IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13382

A Scalable Key-Splitting Protocol for Secure Data Sharing in IoT Devices

P. Sriram[1], Pratik Patel[2], Noor Alam Mansoor[3], T. Devender Rao[4]

Student, Computer Science and Engineering, Guru Nanak Institutions Technical Campus Hyderabad, India.[1]

Student, Computer Science and Engineering, Guru Nanak Institutions Technical Campus Hyderabad, India.[2]

Student, Computer Science and Engineering, Guru Nanak Institutions Technical Campus Hyderabad, India.[3]

Assistant Professor, Computer Science and Engineering,

Guru Nanak Institutions Technical Campus Hyderabad, India.[4]

Abstract: As the Internet of Things (IoT) technology is becoming more popular, the information that is being generated is in vast quantity and rich with sensitive information and that information has to be shared and processed safely within the cloud infrastructure. However, privacy preserving methods like secret sharing and secure multi-party computation need several encrypted shares to be exchanged with various nodes making the communication overhead of IoT devices large. This paper presents a safe data sharing model of the IoT systems, that is effective in reducing the overhead of communication. The combination of the performance advantages of the Elliptic Curve Cryptography (ECC) on secure key exchange, NTRU cryptosystem on efficient post-quantum cryptography, and a threshold based secret sharing scheme on distributed key management has been achieved in this respect. proxy re-encryption in this system also ensures that the key shares are distributed safely to the authorized stakeholders without causing harm to the original secret information. Thereby only one time the data are encrypted and therefore several key fragments are delivered to the receiver rather than several ciphertexts, thereby, reducing the overhead of communications but at the same time having high data confidentiality.

Keywords: Internet of Things, Data Sharing, Elliptic Curve Cryptography, NTRU Cryptosystem, Secret Sharing, Proxy Re Encryption.

I. INTRODUCTION

The active evolution and implementation of the Internet of Things (IoT) technology has led to billions of connected devices producing and exchanging large volumes of data. IoT devices are increasingly used in smart city technologies, health monitoring systems, industry automation systems, and smart transport systems. Although cloud computing enables easy storage and processing of IoT data, it introduces several privacy and security issues. The generated data may remain unprotected against unauthorized access and attacks during both storage and transmission [1]–[3]. To address these challenges, several cryptographic approaches such as Secret Sharing and Secure Multi-Party Computation have been studied for IoT networks [4], [5]. However, in existing secret-sharing based data-sharing solutions, IoT devices must split their data into multiple components and transmit them to different nodes using secure channels. This increases communication overhead and energy consumption making such approaches unsuitable for resource-constrained IoT environments.

Recently, different advanced cryptographic schemes including lattice-based encryption, proxy re-encryption, and threshold cryptography have been explored to improve data-sharing systems in IoT networks [6]–[8]. These techniques enable secure sharing of encrypted data among multiple entities without compromising confidentiality. Motivated by these challenges, this paper proposes an efficient data-sharing framework for IoT networks. The frame work utilizes Elliptic Curve Cryptography for secure key exchange, the NTRU public-key encryption algorithm for efficient data encryption, and a threshold-based secret-sharing scheme for distributed key management. Proxy Re-Encryption is further applied to distribute key shares among stakeholders so that data can be reconstructed only when a predefined number of participants collaborate. By encrypting IoT data once and distributing key fragments instead of ciphertext fragments, the proposed approach reduces communication overhead while maintaining strong data confidentiality.

The key aims of the suggested system may be said as follows:

i. To come up with a safe architecture of securing the sensitive IoT data within the cloud environment.
ii. To include lightweight cryptography methods such as ECC and NTRU so as to encrypt data efficiently.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13382

iii. To apply proxy re-encryption to access dynamic and secure data accessibility control.
iv. To lessen communication overhead and to offer resource constrained IoT devices scalability.

