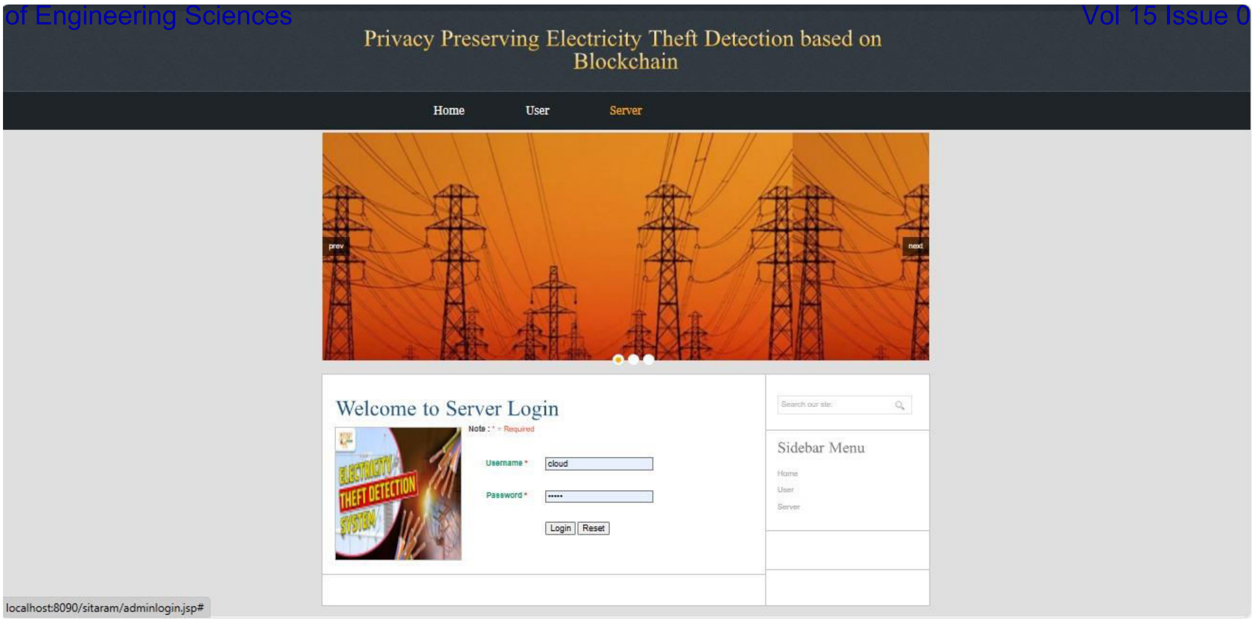
6.2.1 HOME PAGE



Privacy Preserving Electricity Theft Detection based on Blockchain

In most electricity theft detection schemes, consumers' power consumption data is directly input into the detection center. Although it is valid in detecting the theft of consumers, the privacy of all consumers is at risk unless the detection center is assumed to be trusted. In fact, it is impractical. Moreover, existing schemes may result in some security problems, such as the collusion attack due to the presence of a trusted third party, and malicious data tampering caused by the system operator (SO) being attacked. Aiming at the problems above, we propose a blockchain-based privacy-preserving electricity theft detection scheme without a third party.

