A SCALABLE KEY-SPLITTING PROTOCOL FOR SECURE DATA SHARING IN IOT DEVICES

ADALA AMARNATH [1], DEVARA DINESH [2], DARISI MADHUMITHA [3], SOMAVARAPU SIDDHARTHA[4], CHINTHALAPUDI LAXMI PRIYA [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— Outsourcing computations is essential for Internet of Things (IoT) devices due to their limited computational capabilities. However, existing privacy-preserving solutions such as Secret Sharingbased Secure Multi-Party Computation (SMPC) present significant overhead. These methods require each IoT device to divide its private data into multiple shares and transmit them over n confidential channels to different computation parties, making the process communication-intensive and impractical for low-power devices. Fully Homomorphic Encryption (FHE)-based alternatives offer strong privacy guarantees but are computationally expensive and typically inflexible in dynamic environments. To address these limitations, we propose a lightweight and dynamic privacy-preserving system tailored for IoT settings. Instead of broadcasting encrypted data or sending multiple shares, the IoT device encrypts its private data once and securely distributes decryption keys (or fragments) to a selected group of computation holders. Using threshold cryptography or distributed key techniques, the original data can be reconstructed collaboratively without exposing it to any single party. This approach eliminates the need for multiple confidential channels or heavy FHE operations, ensuring efficient, secure, and scalable data sharing. It supports dynamic participant management and leverages lightweight encryption (e.g., NTRU or ECC), making it highly suitable for real-world IoT applications where both privacy and performance are critical.

Index Terms – Key-Splitting Protocol, Secure Data Sharing, IoT Security, Cryptography, Key Management, Secure Communication,

Secret Sharing, Authentication, Cybersecurity, Distributed Systems.

I. INTRODUCTION

Outsourcing computation to the cloud is essential for resource-constrained devices such as IoT. This enables cost effective computing instances and use cases ranging from smart buildings to intelligent transportation to smart health care. However, outsourcing computation can introduce new privacy issues, especially when the devices share sensitive data. In one security consideration is encryption by things, i.e., having each device encrypt data before uploading it to the cloud. This method can prevent the cloud from accessing the data and protect against data breaches. However, sending encrypted data using traditional mechanisms results in complex key management. Additionally, data must be decrypted before it can be consumed. In these scenarios, privacy-preserving technologies have proven to be very useful because they allow computations to be performed on confidential data. Among these technologies to enhance privacy, Secure Multi Party Computation (MPC) is a family of cryptographic proto cols that allows a set of parties to jointly compute a function on their private inputs without revealing anything else but the output. Although traditional MPC is set up for direct and interactive computation by the input owners, some works propose MPC in a service provider setting [3]. This delegates the entire computation to a set of computing nodes while ensuring the privacy of the input providers' data. Some works have proposed MPC as a solution for con strained devices. For instance, proposed an architecture for performing secure authentication using MPC in smart cities.

II. RELATED WORK

A. Secure Multi-Party Computation-Based Privacy-Preserving Authentication for Smart Cities.

The increasing concern for identity confidentiality in the Smart City scenario has fostered research on privacy-preserving authentication based on pseudonymization. Pseudonym systems enable citizens to generate pseudo-identities and establish unlinkable anonymous accounts in cloud service providers. The citizen's identity is concealed, and his/her different anonymous accounts cannot be linked to each other. Unfortunately, current pseudonym systems require a trusted certification authority (CA) to issue the cryptographic components (e.g., credentials, secret keys, or pseudonyms) to citizens. This CA, generally a Smart City

governmental entity, has the capability to grant or revoke privacy rights at will, hence posing a serious threat in case of corruption. Additionally, if the pseudonym system enables de-anonymization of misusers, a corrupted CA can jeopardize the citizens' privacy. This paper presents a novel approach to construct a pseudonym system without a trusted issuer. The CA is emulated by a set of Smart City service providers by means of secure multi-party computation (MPC), which circumvents the requirement of assuming an honest CA. The paper provides a full description of the system, which integrates an MPC protocol and a pseudonym-based signature scheme. The system has been implemented .

