International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

SECURE MULTI-AUTHORITY KEY-POLICY ATTRIBUTE-BASED ENCRYPTION WITH ECC INTEGRATION

VANGALA SWATHI [1], GADDAMEEDI HASINI [2], ANNU ANSIKA REDDY [3], ANGAJALA KISHORE [4], KERAVELLY ARSHITH REDDY [5]

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

ABSTRACT— The rapid and expansive integration of Internet of Things (IoT) environments across various industrial sectors has led to an unprecedented surge in data generation and management. This exponential growth in data underscores the critical necessity for robust data security methodologies that can effectively safeguard the confidentiality and integrity of information without imposing undue computational burdens. In response to this challenge, numerous studies have sought to leverage Attribute-Based Encryption (ABE) as a means to enable fine-grained access control. Among the ABE variants, Ciphertext Policy ABE (CP-ABE) and bilinear pairings have emerged as popular choices to construct security schemes that strike a balance between robust protection and computational efficiency. Despite the progress made through Ciphertext-Policy Attribute-Based Encryption (CP-ABE) and bilinear pairings, the use of Linear Secret Sharing Scheme (LSSS) access policies continues to pose challenges. Although LSSS policies offer flexible and expressive access control, they often lead to increased encryption execution times, impacting overall system performance. This study addresses this issue by investigating the potential of Key-Policy Attribute-Based Encryption (KP-ABE) as an alternative approach. The primary goal is to

reduce the computational burden during encryption, thereby improving the efficiency of data protection mechanisms within IoT environments. In addition, this research explores the integration of Elliptic Curve Cryptography (ECC) for key generation. Known for its strong security guarantees and computational efficiency, ECC presents a promising method to enhance data security while minimizing computational costs. By combining KP-ABE with ECC, the study aims to develop a holistic solution that delivers robust security alongside optimized performance tailored for the complexities of IoT systems. Through comprehensive analysis and empirical evaluation, this work seeks to contribute meaningful advancements to the ongoing efforts in securing IoT data, balancing the critical demands of both security and computational efficiency.

Index Terms – Internet of Things (IoT), data security, Attribute-Based Encryption (ABE), Key-Policy Attribute-Based Encryption (KP-ABE), Ciphertext-Policy Attribute-Based Encryption (CP-ABE), computational efficiency, secure data sharing.

I. INTRODUCTION

INERNET of Things (IoT) environments have gained a great deal of traction in recent years. Sectors such as healthcare, agriculture and power generation have adopted IoT environments to automate and improve their operations. However, one of the consequences of this is that IoT environments are also becoming larger, containing more devices which produce more data. This increase in data has increased the computational overhead of traditional data security methods used in IoT environments. Emphasis has been placed on developing low computationally intense INERNET of Things (IoT) environments have gained a great deal of traction in recent years. Sectors such as healthcare, agriculture and power generation have adopted IoT environments to automate and improve their operations. However, one of the consequences of this is that IoT environments are also becoming larger, containing more devices which produce more data This increase in data has increased the computational overhead of traditional data security methods used in IoT environments. Emphasis has been placed on developing low computationally intense ethods, as oppositions in data security are only improving. methods of ensuring data security. This includes attempting to decrease total execution time of data security procedures and reducing the text size of messages sent. There is also an emphasis on

creating more robust data security methods, as oppositions in data security are only improving. methods of ensuring data security. This includes attempting to decrease total execution time of data security procedures and reducing the text size of messages sent. There is also an emphasis on creating more robust data security methods, as oppositions in data security as digital signature schemes. One example of such a scheme is the work produced by C. Meshram et al. This scheme utilized one way hash functions and multi-variable signatures with extended chaos maps to provide provable security. This scheme outperformed other signature schemes in both signing execution time and verification time. These improvements are significant with a performance benefit of up to 8500ms in total execution time. All data security schemes in IoT systems must incorporate a public key infrastructure (PKI), as traditional symmetric key infrastructures are too unreliable in systems with as many entities as IoT systems. There have been attempts at creating hybrid structures which utilize symmetric and asymmetric methods, such as digital signature schemes. One example of such a scheme is the work produced by C. Meshram et al. This scheme utilized one way hash functions and multi-variable signatures with extended chaos maps to provide provable security. This scheme outperformed other signature schemes in both signing execution time and verification time. These improvements are significant with a performance benefit of up to 8500ms in total execution time. All data security schemes in IoT systems must incorporate a public key infrastructure (PKI), as traditional symmetric key infrastructures are too unreliable in systems with as many entities as IoT systems. There have been attempts at creating hybrid structures which utilize symmetric and asymmetric methods, such as digital signature schemes. One example of such a scheme is the work produced by C. Meshram et al. This scheme utilized one way hash functions and multi-variable signatures with extended chaos maps to provide provable security. This scheme outperformed other signature schemes in both signing execution time and verification time. These improvements are significant with a performance benefit of up to 8500ms in time and analysed, however, empirical analysis of the computation time of both constructions were not considered in the study. Only the theoretical analysis of both constructions was considered. However, the literature landscape has preferred the use of pure PKI, such as the work conducted by P. Liu. P. Liu

