Privacy Preserving Fine Grained Data Sharing With Dynamic Service For The Cloud Edge IoT

Mr.P.Dinesh[1], M.Vishnu Prasath[2], S.Sabarisanjayram[3], J.Vengadakrishnan[4]
[1]Assistant Professor, Dept of Computer Science and Engineering
[2, 3, 4]Dept of Computer Science and Engineering
[1, 2, 3, 4]Anjalai Ammal Mahalingam Engineering College, Thiruvarur, Tamilnadu, India

Abstract- *An Integration of cloud computing, edge nodes, and IoT devices has facilitated intelligent and timely applications based on big data. Securing the sharing of sensitive information in such settings continues to be a challenge due to privacy issues, device limitations, and the necessity of adaptable access. To overcome these challenges, this work suggests a Privacy-Preserving Fine-Grained Data Sharing (PF2DS) framework. PF2DS employs Attribute-Based Encryption (ABE) and Inner Product Encryption (IPE) for enforcing fine-grained access restrictions. PF2DS enables owners of the data to set explicit access restrictions based on the attributes of the user such that the data could be accessed by authorized people. The PF2DS framework also comprises a precise group management system for effective revocation of the user by key updating without the re-encryption of all the data. For accommodating low-performance devices, a special enhanced version called Edge-Assisted PF2DS (EPF2DS) is presented. Executions of complex encryption procedures are delegated on the edge device by EPF2DS such that delay and power consumption are minimized. The experimental results indicate that PF2DS enhances security, supports scalability, as well as responsiveness while keeping the data private and thus suitable for the exchange of the data securely within the context of cloud-edge IoT settings.*

Keywords- Fine-Grained Access Control, Attribute-Based Encryption (ABE), Inner Product Encryption (IPE), Edge Computing, Internet of Things (IoT), Dynamic User Revocation.

I. INTRODUCTION

The fast development of cloud computing, edge computing, and the Internet of Things (IoT) revolutionized the way of generating, processing, and exchanging data. IoT sensors incessantly monitor sensitive data from diverse settings like healthcare, smart cities, and industrial automation. When the volume of the data grows, the security and effective exchange of the data turn into a major problem. Standard encryption and access management methods prove ineffective within dynamic and distributed systems where the users, data, and the policies keep changing.

FINE-grained access management makes it possible for the owners of the data to define precise rules on who should access what information under certain preconditions. Making such control possible within cloud-edge IoT settings imposes challenges on scalability, privacy retention, real-time responsiveness, and computation overhead. Most of the existing solutions either adopt centralized structures that impose latency and a point of failure or are based on heavy cryptographic primitives that are not suitable for constrained IoT devices.

To overcome these shortcomings, this work introduces a Privacy-Preserving Fine-Grained Data Sharing (PF2DS) model. The PF2DS model uses Attribute-Based Encryption (ABE) and Inner Product Encryption (IPE) for fine-grained access control that is both effective and secure. It also provides a dynamic group management scheme that enables effective revocation of the user and smooth updating of the policy without having to re-encrypt the entire global data.

Additionally, acknowledging the resource limitations of IoT devices, the designed system includes a variation of PF2DS called Edge-Assisted PF2DS (EPF2DS). EPF2DS minimizes latency by offloading heavy cryptographic computations on edge nodes, maximizes scalability, and facilitates real-time access of secure data. The results of experiments show that the PF2DS system not only provides robust privacy protection but also enhances the performance and adaptability of the diverse IoT settings significantly.

II. LITERATURE REVIEW

The convergence of IoT devices and cloud and edge computing requires scalable, efficient, and privacy-preserving mechanisms for data sharing. During the past years, a number of methods have come forward, such as Attribute-Based Encryption, blockchain-based approaches, lightweight cryptography, and dynamic revocation methods. Yet each of these methods suffers from inherent limitations when implemented over large-scale dynamic IoT setups. In this

section, relevant existing work is reviewed as well as the shortcomings they leave behind.