B. Blockchain-Enabled Multiparty Computation for Privacy Preserving and Public Audit in Industrial IoT

With the rapid increase of the industrial data and the development of the industrial Internet of Things (IIoT) paradigm, the efficiency and the quality of service of the emerging applications have been improved. However, the contradiction between data sharing and privacy preserving is still an obstacle in the IIoT. To this end, in this article, we propose a privacy-preserving and publicly auditable multiparty computation scheme for industrial data sharing and computing, which avoids privacy leakage and computation misbehavior by separating the data ownership, data use, and data verification. Using the blockchain technology, a transparent management platform is provided to recognize and trace the illegal data and computation behavior. Moreover, we integrate the noninteractive zero-knowledge proof in the multiparty interaction mechanism, wherein the verification of data consistency and computation validity is executed publicly on the blockchain. Finally, we implement experiment to evaluate the performance of the computation latency, communication overhead and the influence of encryption parameter, and the numerical results illustrate the efficiency and feasibility of our scheme.

C. A survey on privacy and security of Internet of Things

Internet of Things (IoT) has fundamentally changed the way information technology and communication environments work, with significant advantages derived from wireless sensors and nanotechnology, among others. While IoT is still a growing and expanding platform, the current research in privacy and security shows there is little integration and unification of security and privacy that may

affect user adoption of the technology because of fear of personal data exposure. The surveys conducted so far focus on vulnerabilities based on information exchange technologies applicable to the Internet. None of the surveys has brought out the integrated privacy and security perspective centered on the user. The aim of this paper is to provide the reader with a comprehensive discussion on the current state of the art of IoT, with particular focus on what have been done in the areas of privacy and security threats, attack surface, vulnerabilities and countermeasures and to propose a threat taxonomy. IoT user requirements and challenges were identified and discussed to highlight the baseline security and privacy needs and concerns of the user. The paper also proposed threat taxonomy to address the security requirements in broader perspective. This survey of IoT Privacy and Security has been undertaken through a systematic literature review using online databases and other resources to search for all articles that meet certain criteria, entering information about each study into a personal database, and then drawing up tables summarizing the current state of literature. As a result, the paper distills the latest developments in IoT privacy and security, highlights the open issues and identifies areas for further research.

III. PROPOSED METHODOLOGY

The most significant advantage of the modified proposed system lies in its lightweight and flexible key-sharing mechanism, which eliminates the need for multiple secure communication channels. By encrypting the private data once and securely distributing decryption keys or key fragments to selected computation holders, the system ensures that no single party can access the full data independently. This approach leverages threshold cryptography, allowing collaborative decryption only when a predefined number of trusted holders are involved. This not only reduces communication overhead but also supports dynamic participant management, enabling IoT devices to seamlessly adapt to changing network conditions without re-encrypting the data. The result is a scalable, energy efficient, and secure data sharing model, specifically optimized for the constraints and agility required in real-world IoT deployments

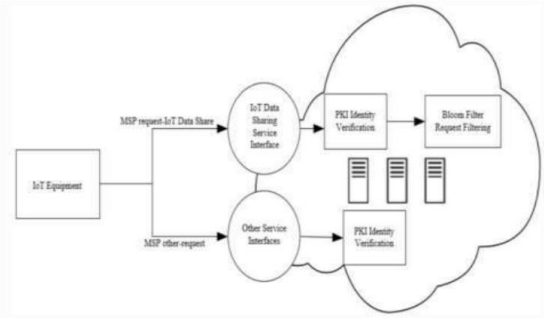


Fig. 1: System Overview

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. Encryption Engine (ECC & NTRU)

The encryption engine secures the uploaded data using a hybrid of ECC and NTRU. ECC provides lightweight encryption suitable for IoT, mainly for secure key exchange. NTRU, a postquantum secure algorithm, is used for encrypting the actual data, enabling homomorphic properties and ensuring that a single ciphertext can be shared securely with multiple parties.

