SECURE ACCESS CONTROL WITH ABE SCHEME IN BLOCKCHAIN

[1]Dr.B. SRINIVAS RAO, [2]SHAIK ZAHEER, [3]G. SHIVA, [4]P. VEERESH

[1](Professor) ,**CSE.** Teegala Krishna Reddy Engineering College Hyderabad

[234]B,tech scholar ,**CSE.** Teegala Krishna Reddy Engineering College Hyderabad

ABSTRACT

The Internet of Things (IoT) has witnessed widespread adoption across various domains in recent years, significantly impacting our daily lives. As the IoT continues to proliferate, ensuring its security becomes paramount. However, numerous security challenges persist, rendering IoT vulnerable to potential threats. In this paper, we present a novel secure access management scheme for IoT based on blockchain technology, addressing these critical security concerns.Our approach begins by introducing a robust Key-policy Attribute-based Encryption (KP-ABE) scheme, leveraging the Decisional Learning with Error (DLWE) problem. This scheme enables fine-grained access control within IoT environments, enhancing overall security measures. Subsequently, we integrate blockchain technology to tackle authentication and access management challenges effectively. The use of blockchain introduces a decentralized and tamper-resistant framework, ensuring trust and transparency in IoT transactions.

Furthermore, our scheme leverages smart contracts within the blockchain network. Smart contracts automate transaction processing, significantly reducing management costs and operational time associated with access control in IoT systems.To validate the efficacy of our proposed scheme, we conduct a comprehensive security analysis. The results demonstrate the scheme's resilience against common IoT attacks, affirming its robustness and efficiency in securing IoT environments.

In summary, our proposed secure access management scheme offers a holistic approach to IoT security, combining KP-ABE for fine-grained access control and blockchain technology for authentication and transaction management. This integrated solution not only enhances security but also improves operational efficiency, making it well-suited for diverse IoT applications.

1.INTRODUCTION

The Internet of Things (IoT) has evolved into a pivotal technological concept with widespread practical applications since its inception by MIT's Automatic Identification Center in 1999. Initially described as a fusion of Radio Frequency Identification (RFID) and sensor technologies, IoT has matured to encompass sensor networks and intelligent devices, revolutionizing data capture and analysis for heightened operational efficiency and cost-effectiveness.

Despite these advancements, IoT faces formidable security challenges. Reliance on Internet Protocol (IP) and integration of technologies like Wireless Sensor Networks (WSN), Machine-to-Machine (M2M) communication, and Cyber-Physical Systems (CPS) introduce vulnerabilities demanding meticulous attention. Inadequate encryption, authentication mechanisms, and access control protocols, compounded by outdated software versions, render these systems susceptible to cyber threats.

The emergence of blockchain technology in 2008 introduced a paradigm shift in decentralized and secure data management. Leveraging cryptographic primitives and consensus mechanisms, blockchain ensures data integrity and security within a distributed network, garnering significant interest for fortifying IoT security.

Our researchfocuses on integrating blockchain with IoT, introducing a pioneering Key-policy Attribute-based Encryption (KP-ABE) framework for robust access control. Our contributions include:

1. Proposing a lattice-based KP-ABE scheme for fine-grained access control in IoT.
2. Developing a secure access management protocol using blockchain for trustworthy authentication.
3. Conducting a rigorous security analysis against prevalent IoT threats.

Our novel methodology not only enhances IoT security but also facilitates the secure transmission of IoT data between users, streamlining deployment and ownership transfers of smart devices, and mitigating common security risks.

PROBLEM STATEMENT:

The increasing complexity and scale of IoT deployments have underscored the critical need for an access control mechanism that not only meets stringent security requirements but also operates with heightened efficiency and precision. This imperative arises from the inherent challenges posed by the burgeoning number of IoT devices and users, necessitating a paradigm shift towards a more sophisticated and fine-grained access control

framework. To achieve this, it is imperative to integrate advanced technologies such as secure lattice-based Key-policy Attribute-based Encryption (KP-ABE) scheme techniques and blockchain for authentication and access management. These cutting-edge solutions offer enhanced security measures while minimizing overhead and redundancy, thereby addressing the evolving security landscape of IoT environments. Moving away from traditional centralized access control methods becomes essential in this context, as they struggle to cope with the dynamic nature and sheer volume of IoT devices and users, highlighting the urgency and significance of adopting a more decentralized and efficient approach to access control in IoT ecosystems.