6.2.2 SERVER LOGIN PAGE



Privacy Preserving Electricity Theft Detection based on Blockchain

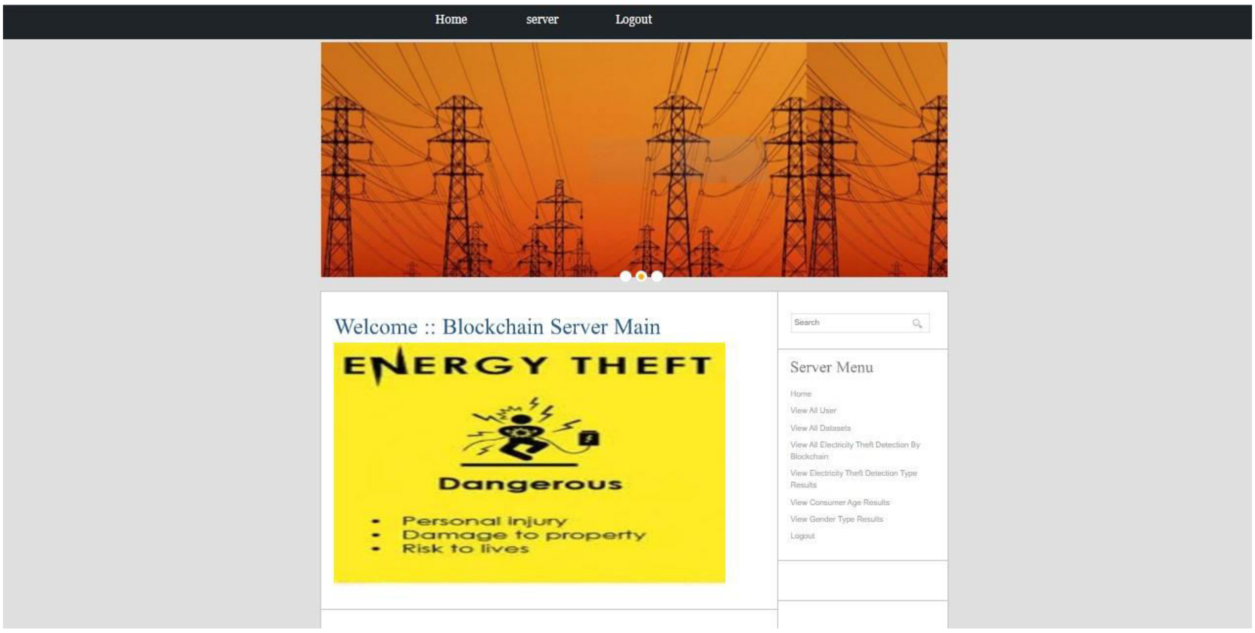
Welcome to Server Login

Note : * = Required

Username * cloud

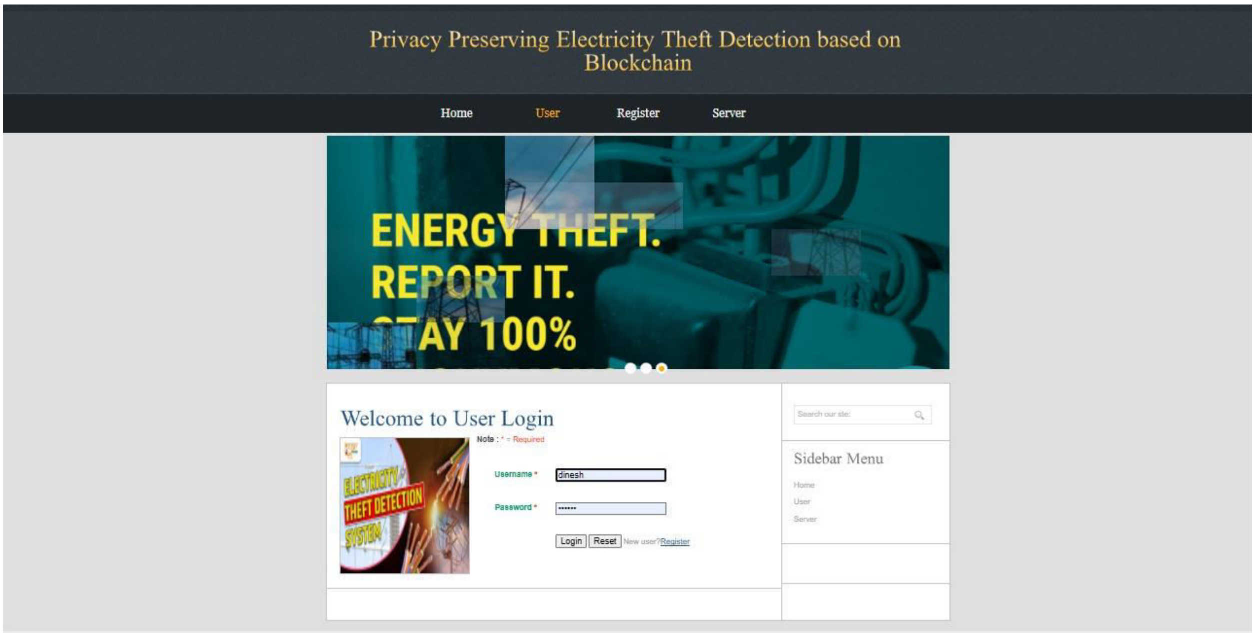
Password * •••••

6.2.3 SAEVER HOME PAGE



Welcome :: Blockchain Server Main

6.2.4 USER LOGIN PAGE



Privacy Preserving Electricity Theft Detection based on Blockchain

Welcome to User Login

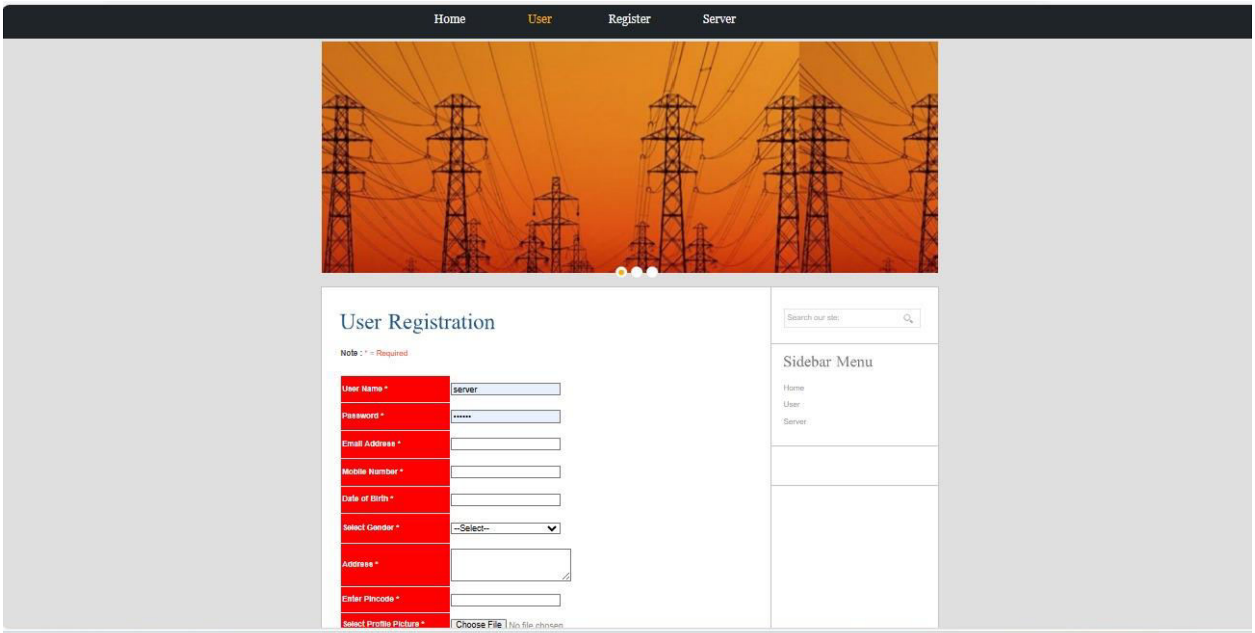
Note : * = Required

Username * dinesh

Password * ••••••

New user?Register

6.2.5 USER REGISTRITIOMN PAGE

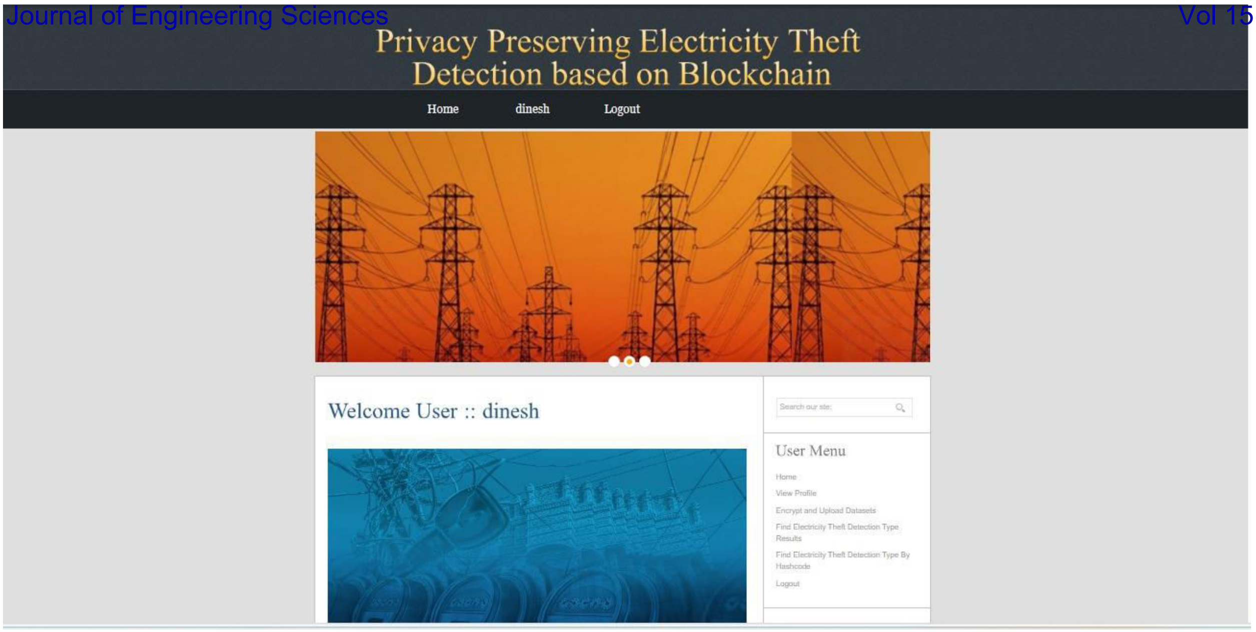


User Registration

Note : * = Required

User Name *	server
Password *	••••••
Email Address *	
Mobile Number *	
Date of Birth *	
Select Gender *	--Select--
Address *	
Enter Pincode *	
Select Profile Picture *	Choose File No file chosen

6.2.5 USER HOME PAGE



Privacy Preserving Electricity Theft Detection based on Blockchain

Welcome User :: dinesh

Home
dinesh
Logout
Search our site
User Menu
Home
View Profile
Encrypt and Upload Datasets
Find Electricity Theft Detection Type Results
Find Electricity Theft Detection Type By Hashcode
Logout

VI CONCLUSION