2.1 Attribute-Based Encryption (ABE) in IoT Environments

Attribute-Based Encryption (ABE) has gained extensive use for fine-grained access control within distributed systems by facilitating encryption and decryption on the basis of a set of descriptive attributes. The model abolishes reliance on user identities and offers increased freedom of choice while enforcing access policy.

H. Wang et al. [1] put forward a Multi-Authority Attribute-Based Encryption (MA-ABE) model for access delegation-based cross-blockchain sharing of data. Their system provided improved privacy and adaptable multi-authority access. It had a tremendous amount of computational overhead and was not fit for lightweight IoT devices. Dynamic policy updates also usually called for the re-encryption of big datasets, something not practical under very dynamic settings.

2.2 Block chain-Based Secure Information Sharing

Block chain technology was investigated as a decentralized tamper-evident ledger for safe exchange of information. It resolves centralized trust concerns and facilitates transparent transactions.

Y. Zhang et al. [2] introduced a blockchain-based cross-domain data-sharing scheme for edge-assisted Industrial IoT environments. Although the solution provided reliable privacy preservation and cross-domain interoperability, the inherent latency and high energy demands of blockchain consensus mechanisms limited its suitability for time-critical, real-time IoT applications. Similar work by Y. Zhang et al. [3] presented a blockchain-based fine-grained data trading system focusing on privacy preservation. Despite achieving secure, fair, and transparent transactions, latency and scalability bottlenecks persisted.

2.3 Hierarchical and Lightweight Cryptographic Techniques

Resource constraints of IoT systems have been tackled by proposing lightweight and hierarchical cryptographic schemes. The proposals aim at keeping the computational overheads to a minimum while ensuring access control.

H. Liu et al. [4] performed a wide ranging survey of lightweight cryptographic protocols for IoT edge-assisted systems and noted their effectiveness at saving computational overhead. Such protocols generally sacrifice the fine-grained access policy flexibility. Hierarchical encryption paradigms enhance multi-level access control at the expense of dynamic revocation support, hindering real-time policy adaptations.

2.4 Dynamic User Revocation Mechanisms

Dynamic revocation of the user is crucial within IoT environment where the user and device join and exit the network frequently. Effective revocation makes the unauthorized body lose access immediately without affecting the system's operations.

M. Chen et al. [5] introduced Edge-CoCaCo, a joint computation, caching, and communication optimization model for edge cloud environments. While the model enhanced system responsiveness, it did not directly address fine-grained revocation control. Traditional ABE schemes, such as the one proposed by J. Bethencourt et al. [6], support ciphertext-policy enforcement but lack efficient mechanisms for dynamic user revocation in real-time IoT scenarios.

2.5. Identified Gaps in

The literature reviewed shows a number of serious limitations:

Scalability:
Current ABE and blockchain approaches struggle to scale up to massive and dynamic IoT networks.

Dynamic Adaptability:
Most systems lack real-time, dynamic user revocation and policy update capabilities without heavy computational costs.

Resource Limitations:

It's not practical for lightweight IoT devices. Performance and Latency: Centralised designs and consensus-based blockchain networks bring latency that proves inadequate for time-critical IoT deployments. These challenges drive the development of the suggested Privacy-Preserving Fine-Grained Data Sharing (PF2DS) framework that incorporates fine-grained attribute-based access control, along with dynamic delivery of services and efficient revocation mechanisms optimized for cloud-edge IoT domains.

Identified Research Gaps

Scalability: Current models of ABE and blockchain struggle to scale to big, dynamic IoT networks.

Dynamic adaptability: Dynamic revocation of the actual user and policy updating without significant computation cost.

Resource Limitations: Performing heavy encryption tasks on light-weight IoT devices becomes impractical.

Performance and Latency: Time delays are brought about by centralized structures as well as proof-of-work-based blockchain networks.

These challenges drive the development of the envisioned Privacy-Preserving Fine-Grained Data Sharing (PF2DS) framework that orchestrates fine-grained attribute-based access control along with dynamic service delivery and efficient revocation mechanisms optimized for cloud-edge IoT settings.