1.2 Description:

A more efficient and fine-grained access control mechanism in IoT is achieved by combining a secure Key-policy Attribute-based Encryption (KP-ABE) scheme with blockchain technology. This lattice-based KP-ABE scheme supports flexible access policies and robust privacy protection, facilitating fine-grained access control within IoT environments. Integration with blockchain enhances authentication and access management, ensuring secure identity verification and data integrity. A comprehensive security analysis validates the effectiveness of this approach against common IoT attacks, providing scalability and mitigating security risks while addressing challenges in ownership transfer for smart devices, thus offering a robust and efficient access control mechanism for IoT.

2.LITERATURE SURVEY

The rapid evolution of the Internet of Things (IoT) has ushered in a new era of technological advancement, integrating diverse devices and sensors to optimize efficiency and cost-effectiveness across various sectors. However, this expansion has also exposed IoT systems to significant security vulnerabilities. Traditional access control mechanisms such as role-based access control (RBAC), attribute-based access control (ABAC), and usage control (UCON) have proven inadequate in meeting the dynamic and complex security needs of IoT environments. As a result, there is a growing emphasis on pioneering security strategies capable of delivering precise access control and robust authentication mechanisms. Blockchain's decentralized and immutable nature presents opportunities to fortify authentication, access control, and data integrity within IoT infrastructures. Research endeavors have explored blockchain-based solutions for securing access management in IoT, encompassing innovative frameworks based on smart contracts, decentralized RBAC models, and permission attribute-based access control frameworks.

Another pivotal aspect of IoT security enhancement revolves around attribute-based encryption (ABE) schemes. ABE offers a granular approach to access control, leveraging attributes such as user roles and device characteristics to bolster privacy and security in IoT communications. Recent advancements have seen the development of robust lattice-based ABE schemes, leveraging cryptographic methodologies like the Decisional Learning with Error (DLWE) problem to elevate security and privacy standards.

The integration of blockchain technology with secure ABE schemes presents a compelling strategy to tackle the multifaceted security challenges in IoT comprehensively. By amalgamating blockchain for authentication and access management with secure ABE schemes for fine-grained access control, researchers aim to elevate the overall security, privacy, and operational efficiency of IoT systems. These endeavors entail rigorous security assessments to gauge the efficacy of these integrated solutions in thwarting common IoT threats while safeguarding data confidentiality, integrity, and availability. In essence, the literature underscores the burgeoning significance of cutting-edge security methodologies, such as blockchain-driven authentication and secure ABE schemes, in confronting the evolving security landscape within IoT environments. These integrated solutions hold promise in delivering enhanced security, fortified privacy measures, and resilience against cyber threats in IoT ecosystems.

3.SYSTEM DESIGN

3.1 SYSTEMARCHITECTURE

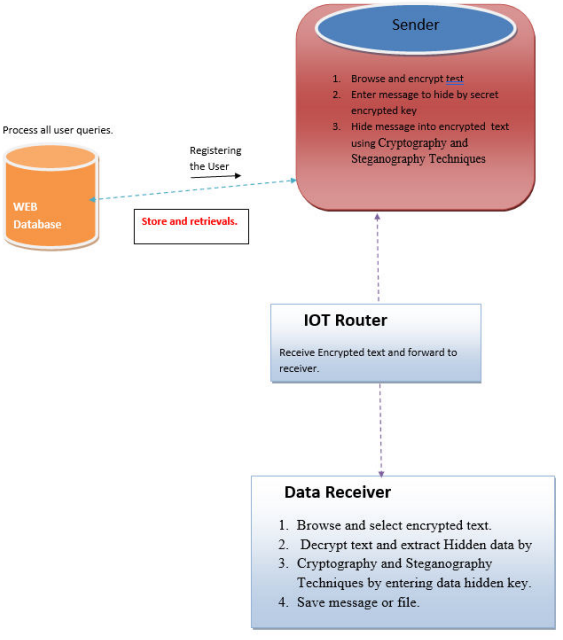

Fig 3.1System Architecture

The above description outlines a comprehensive process of secure communication using cryptography and steganography techniques within an IoT context. The core of this system