had researched the use of indistinguishability obfuscation and weak related key attack (RKA) secure one-way functions to ensure a scheme that is Related Randomness Attack (RRA) model secure. Two constructions were produced and analysed, however, empirical analysis of the computation time of both constructions were not considered in the study. Only the theoretical analysis of both constructions was considered.

II. RELATED WORK

A. Attribute-based encryption of LSSS access structure with expressive dynamic attributes based on consortium blockchain

Attribute-based encryption (ABE) allows users to encrypt and decrypt data based on attributes. It realizes fine-grained access control and can effectively solve the one-to-many encryption and decryption problem in open cloud application. Linear secret sharing scheme (LSSS) is the common access structure with a matrix on the attributes in ABE schemes, which may depict AND, OR, threshold operations, etc.

However, LSSS access structure does not depict the complex and dynamic access policy of attributes, such as the complicated relationship of different attributes and the generation of dynamic attributes. It severely restricts the expansion of the practical application of ABE. Besides, there exists another problem; attribute authority (AA) in traditional ABE has a concentration of power and easily suffers from single-point failure or privacy leakage for being attacked or corrupted. Blockchain is a decentralized, tamper-free, traceable, and multi-party distributed database technology.

Consortium blockchain (CB) is a partially centralized blockchain, whose openness is between the public blockchain and the private blockchain. In this paper, an ABE scheme on LSSS access structure with expressive dynamic attributes (EDA) based on CB (LSSS-EDA-ABE-CB) was proposed to resolve the above issues. EDA can construct the comprehensive attribute calculation expressions by conducting various operations, such as arithmetic operations, relational operations, and string operations. In virtue of the application of EDA, the proposed scheme can reconstruct new composite attributes to realize the dynamic adjustment of attributes. A partitioning method of EDA avoids one attribute appearing in two different EDA expressions.

The CB technology enhanced the authority and trustworthiness of AA by openly recording AA's attribute key distributions in

CB transactions. The scheme in the paper was proven CPA-secure under the decision q-PBDHE assumption in standard model in the CB application environment.

B. *Multiauthority CP-ABE-based Access Control Model for IoT-enabled Healthcare Infrastructure*

The exponential growth of the Internet of Things (IoT) technologies requires high data security. Here, data security is very critical as all IoT devices transfer data over the Internet. The fine-grained access control provided by the ciphertext policy attribute-based encryption (CP-ABE) technique can be considered as a potential solution to this issue. However, most of the CP-ABE schemes use bilinear pairing operations for its internal working, which is expensive for any resource constraint device. An elliptic curve cryptography (ECC) based CP-ABE scheme can be well suited for resource constraint IoT framework because ECC takes less computational time. This article proposes a novel CP-ABE technique based on ECC to achieve fine-grained access control over data or resources. The proposed technique includes multiple attribute authorities to manage attributes and key generation, which can reduce the work overhead of having a single authority in traditional CP-ABE systems. In addition, the proposed scheme outsources the decryption process to a user assistant entity to reduce the decryption overhead of the end-users. To prove the efficiency of the proposed scheme, both formal security analysis and performance comparisons are presented in this article. The result and findings prove the effectiveness of the proposed scheme over some well-known schemes.

C. *A Lightweight and Verifiable Access Control Scheme With Constant Size Ciphertext in Edge-Computing-Assisted IoT*

As an extension of cloud computing, edge computing has attracted the attention of academia and industry because of its characteristics of low latency, high bandwidth, and low energy consumption. However, due to limited terminal resources and insufficient security design, the edge computing environment still faces many challenges in terms of data security and privacy protection. Among them, how to effectively control access to outsourced data is one of the main issues. In this article, we propose a lightweight and verifiable ciphertext-policy attribute-based encryption (CP-ABE)-based multiauthority access control scheme for edge computing-assisted Internet of Things (IoT), which adopts the method of outsourcing decryption to mitigate

the computational cost of data users with limited resources. In addition, our scheme realizes the feature of attribute revocation, and the design of the multiauthority mechanism enables our scheme to avoid the problem of key escrow. Therefore, our proposed scheme not only ensures data confidentiality but also can resist the collusion attack. Besides, our scheme is secure against the chosen plaintext attack in the random oracle model under the decision q -BDHE assumption. Finally, we compared our scheme with some related work in performance, and the results demonstrate that our scheme is efficient in computation and communication. Because our scheme greatly mitigates the overhead of data users, it is very suitable for edge computing supported IoT applications with restricted computation resources.