II. LITERATURE SURVEY

The rapid growth of the IoT systems is also associated with new challenges in ensuring sensitive data of the IoT devices that are resource-constrained. Cloud platform is also widely used in storage and information processing of IoT system thereby introducing security issues and privacy concerns in IoT systems. Some of the researchers have also dealt with secure IoT systems and several privacy preserving protocols of the IoT cloud system. Ray [1] introduced to the overview of the IoT cloud platforms also mentioned the need to have secure management of the data in a distributed IoT system. [2] An other security issue that Singh et al. discovered is that cloud based IoT systems are prone to a range of security-related challenges, such as data privacy, secure communications over the network, and user authentication.

Theemann et al. have also analyzed different protocols of Secure Multi-Party Computation to distributed systems to ensure privacy of data in the distributed systems. The Secure Multi-Party Computation is a protocol that provides different functionalities to compute information using distributed environment without revealing any sensitive data to all of the users [4]. We have also seen that there are other homomorphic encryption protocols which can have other functionalities in respect to Secure Multi-Party Computation protocols in distributed systems as shown by Damgard et al. [5] SEPIA, however, also developed different protocols to the data aggregation in a distributed system based on the secure multiparty protocols in the modern IoT and smart cities in which SMPC can be deployed in privacy-sensitive authentication and data processing protocols [9].Despite the fact that these approaches provide formidable assurances that user privacy might be upheld, they often may be expensive in computational and communication overheads and are hence ill to execute these methods to the resources of a resource limited IoT system [10].

However, the latest researches have been performed on using the lattice-based cryptography to improve the safety and productivity of the distributed systems. A lattice based homomorphic encryption scheme proposed by Marandi et al. [6]is suggested to be used in privacy preserving smart metrical analytics. Lattice-based cryptography has been discovered as one of the most important areas in the development of the next generation systems since it is resistance to quantum attacks. Additionally, Marcolla et al. managed to provide a comfortable overview of Fully Homomorphic Encryption (FHE) and its applications to privacy-preserving systems. [8] Despite the fact that the security offered by this technique is high, it has a high computational overhead making this technique less efficient in the IoT devices. and studies on the application of privacy preserving deep learning models of multiparty computation to IoT systems have been conducted [11].

TABLE I: Comparison of Existing Secure Data Sharing Approaches

Study	Technique Used	Advantages	Limitations
Ray [1]	IoTclouds	Efficient data sharing with the cloud in the IoT systems	Limit scope of discussion to secure means of data sharing
Evans et al. [4]	Secure Multi-Party Computation	Outsource various parties to a server and Enough privacy	High computational and overhead communication
Damg˚ard et al. [5]	Homomorphic Encryption based MPC	Homomorphic Intensive MPC Data computation	perations are encrypted with the help Homomorphic Encryption-based MPC
Herranz et al. [15]	Multi-secret Sharing Schemes	Secure key distribution among multiple parties	It needs more than a one secure communication channel
Marandi et al. [6]	Lattice-based Homomorphic Encryption	Post-quantum security and privacy protection	Computational complexity for IoT devices
Qin et al. [7]	Proxy Re-Encryption	Flexible delegation of decryption privileges	Requires proxy infrastructure
Yang et al. [14]	Blockchain + MPC	Transparent and auditable data sharing	Increased system complexity
Proposed System	ECC + NTRU + Secret Sharing + PRE	Lightweight, scalable, reduced communication overhead	Needs threshold cooperation to Break into parts Decryption

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13382

Another possible method of data sharing that can be deployed to share data securely is Proxy Re-Encryption using which the proxy server has the capability of re-encrypting the data to be re-distributed to another user without having the original secret key publicly revealed. Qin et al. presented a survey on Proxy Re-Encryption-based techniques procurement of distributing cloud data and its merits on distributed systems, protogy [7] Canetti and Hohenberger were also able to propose a safe methodology to proxy re-encryption [12].