is the WEB Database, which processes user queries and manages data storage and retrieval during the user registration process. The Sender component initiates secure communication by selecting and encrypting the text message using robust cryptographic algorithms. The sender then embeds a hidden message within the encrypted text, enhancing security through a combination of cryptography and steganography techniques. The IOT Router acts as an intermediary, receiving and routing the encrypted text to the Data Receiver module for decryption.

The Data Receiver module decrypts the received text and extracts the hidden message using cryptographic techniques. Once decrypted, the message or file is securely saved, completing the communication cycle. This secure communication method addresses the critical need for privacy and security in IoT devices, safeguarding data from unauthorized access and ensuring communication integrity. The integration of cryptography and steganography enhances data protection, making it suitable for applications where data confidentiality is essential.

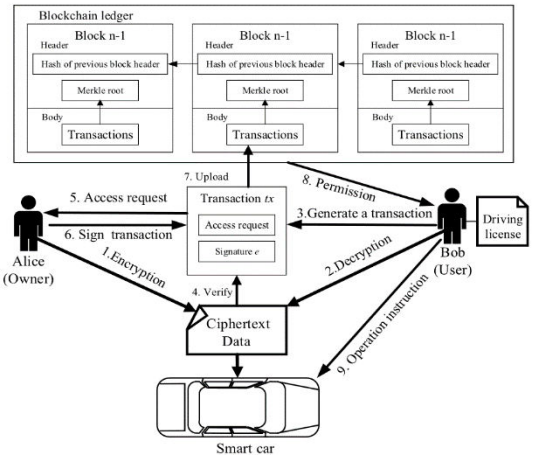

Fig 3.1.2 System Architecture

The image illustrates a blockchain-based access control process for a smart car, ensuring secure and transparent management of access permissions. The blockchain ledger, consisting of interconnected blocks with transaction details like access requests and operational instructions, maintains data integrity through cryptographic hashing and chain linking mechanisms. Users interact with the blockchain by initiating access request transactions, which are encrypted, signed, and permanently recorded on the ledger.

Upon receiving permission via the blockchain network, users can generate transactions containing decryption keys and operational instructions for accessing and operating IoT devices like smart cars. This process promotes transparency and trust, enabling secure data sharing between IoT devices and authorized users while minimizing risks associated with unauthorized access.Overall, the blockchain-based access control system depicted in the image provides a robust framework for managing access permissions in IoT devices, enhancing security, transparency, and data sharing capabilities.

3.2 ACTIVITYDIAGRAM

The activity diagram illustrates a step-by-step process for handling authentication, encrypting and decrypting messages or images, and managing failed login attempts in a secure system.

The process begins with users attempting to log in, where their credentials are checked against stored data for authentication. If the credentials are correct, users proceed to encrypt messages or images, which can then be securely sent or stored. On the other hand, if the login attempt fails, users are given the option to retry logging in. If repeated attempts fail, the process ends.

The diagram includes decision nodes to handle successful and failed login scenarios, ensuring that only authenticated users can access encryption and decryption functionalities. It also incorporates flow control elements like fork/join nodes for parallel processes and swim-lanes to differentiate actions by different roles or systems.

Overall, the activity diagram provides a clear visual representation of the secure data handling process, emphasizing the importance of authentication in maintaining data confidentiality and integrity.