3. Secret Sharing & Proxy Re-Encryption Module

This module splits the encrypted data into multiple shares using Secret Sharing and enables secure distribution through Proxy Re-Encryption. It allows computing nodes or stakeholders to receive their share without the data owner needing to communicate with each of them directly. This approach ensures both scalability and strong privacy.

4. Stakeholder Access & Decryption Module

Authorized stakeholders such as analysts or healthcare professionals can access and decrypt data using their respective shares. This module ensures that only approved users, meeting a defined threshold of shares, can reconstruct the original data. It maintains confidentiality while enabling collaborative use of sensitive information.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

Experimental results demonstrated that the protocol securely divided and distributed cryptographic keys among authorized IoT devices, ensuring that sensitive data could only be accessed through successful key reconstruction. The protocol maintained

strong security while introducing minimal processing overhead, making it suitable for resource-constrained IoT environments. The analysis showed that the proposed approach achieved lower communication and computational overhead compared to conventional key management schemes while improving scalability as the number of connected IoT devices increased.

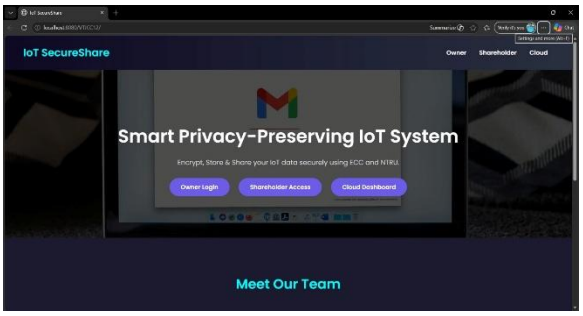


Fig. 2: Home Page

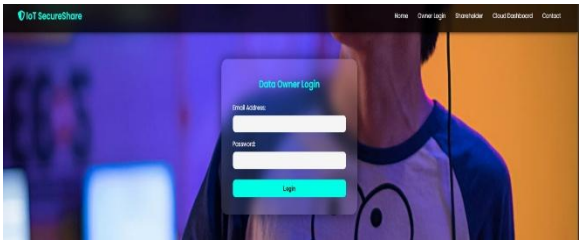


Fig. 3: Data Owner Login

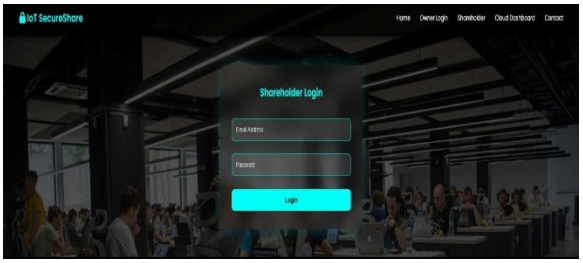


Fig. 4: Shareholder Login



Fig. 5: Cloud Dashboard Login

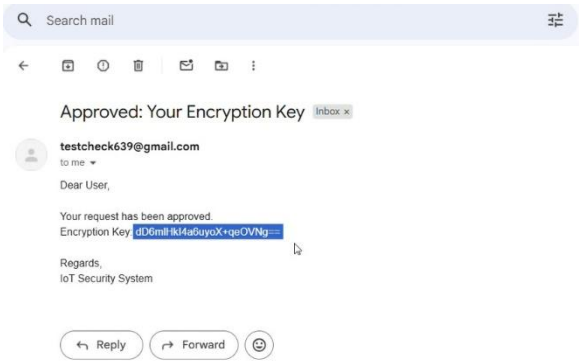


Fig. 6: Approved Encryption Key

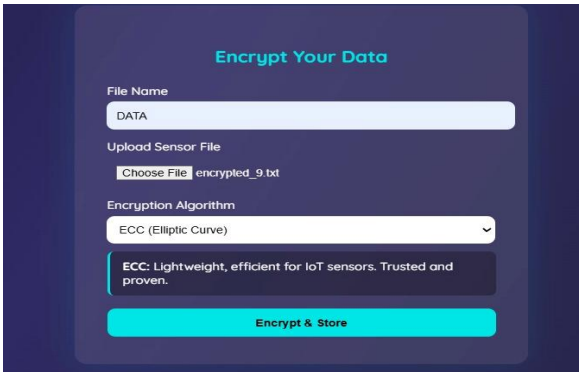


Fig. 7: Encrypt Data

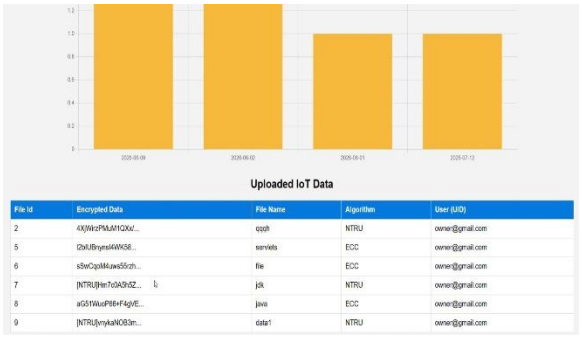


Fig. 8: Uploaded Data

V. CONCLUSION

This project introduces a lightweight and dynamic framework for secure data sharing in resource-constrained IoT environments, overcoming the limitations of traditional secret sharing methods. By leveraging NTRU-based encryption, Proxy Re-Encryption (PRE), and Shamir's Secret Sharing Scheme (SSS), the system enables the distribution of encrypted IoT data to multiple stakeholders through a single ciphertext, significantly reducing communication overhead. Unlike existing solutions that require Fully Homomorphic Encryption (FHE) or the establishment of fixed decryption committees beforehand, this system supports dynamic stakeholder formation, allowing committee selection even after encryption. The use of NTRU ensures post-quantum