Moreover, the recent studies initially tended toward the design of hybrid cryptography systems which are founded on the principles of the secret sharing, homomorphic cryptography and on the view of the distributed computing. High level homomorphic secret sharing was presented by Chillotti et al. between multiple parties, whereby it is possible to prove the conviction of secret computation [13]. The authors of the research on the topic have also published another article on the topic by Yang et al. where they discuss the paradigmatic system multiparty computation through the use of blockchain when sharing the data safely in the industrial IoT systems [14].

Such solutions are excellent security and privacy guarantees to the data, and yet, the current solutions in the key management and the computational cost of big IoT networks pose a problem. As such, there is a necessity of cryptographic systems, which can be able to provide communication overhead that is not only low but also provides the level of security. The problematic issues mentioned above can be turned out through the offered system that will implement the lightweight encryption methods, secret sharing, on the basis of the thresh old, and proxy re-encryption approaches. The information in the proposed system is encrypted only once and the key is divided to various parts as compared to encrypting the information more than once and cutting the encrypted data to different pieces.

III. THEORETICAL BACKGROUND

In a bid to be safe when sharing data in the IoT networks, there is necessity to incorporate optimal cryptographic elements so as to avail the data sharing process with security and efficiency. Under the conventional methods of data encryption, the security-of-key systems cannot be centralized easily and therefore presents a security risk to remote systems. To overcome the flaws posed by the conventional approaches, it is requiring an integration of secure data sharing tools by the application of different modes of cryptographic rules such as public key encryption, secret sharing, and proxy re-encryption in secure data sharing models [1], [2]. The proposed system introduces the use of lightweight encryption, post-quantum cryptography and threshold key distribution to make sure that data sharing in the IoT networks are effective and secure. Cryptographic schemes such as Elliptic Curve Cryptography (ECC), NTRU cryptosystem, secret sharing mechanism, and proxy re-encryption mechanism are the theoretical foundations of the proposed system.

A. Elliptic Curve Cryptography (ECC)

Elliptic Curve cryptography is a method of conducting public-key cryptography that is utilized in performing secure communication in IoT systems. ECC provides the same level of security as other algorithms but with much smaller key sizes, making it computationally efficient. ECC is used in IoT systems during key exchange between communicating parties. ECC facilitates protection of encrypted data by utilizing elliptic curve mathematics to produce pairs of keys for secure communication [2].

B. NTRU Cryptosystem

NTRU is a lattice based encryption algorithm and a public key algorithm that is quantum resistant and has high speed. The NTRU algorithm functions in a polynomial ring rather than the traditional number ring and enables efficient encryption and decryption operations. Lattice-based cryptography is considered a promising structure for building secure systems in the future as it offers protection against quantum adversaries [6]. In the proposed system, the information is coded using the NTRU algorithm before transmitting the data to the cloud service.

C. Secret Sharing and Threshold Cryptography

Secret sharing schemes divide a secret value into different segments and distribute them among multiple participants. The original secret can only be reconstructed when a sufficient number of shares are combined. These schemes are widely used in cryptographic protocols including secure multi-party computation to establish trust among different parties [4], [15]. In the suggested system, a threshold secret sharing technique is used to divide the decryption key into multiple parts that are distributed among stakeholders.

D. Proxy Re-Encryption

Proxy Re-Encryption (PRE) is a cryptographic technique that allows a semi-trusted proxy server to transform ciphertext encrypted with one key into ciphertext that can be decrypted with another key without revealing the plaintext [7], [12]. PRE is useful in distributed data sharing systems where encrypted data must be securely shared

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13382

with multiple stake holders. In this approach the proxy server performs the re encryption operation while remaining unaware of the actual data content.

E. Secure Multi-Party Computation

Secure Multi-Party Computation (SMPC) allows multiple parties to jointly compute functions over their private inputs while keeping those inputs confidential. SMPC techniques are widely used in distributed computation systems and privacy preserving data processing environments [5], [8].