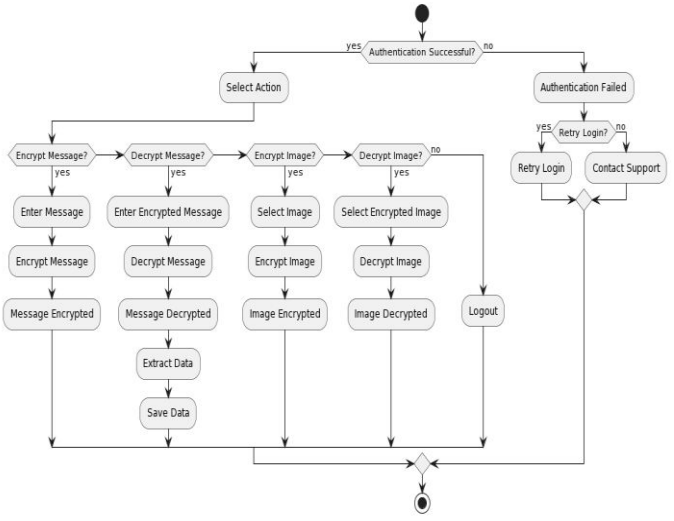

Fig 3.2 Represents Activity Diagram

4.OUTPUT SCREENS

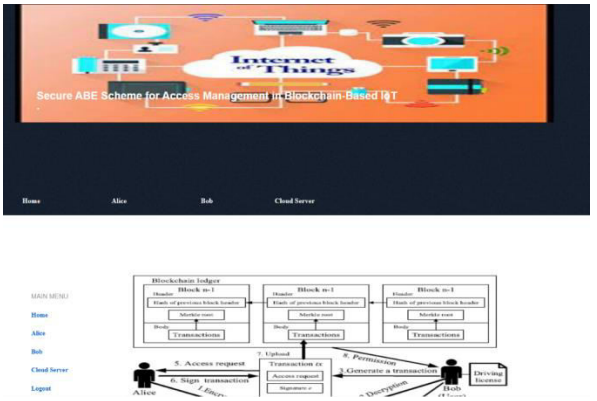

Fig 4.1RepresentsUser Home Screen

This is the basic user view while entering the website.

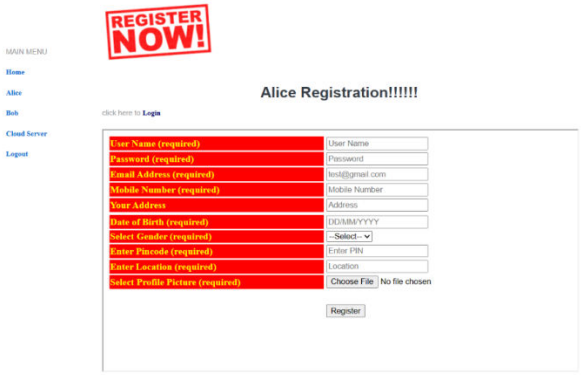

Fig 4.2 RepresentsOwnerand User RegistrationScreen

Owner and user can register using their credentials.

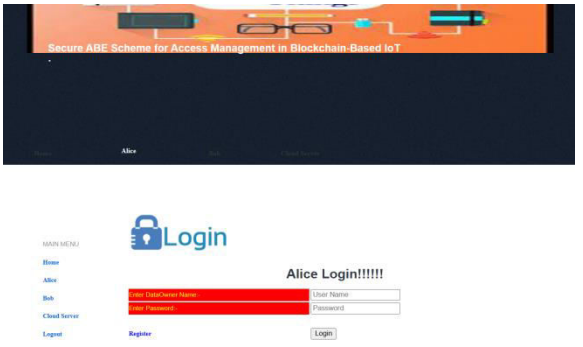

Fig 4.3: Represents Owner Login Screen

Owner can login using their credentials.