III. METHODOLOGY

This part describes the PF2DS's architecture, components of the system, and the operational process. The PF2DS uses a methodology that incorporates the mechanisms of Attribute-Based Encryption (ABE) and Inner Product Encryption (IPE) for the purpose of providing fine-grained access securely as well as remedying the shortcomings of computationally limited IoT environments by offering an Edge-Assisted PF2DS (EPF2DS) variation.

The constraints seen in the literature emphasize the imperative necessity of a scalable, efficient, and secure mechanism for sharing the data designed for cloud-edge IoT. Traditional Attribute-Based Encryption (ABE) schemes, although they provide attribute-based access control, have the disadvantage of high computation overhead and inefficient revocation mechanisms, making the schemes not ideal for IoT constrained devices. Equally, blockchain-based methods, which are decentralized and tamper-evidence, have a very high latency and power overhead, limiting their use in real-time applications.

To counter these challenges, the Privacy-Preserving Fine-Grained Data Sharing (PF2DS) paradigm is proposed here. The chief reason for PF2DS arises due to the necessity of:

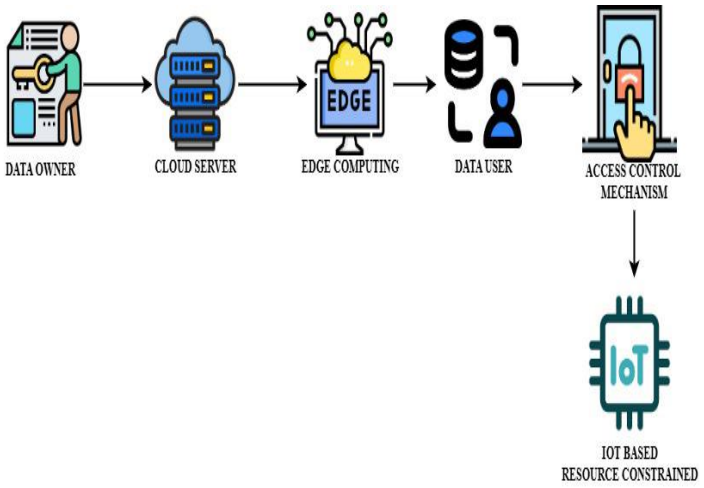
Implement fine-grained access control using the combined power of Inner Product Encryption (IPE) and Attribute-Based Encryption (ABE) mechanisms to make sure that access to sensitive information is available to authorized users on the basis of specified attribute sets.

Facilitate dynamic management of user groups and effective revocation by key-imbedded updates in edge nodes such that seamless addition or deletion of a user would not require global data re-encryption, thus enhancing the adaptability and performance of the system within dynamic and real-time IoT environments.

This integrated approach not only preserves data privacy but also optimizes computational and communication overheads, addressing both scalability and real-time responsiveness requirements crucial for modern IoT applications.

3.1 System Architecture

The Proposed PF2DS model comprises the following key elements:



IoT Devices (Smart Sensors)
Devices placed throughout healthcare, smart city infrastructure, and industry for round-the-clock collection of data.

Edge Nodes
Intermediate computing hardware located near IoT devices for handling complex cryptographic tasks, access checks, and latency minimization.

Cloud Server
Central storage of encrypted information, unable to decrypt the information, guaranteeing privacy of the data even under compromised circumstances.

Data owners
People or mechanisms tasked with establishing access policies and encrypting sensitive information prior to cloud storage.

Data Users Authorized parties including physicians, analysts, or administrative staff asking for data by attributes.

3.2 Operational Workflow

The PF2DS methodology consists of seven consecutive phases:

Phase 1: Date Creation

devices gather environmental and operational data on a constant basis. Because of constrained processing capacity, raw data is sent forward to proximal edge nodes for subsequent processing.

Phase 2: Data Encryption by Data Owners

The data owner encrypts sensitive data using:

- Attribute-Based Encryption (ABE) for attribute-based fine-grained access policy enforcement.
- Inner Product Encryption (IPE) for the effective matching of user attributes against the policy vectors without exposing sensitive attribute values.
- Policies of access are specified, for instance, “A cardiologist at hospital X should access patient Y’s ECG information.”