D. Distributed and Privacy-Preserving Data Dissemination at the Network Edge via Attribute-Based Searchable Encryption

Multi-Access Edge computing represents one of the most important enabling technologies for the Industrial Internet of Things. It allows advanced data processing and customized service provisioning, very close to the end-users. In the presence of many Multi-Access Edge computing applications, however, it is fundamental to ensure effective and privacy-preserving data dissemination at the network edge. From the security perspective, Attribute-based Encryption and Searchable Encryption techniques can be jointly used to achieve data confidentiality, flexible protection against unauthorized access, and privacy-preserving data dissemination. Available solutions, however, generally focus the attention on cloud-based approaches, use edge computing to implement some of the cryptographic tasks, and limit the investigation to single cryptographic operations. Indeed, no works investigate the adoption of these techniques in scenarios with multiple data producers and end-users, and fully operating at the network edge. To bridge this gap, this work proposes a novel methodology supporting fast and privacy-oriented data dissemination directly at the network edge. In the considered distributed network infrastructure, Multi-Access Edge computing applications express the interest to receive specific data by sending Trapdoors to Edge Servers. Data sources protect their contents through Attribute-based Encryption and deliver them to Edge Servers. In turn, Edge Servers implement Attribute-based Searchable Encryption functionalities to properly disseminate received contents towards Multi-

Access Edge nodes hosting the applications that generated valid Trapdoors. The performance of the conceived approach has been evaluated through computer simulations.

Obtained results highlight the benefits achieved against baseline (i.e., cloud-based) solutions.

III. PROPOSED METHODOLOGY

To overcome these limitations, the proposed system introduces a combination of Key-Policy Attribute-Based Encryption (KP-ABE) and Elliptic Curve Cryptography (ECC). KP-ABE shifts the complexity from encryption to key management, potentially reducing encryption time. Meanwhile, ECC is employed for key generation due to its strong security features and lower computational demands compared to traditional cryptographic schemes. By integrating KP-ABE with ECC, the new system aims to deliver robust data security for IoT applications while significantly improving computational efficiency, making it well-suited for resource.

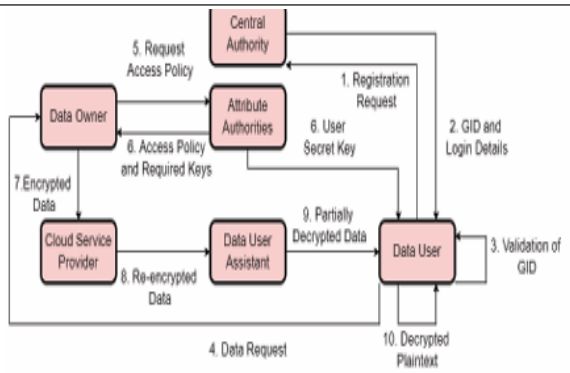
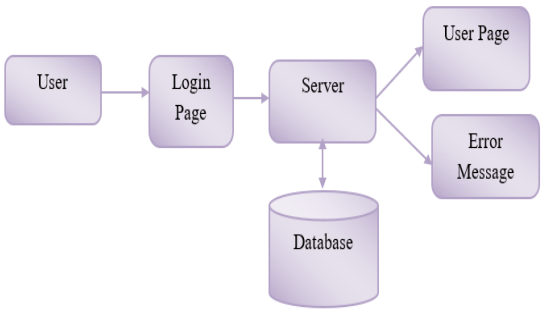


Fig. 1: System Overview

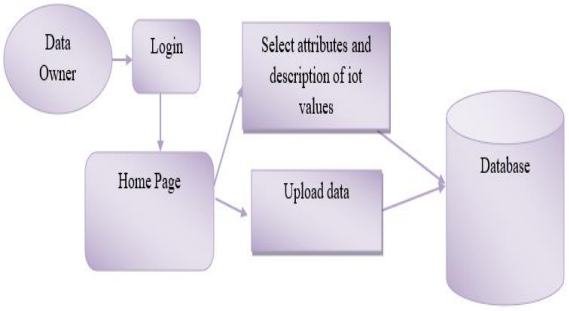
1. User Interface Design

To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password, Email id, City and Country into the server. Database will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page. It will search the query and display the query.