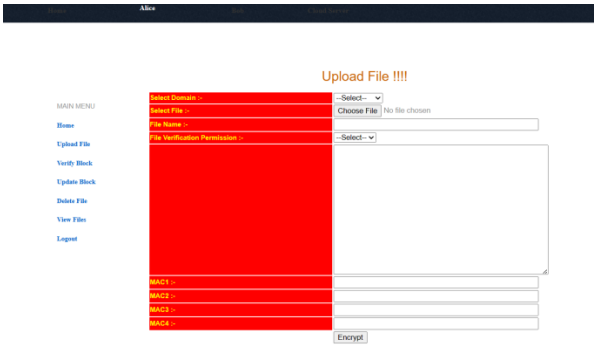

Fig 4.4: File Uploading

The owner will add the data which he wants to encrypt

Fig 4.5: Block of Encrypted Data .

The data provided by the owner is encrypted and the encrypted data is in blocks

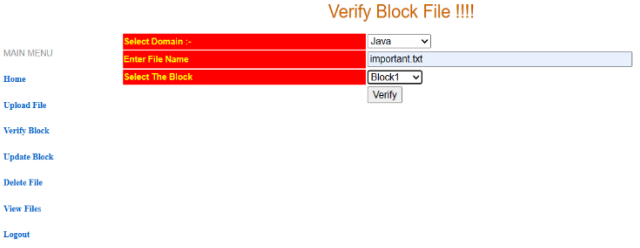

Fig 4.6: Blocks of Encrypted Data

After encrypting the data we can view the encrypted data which is stored in block format.

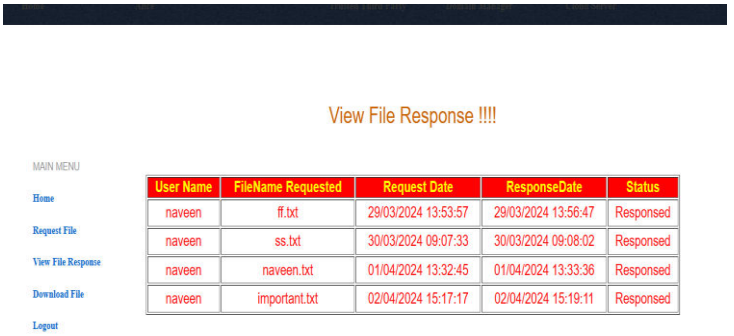

Fig 4.7 : File Response

. The file requested is responded by the admin .

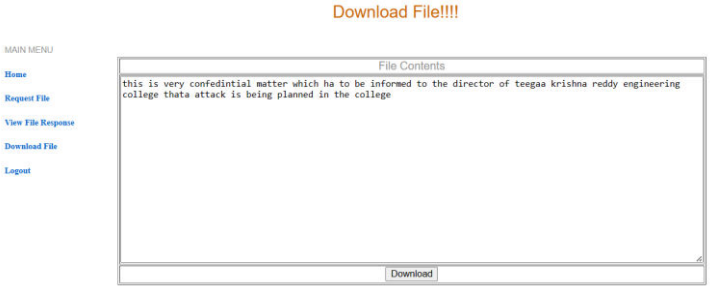

Fig 4.8: Downloading file (Decrypted).

After decrypting the file the user can now download the file.

Fig 4.9 : List of Users.

The list of users can be viewed here .

Fig 4.10 :Represents the list of files.

The files list can be viewed here

5. CONCLUSION

In conclusion, the dynamic realm of IoT, security isn't just a concern; it's a paramount necessity. With the proliferation of connected devices projected to exceed 50 billion by 2020, the urgency for robust security measures has never been more palpable. This is where our innovative approach steps in, combining cutting-edge technologies like KP-ABE and blockchain to forge a formidable shield around IoT ecosystems.At the core of our strategy is fine-grained access control powered by KP-ABE, ensuring that only authorized entities navigate the IoT landscape. Leveraging blockchain's immutable ledger, we establish a fortress of data security, impervious to tampering and unauthorized access attempts. Our authentication protocols, fortified by blockchain's signature verification, guarantee the sanctity of communications within IoT networks.But we don't stop there. Our scheme integrates smart contract functionalities, ushering in a new era of efficiency and security in transaction processing. This strategic augmentation not only streamlines operations but also bolsters the overall security posture of IoT systems.Through rigorous analysis and testing, our approach has not only proven its security prowess but also showcased unmatched efficiency when compared to traditional methods. As we chart the course forward, our unwavering focus remains on navigating the ever-evolving cybersecurity landscape of IoT, ensuring seamless access management and data sharing for a safer digital future.