In the proposed system, the concept of SMPC is applied through threshold cryptography and distributed key management. The system combines secret sharing with proxy re encryption to ensure that encrypted information can only be accessed collaboratively by authorized stakeholders. Combined, these cryptographic techniques support the proposed framework in providing a secure, scalable, and efficient information sharing system for IoT environments while maintaining low communication overhead and protecting sensitive data.

IV. DATA ACQUISITION AND SECURE DATA PREPARATION

The purchase and pre-process of the data before any cryptography action is undertaken on the data are key in the safe data sharing of the IoT operating environments. The IoT devices produce mass of unstructured data in unidentified formats produced by different sensors within the environment. This is why it is extremely important to ensure that the process of data preparation is efficient so that the obtained data will be in a proper format which also will allow it to be encrypted safely and shared. In this case, we are talking of the process of information-gathering within the IoT sensors, data consideration to be shared in a secure manner, and features concerning heterogeneous information of sensors within a distributed environment.

A. IoT Data Collection and Normalization

The proposed system will use the data produced by the IoT devices e.g. sensors, monitoring devices and infrastructure systems that are smart. The IoT devices learn a lot about the context of the surrounding or they work in a real time manner. The data received by the IoT devices can be of different devices in different format and communication protocols. Therefore data normalization is necessary in giving constant presentation of information derived before encryption Normalization stage deals with the formatting of the raw information collected by the sensor into a standard format that ensures that the information is in a safe format since it is still subjected to encryption module. The IoT data management system tends to perform the data processing in a normal form or familiar form by normalizing the data provided on the system and in so doing optimization of outliers in the final data set that is derived [1], [2]. In general, the data encryption procedure will be performed in the most efficient manner possible due to normalization of the information, which was collected with the help of the IoT devices.

B. Secure Data Representation

After the data has undergone the process of data normalization, this is followed by coding the data in a safer manner so as to offer effective coding of data by the encryption unit in the IoT model. The data received with the help of IoT is perceived as confidential message, which should be transmitted in a secure manner to the cloud system according to the application of the public key cryptography that does not allow the third party to read it and comprehend its content, according to the suggested model of IoT. The resulting normalized data is then encrypted using the NTRU cryptosystem, which is a quantum resistant lattice based system with a high level of efficiency and fast with low power consumption per cycle [6].The NTRU cryptosystem is also based on the ring structure of the polynomials and offers an efficient sorting out and de-sorting of the data which is vital in the issuance of the IoT technique when the resources are scarce.

C. Key Generation and Distribution

Key generation and distribution: In order to get efficiency in encryption of the data, there must be key generation and distribution systems of the system that would be effective. According to the suggested system, the cryptographic keys are created by Elliptic Curve Cryptography (ECC) key generation algorithm that is extremely efficient in key creating applications in the IoT and offers high efficiency with format keys, compared to standard implementation briefs. The system after generating the keys to the encryption uses the threshold-based secret sharing approach through which the decryption key is shared to the system stakeholders. [2]. This means that the secret key will be distributed to the stakeholders in the proposed system through the secret sharing technique whereby in the system the shared key will be distributed to the stakeholders in the form of shares and when a specific number of stakeholders combine with the rest, the secret will be reconstructed [4], [15].

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13382

D. Handling Data Security Challenges

The problems with data security in the IoT setting are mainly founded on the different architecture of devices, the constrained capacity of the devices to perform computation and protection of data in communication. Conventional encrypting algorithms also require the presence of multiple retransmitters in the encrypted part of the data, which consumes more resources in data transmission and consumes more energy when used by an IoT device. It is suggested that the above model is formulated to accommodate the problem of data security in the IoT set ups by encrypting the information only once and transferring the decryption key fragments and to the stakeholders through the proxy re-encryption approach. In Proxy Re encryption, the semi-trusted proxy server may encrypt the ciphertexts as it pleases to be re-decrypted by the authorized parties without enabling the server to see the actual plaintext that is being encrypted, see refs. proxy re-encryption [7], [12].