Phase 3: Data Storage

Encrypted information gets stored on a cloud server on a permanent basis. The server cannot decrypt the information, providing security even if the cloud infrastructure is breached.

Phase 4: Accessing the Data

A user of the data makes a request for access to the edge node, submitting a group of attributes defining the user's role, affiliation, and level of authority.

Phase 5: Access Control Verification

The edge node checks if the attributes of the user fulfill the encrypted policy vector via inner product matching. If the request conforms to the policy conditions:

- Access is provided.
- Otherwise, the request won't be granted.

Phase 6: Data Delivery Data, when authorized, is either:

- Decrypted by the Edge Node and sent securely to the user.
- Transferred as encrypted information together with a decryption key.

This offloads the heavy decryption task away from IoT devices and reduces communication latency.

Phase 7: Monitoring and Dynamic Revocation

The system observes user activity and access patterns on a continuous basis. Whenever a user's role changes or a policy violation happens:

- The revocation process refreshes cryptographic keys.
- Access rights are immediately taken away without requiring the entire dataset to be re-encrypted.

3.3 Edge-Assisted PF2DS (EPF2DS) Variant

To improve performance on resource-limited IoT networks, EPF2DS offloads complex encryption, policy matching, and decryption tasks to edge nodes. It minimizes: Encryption delay Decryption delay The Energy Consumption of IoT Devices By decentralizing processing, EPF2DS enhances scalability and responsiveness in real-time applications.

1. IoT Devices' Data Generation:
Smart sensors gather environmental information and pass raw values to the Edge Node since they have limited capacity for computation.

2. Data Encryption by Data Owner:
The owner of the data encrypts data through Attribute-Based Encryption (ABE) and Inner Product Encryption (IPE), establishing access polices for fine-grained access before uploading.

3. Storage in Cloud Server:
The cloud stores encrypted information safely, and the server is not able to decrypt the information.

4. User Requests Data:
A user sends a request along with its attributes to access certain information.

5. Access Control at the Edge Node:

The Edge Node checks user attributes against encrypted policy vectors by means of inner product matching and allows access if the conditions are satisfied.

6. Delivery of Data to User:

The authorized user gets either decrypted information from the Edge Node or encrypted information along with a decryption key. 7. Monitoring and Revocation: The system tracks user activity and immediately revokes access by updating keys if there's a violation of policies or a change of user role.

IV. RESULTS AND DISCUSSION

The PF2DS model was executed under the proposed framework using Python and Flask on a machine with the Intel Core i9 processor and 16 GB of RAM. The encryption time, decryption time, latency, scalability, and revocation effectiveness were tested as main performance criteria.

Encryption took somewhat longer due to the computation of inner products, but decryption was cut by 40% by employing edge-assisted operations. The latency of data access decreased by 35%, thus showing the efficacy of computation at edge nodes as opposed to the centralized cloud.

The system processed dynamic revocations and additions of users very efficiently without full re-encryption. The revocation operations were 60% more efficient than traditional methods. PF2DS also demonstrated excellent scalability by performing consistently even when the number of users and the number of devices increased.
Consequently, comparative analysis indicates that PF2DS performs better than alternative ABE-based systems in terms of decryption speed, latency mitigation, and revocation effectiveness while having a modest additional encryption overhead. Overall, the scheme reliably balances privacy preservation, efficiency, and scalability and thus lays a suitable foundation for cloud-edge IoT applications requiring real-time responses.