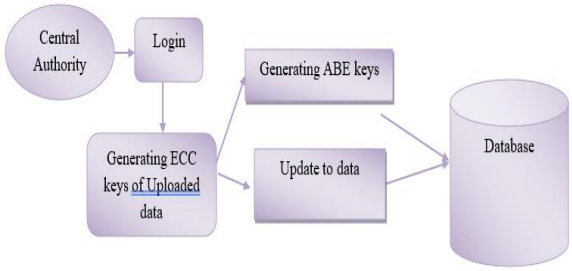
2. Data (Data Upload)

This module allows Data Owners to simulate the upload of sensitive IoT data through a web form. While uploading, users can assign access attributes (e.g., "sensor values", "temperature values") that define who should be able to access the data. The uploaded file is then passed through the encryption engine for secure storage.



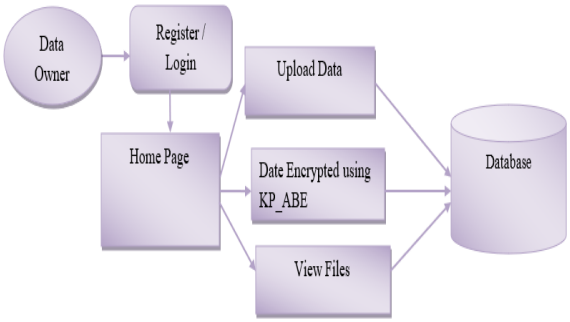
3. Key Authority (Admin Panel)

The Central Authority (CA) manages this panel and is responsible for defining valid attributes, generating KP-ABE keys, and assigning them to Data Users based on eligibility. The admin can approve requests, issue ECC keys, and enforce fine-grained access control policies.



4. Encryption Engine

This module handles the data encryption process using a hybrid approach that combines Elliptic Curve Cryptography (ECC) and Key-Policy Attribute-Based Encryption (KP-ABE). It ensures that data is protected at rest and can only be accessed by users holding matching attribute-based keys.



5. Decryption Engine

Located within the Data User module, this engine checks whether the user's KP-ABE key satisfies the access policy tied to the encrypted file. If matched, it uses the ECC key to securely decrypt and download the original file content, ensuring confidentiality and controlled access.



6. JSP Dashboard

A dynamic interface for each role—CA, CSP, Data Owner, and Data User—that displays current activities such as uploaded files, approval status, encrypted data lists, and key assignments. It also includes status indicators for access control policy matches and downloads.

7. MySQL Database

This is the system's central storage that holds all critical information—encrypted files, file metadata, attribute sets, keys, user registrations, access logs, and transaction statuses. It ensures seamless data retrieval, consistency, and auditability across all modules.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

The experimental results indicate that the proposed KP-ABE with ECC integration provides secure and efficient data protection for IoT environments. It reduces encryption complexity compared to traditional CP-ABE approaches while maintaining fine-grained access control.

The use of ECC improves key generation efficiency and strengthens overall security. Overall, the framework achieves a good balance between data confidentiality, access control, and computational performance.