In this paper, we propose a more secure block chain based privacy-preserving electricity theft detection scheme. The proposed scheme does not require a third party, which avoids the security and privacy issues brought about by a third party. Meanwhile, the distributed storage scheme of block chain prevents security issues such as data tampering and forgery. In addition, a real dataset and environment are used for simulation evaluation. The experimental results show that the proposed scheme can detect malicious consumers more accurately with acceptable communication and computational overhead.System analysis shows that the proposed scheme is more secure compared to existing schemes. For our future work, we intend to improve the proposed scheme by reducing communication and computation overhead

VII REFERENCES

[1] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke, “A survey on smart grid potential applications and communication requirements,” IEEE Transactions on industrial informatics, vol. 9, no. 1, pp. 28–42, 2012.

[2] Y. Wang, Q. Chen, T. Hong, and C. Kang, “Review of smart meter data analytics: Applications, methodologies, and challenges,” IEEETransactions on Smart Grid, vol. 10, no. 3, pp. 3125–3148, 2018.

3] Z. Zeng, X. Wang, Y. Liu, and L. Chang, “Msda: multi-subset data aggregation scheme without trusted third party,” Frontiers of Computer Science, vol. 16, no. 1, pp. 1–7, 2022.

[4] X. Xia, Y. Xiao, and W. Liang, “Sai: A suspicion assessment-basedinspection algorithm to detect malicious users in smart grid,” IEEE Transactions on Information Forensics and Security, vol. 15, pp. 361–374, 2019.

[5] P. McDaniel and S. McLaughlin, “Security and privacy challenges in th smart grid,” IEEE security & privacy, vol. 7, no. 3, pp. 75–77, 2009.

[6] P. Gope and B. Sikdar, “Privacy-aware authenticated key agreementscheme for secure smart grid communication,” IEEE Transactions on Smart Grid, vol. 10, no. 4, pp. 3953–3962, 2018.

[7] P. Jokar, N. Arianpoo, and V. C. Leung, “Electricity theft detection in ami using customers’ consumption patterns,” IEEE Transactions on Smart Grid, vol. 7, no. 1, pp. 216–226, 2015.

[8] Z. Zheng, Y. Yang, X. Niu, H.-N. Dai, and Y. Zhou, “Wide and deep neural networks for electricity-theft detection to secure grids,” IEEE Transactions on Industrial Informatics, vol. 14, no. 4, pp. 1606–1615, 2017.