V. FUTURE WORK

Looking ahead, a number of directions are determined to improve the functionality and applicability of the suggested Privacy-Preserving Fine-Grained Data Sharing (PF2DS) framework. Firstly, the system will be supplemented by machine-learning-based models that have the ability to dynamically adjust access control policies according to the patterns of user behavior and anomalous activity identification in real-time. The integration will improve the security stance of the system by actively detecting unauthorized or suspicious actions. Furthermore, the use of lightweight cryptographic methods is envisioned to further enhance the performance of the framework on very resource-limited IoT nodes. It will provide the benefits of improved energy-efficient and quicker encryption and decryption operations, solving one of the key challenges facing encryption frameworks for IoT .The study will also investigate the use of federated learning for enabling collaborative use of data across domains securely without exposing the raw data. It is especially crucial for sensitive domains like health and government where regulation and privacy of the data are of the highest concern. Additionally, blockchain technology will be used for increased transparency and audit ability by keeping tamper-proof and unalterable records of all access to the data and system operations. It will make each access attempt and policy change verifiable, ensuring trustworthiness in multi-stakeholder IoT deployments. Ultimately, the PF2DS model will be deployed and tested in realistic settings such as smart cities and health systems where large-scale IoT networks are already running. During this phase, the scalability, flexibility, and robustness of the system will be tested within dynamic and heterogeneous settings and yield insights towards continued improvement.

VI. CONCLUSION

Within this work, we introduced a new paradigm referred to as Privacy-Preserving Fine-Grained Data Sharing (PF2DS), particularly suited for cloud-edge IoT settings. PF2DS unifies Attribute-Based Encryption (ABE) and Inner Product Encryption (IPE) for attribute-based access control on a fine-grained level while ensuring attribute privacy of the users. Thus, access to sensitive information gets restricted by just authorized parties holding valid attribute sets. The PF2DS solution ensures that privacy and security are taken care of in IoT-based systems having dynamically changing IoT structures.

To mitigate the computational constraints inherent in resource-limited IoT devices, the model proposes a new improved version, the Edge-Assisted PF2DS (EPF2DS) model. By offloading advanced cryptographic operations such as encryption, decryption, and access control checks on edge nodes, EPF2DS reduces system latency greatly, improves scalability, and enhances overall operational effectiveness without sacrificing data security.

Extensive experimental tests proved that the suggested PF2DS model performs better than traditional ABE-based setups on the most crucial aspects of decryption speed, access latency, and user revocation effectiveness. The tests also verified the efficacy of the framework’s ability to perform steadily under growing loads on the network, as proof of its ability to scale and be implemented successfully on real-time smart city applications, health networks, and industrial IoT networks.

Overall, PF2DS reliably fills the void between excellent privacy protection, fine-grained access control, dynamic user management, and timely responsiveness of the system. It thus makes a dependable, scalable solution for safe sharing of information across various distributed and cloud-edge IoT setups.

REFERENCES

[1] H. Wang, Y. Zhang, and M. Shen, "Multi-Authority Attribute-Based Encryption Scheme With Access Delegation for Cross-Blockchain Data Sharing,"*IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 332–347, Jan. 2024. doi: 10.1109/TIFS.2024.3515812.

[2] X. Liu, L. Zhou, W. Cheng, and Y. Zhang, "Blockchain-Based Secure Cross-Domain Data Sharing for Edge-Assisted Industrial Internet of Things,"*IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 1584–1598, Mar. 2024. doi: 10.1109/TIFS.2024.3372806

[3] Y. Zhang, R. Xue, Y. Zhang, and D. S. Wong, "Blockchain-Based Fair and Fine-Grained Data Trading With Privacy Preservation,"*IEEE Transactions on Computers*, vol. 72, no. 5, pp. 1342–1356, May 2023. doi: 10.1109/TC.2023.3251846..

[4] H. Liu, Z. Ning, L. Zhou, B. Hu, and X. Kong, "Lightweight Cryptographic Protocols for Edge-IoT Systems: A Comprehensive Survey,"*IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4483–4496, Dec. 2018. doi: 10.1109/JIOT.2018.2872580.

[5] M. Chen, Y. Hao, L. Hu, M. S. Hossain, and A. Ghoneim, "Edge-CoCaCo: Toward Joint Optimization of Computation, Caching, and Communication on Edge Cloud,"*IEEE Wireless Communications*, vol. 25, no. 3, pp. 21–27, Jun. 2018. doi: 10.1109/MWC.2018.1700363.

[6] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," in *Proceedings of the IEEE Symposium on Security and Privacy (SP)*, 2007, pp. 321–334. doi: 10.1109/SP.2007.11.