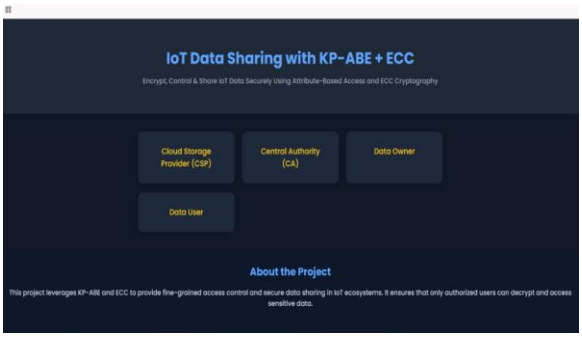


Fig. 2: Home Page



Fig. 3: Registration

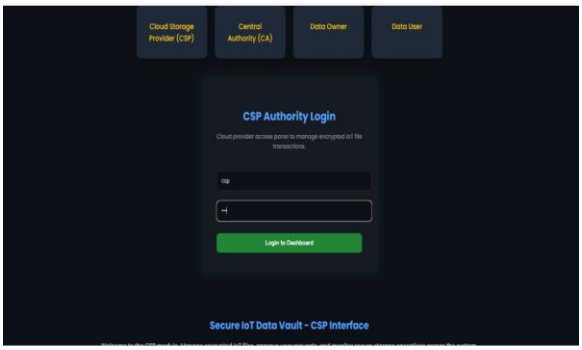


Fig. 4: Login

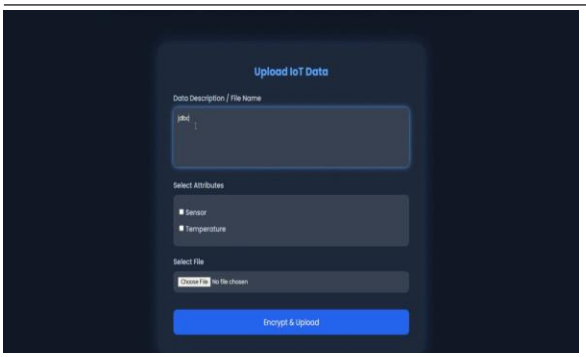


Fig. 5: Upload Data

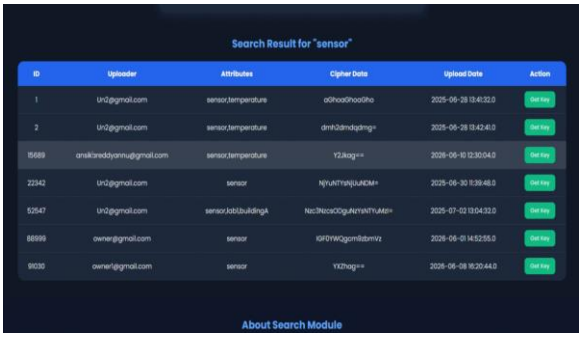


Fig. 6: Search File

V. CONCLUSION

In this study, a lightweight and fine-grained access control model was developed by integrating Elliptic Curve Cryptography (ECC) with Key-Policy Attribute-Based Encryption (KP-ABE). The proposed scheme offers strong protection against various security threats, including collusion attacks, man-in-the-middle attacks, and forgery attacks, ensuring both data confidentiality and data integrity. By employing multiple Attribute Authorities (AAs), the scheme effectively mitigates the risk of key escrow, while its support for outsourced decryption makes it well-suited for IoT environments, where user-end devices often have limited computational resources. Performance evaluations indicate that the proposed model not only maintains high security standards but also demonstrates superior execution times compared to other lightweight schemes in the literature.

REFERENCES

[1] M. De Donno et al. ”Foundations and Evolution of Modern Computing Paradigms: Cloud, IoT, Edge, and Fog,” in IEEE Access, vol. 7

[2] A. Subrahmannian and S. K. Behera, ”Chipless RFID Sensors for IoT Based Healthcare Applications: A Review of State of the Art,” in IEEE Transactions on Instrumentation and Measurement, vol. 71, pp. 1-20, 2022

[3] O. Elijah et al., ”An Overview of Internet of Things (IoT) and Data Analytics in Agriculture: Benefits and Challenges,” in IEEE Internet of Things Journal, vol. 5, no. 5,

[4] M. Asplund and S. Nadjm-Tehrani, ”Attitudes and Perceptions of IoT Security in Critical Societal Services,” in IEEE Access, vol. 4

[5] M. Yahuza et al., "Systematic Review on Security and Privacy Re quirements in Edge Computing: State of the Art and Future Research Opportunities," in IEEE Access, vol. 8

[6] M. Alrowaily and Z. Lu, "Secure Edge Computing in IoT Systems: Review and Case Studies," 2018 IEEE/ACM Symposium on Edge Computing (SEC), Seattle, WA, USA, 2018

[7] K.A. Shim, "A Survey of Public-Key Cryptographic Primitives in Wire less Sensor Networks," in IEEE Communications Surveys & Tutorials, vol. 18, no. 1, pp. 577-601

AUTHORS Profile



Mrs. VANGALA SWATHI has received her B.Tech from JNTUH, Hyderabad in 2015, M.Tech degree in Computer science from JNTUH, Hyderabad in 2017. She is dedicated to teaching field from the last 7 years. Her research area Deep Learning. At present she is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India.



Ms. GADDAMEEDI HASINI pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Ms. ANNU ANSIKA REDDY pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. ANGAJALA KISHORE pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. KERAVELLY ARSHITH REDDY pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions

Technical Campus affiliated to JNTUH in 2022-2026.