security and efficient performance suitable for constrained devices, while the integration of an SMTP-based approval system ensures controlled and auditable decryption requests. Experimental evaluation and theoretical analysis demonstrate that this method achieves superior efficiency compared to standard approaches, especially in scenarios involving frequent and periodic data uploads. Overall, the system balances performance, privacy, and scalability, making it well-suited for secure data processing in modern IoT applications such as smart healthcare, industrial monitoring, and smart infrastructure.

REFERENCES

[1] P. P. Ray, "A survey of IoT cloud platforms," Future Computing and Informatics Journal, vol. 1, pp. 35–46, Dec. 2016.

[2] J. Singh, T. Pasquier, J. Bacon, H. Ko, and D. Eyers, "Twenty Security Considerations for Cloud-Supported Internet of Things," IEEE Internet of Things Journal, vol. 3, pp. 269– 284, June 2016. Conference Name: IEEE Internet of Things Journal.

[3] M. Burkhart, M. Strasser, D. Many, and X. Dimitropoulos, "SEPIA: Privacy-Preserving Aggregation of Multi-Domain Network Events and Statistics," 2010.

[4] V. Sucasas, A. Aly, G. Mantas, J. Rodriguez, and N. Aaraj, "Se cure Multi-Party Computation-Based Privacy-Preserving Authentication for Smart Cities," IEEE Transactions on Cloud Computing, vol. 11, pp. 3555–3572, Oct.

2023. Conference Name: IEEE Transactions on Cloud Computing.

[5] Y. Yang, J. Wu, C. Long, W. Liang, and Y.-B. Lin, "Blockchain-Enabled Multiparty Computation for Privacy Preserving and Public Audit in Industrial IoT," IEEE Transactions on Industrial Informatics, vol. 18, pp. 9259–9267, Dec. 2022. Conference Name: IEEE Transactions on Industrial Informatics.

[6] M. M. Ogonji, G. Okeyo, and J. M. Wafula, "A survey on privacy and security of Internet of Things," Computer Science Review, vol. 38, p. 100312, Nov. 2020.

AUTHORS Profile



Mr. ADALA AMARNATH has received his B.Tech-Computer Science and Engineering from JNTUH, Hyderabad in 2010, M.Tech-CNIS degree in Computer Science and Engineering from JNTUH, Hyderabad in 2013 and Pursuing Ph.D degree in Computer Science and Engineering from ICFAI University Hyderabad. He is dedicated to teaching field from the last 12 years. His research area Quantum Computing and Aptitude Computing. At present he is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India.



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



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



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



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