6.FUTURE ENHANCEMENTS

Implementing a machine learning-based IDS can significantly enhance the project's security posture. By training the system on historical data and real-time network behavior, the IDS can autonomously detect and respond to potential threats, including DDoS attacks and unauthorized access attempts. This proactive approach not only strengthens the system's resilience but also

reduces the response time to security incidents, thereby mitigating risks effectively.

Enhancing authentication mechanisms with MFA adds an extra layer of security by requiring users to provide multiple forms of verification, such as biometric data, one-time passwords, or hardware tokens. Integrating MFA into the project can thwart unauthorized access attempts even if credentials are compromised, bolstering the overall security framework and ensuring secure access management within IoT environments.

Strengthening data encryption protocols and implementing robust privacy measures can further fortify the project's security. Adopting advanced encryption algorithms and techniques like homomorphic encryption or differential privacy ensures that sensitive data remains protected both in transit and at rest. Additionally, incorporating data anonymization techniques minimizes privacy risks and enhances user trust by safeguarding personal information.

11. REFERENCES

[1] G. Zyskind, O. Nathan, and A. S. Pentland, ``Decentralizing privacy: Using blockchain to protect personal data," in Proc. IEEE Secure Privacy Workshops, San Jose, CA, USA, May 2015, pp. 180_184, doi: 10.1109/SPW.2015.27.

[2] M. Hamilton, ``Blockchain distributed ledger technology: An introduction and focus on smart contracts," J. Corporate Accounting Finance, vol. 31, no. 2, pp. 7_12, Apr. 2020.

[3] J. Huang, L. Kong, G. Chen, M.-Y. Wu, X. Liu, and P. Zeng, ``Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism," IEEE Trans. Ind. Informat, vol. 15, no. 6, pp. 3680_3689, Jun. 2019.

[4] A. Abidi, B. Bouallegue, and F. Kahri, ``Implementation of elliptic curve digital signature algorithm (ECDSA)," in Proc. Global Summit Compute. Inf. Technol. (GSCIT), Jun. 2014, pp. 1_6.

[5] Z. Li, Z. Yang, and S. Xie, ``Computing resource trading for edge-cloud-assisted Internet of Things," IEEE Trans. Ind. Informat, vol. 15, no. 6, pp. 3661_3669, Jun. 2019.

[6] F. Chang, J. Dean, S. Ghemawat, W. C. Hsieh, D. A.Wallach, M. Burrows, T. Chandra, A. Fikes, and R. E. Gruber, ``Bigtable: A distributed storage system for structured data," ACM Trans. Comput. Syst., vol. 26, no. 2, pp. 1_26, Jun. 2008.

[7] K. Christidis and M. Devetsikiotis, ``Blockchains and smart contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292_2303, 2016.

[8] C. Li and L.-J. Zhang, ``A blockchain based new secure multi-layer network model for Internet of Things," in Proc. IEEE Int. Congr. Internet Things (ICIOT), Honolulu, HI,

USA, Jun. 2017, pp. 33_41, doi: 10.1109/IEEE.ICIOT.2017.34.

[9] S. Huh, S. Cho, and S. Kim, ``Managing IoT devices using blockchain platform," in Proc. 19th Int. Conf. Adv. Commun. Technol. (ICACT), Bongpyeong, South Korea, 2017, pp. 464_467, doi: 10.23919/ICACT.2017.7890132.

[10] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, ``Role-based access control models," Computer, vol. 29, no. 2, pp. 38_47, 1996.

[11] V. C. Hu, D. R. Kuhn, and D. F. Ferraiolo, “Attribute-based access control” Computer, vol. 48, no. 2, pp. 85_88, Feb. 2015.