E. Prepared Data for Secure Sharing

After a safe preparation of data is done, the information in the IoT is encrypted to key shares to the legitimate participants. The first aspect of data sharing in the proposed system architecture is the prepared data. The information will be decrypted, and it is only accessible on getting sufficient number of participants key sharing. Protection of data in the IoT of the proposed system architecture can be done through the development of encryption, secret sharing and proxy re- encapsulation. The ready data format is efficient in resourcefully sharing the data between the distributed participants in a safe way without affecting the confidentiality of the data and unauthorized access.

V. PROPOSED FRAMEWORK

The paper has proposed a lean and secure data sharing model that may be introduced in the context of the IoT system because IoT devices are very minimal in terms of both computing and communicating abilities. Classical paradigm of introducing the secure multi-party and computing and sharing secrets implies that IoT devices will be obliged to send multiple encrypted values to the various nodes, which it will be impossible to accomplish since only little can be sent by the IoT devices. This weakness is overcome by the proposed framework that encrypts the IoT data and distributes its decryption key into little and minute segments and sends them to the stakeholders as the threshold cryptography and proxy re-encryption approaches. The indicated framework is grounded in the Elliptic Curve Cryptography with the NTRU cryptosystem involved and some specific secret sharing schemes in cooperation with the assistance of the proxy re-encryption schemes, which predetermines the protection and scalability of the proposed framework at the same time [4], [6], [7].

A. Overall System Architecture

The proposed framework is a modular system structure, with five important components:

i. *IoT Device Layer:* The IoT devices get access to sensor data as monitoring sensors, scaling and, application specific monitoring sensors. Such IoT devices are poorly equipped on the aspect of processing power and merely transfers the data that it has collected to the safe processing system.

ii. *Encryption Engine:* The NTRU protection makes use of the encryption of data gathered. NTRU is a lattice-based cryptography algorithm which is an efficient encryption algorithm, quantum computing resistance, and high computing power to support the IoT devices, among others [6].

iii. *Key Management Module:* Elliptic curve Cryptography can be used to come up with cryptographic keys. The algorithm produces and transmits key-sensitive keys and reduces the key sizes in the resource-constrained devices minimum amount of resources are required to execute it [2].

iv. *Secret Sharing and Proxy Re-Encryption Module:* The decryption key is partitioned into various shares under another scheme which is known as a threshold secret sharing scheme. The proxy re-encryption schemes isolate the stock among the various parties. The shares are re-encrypted in proxy server to allow the numerous participants to view them in order to not disclose the true key of the shares to the participants [7], [12].

v. *Stakeholder Access Layer*: The authorized stakeholders are to jointly issue decryption key to the key shares. One can only access the encrypted information on the IoT under the condition that a specific number of participants would collaborate to address this scheme.

B. Secure Data Sharing Workflow

The secure data sharing process consists of the following steps:

i. IoT devices consider sensor data and encrypt.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13382

ii. The sensor readings occupied by the IoT gadgets are transmitted to the encryption module that submits the same to the encrypted form of the NTRU cryptosystem.
iii. The generation of decryption key is done on ECC based item key management.
iv. The encrypted item A threshold secret sharing scheme is utilized in sharing the decryption key by use of secret sharing based on the use of item A threshold secret sharing scheme.
v. The IoT devices encrypt the data and send on the proxy server which redirects it to a proxy re- encryption server.
vi. One can define item Proxy re-encryption scheme as the scheme where the key shares are encrypted and sent to different stakeholders who have the authority to access them.
vii. When a condition has been reached, then decryption of the encrypted IoT data takes place.

The given workflow does not mean that the IoT devices will be obliged to transmit a certain amount of encrased shares. In this manner, overhead on communication would be significantly reduced.

C. *Threshold-Based Decryption Mechanism*

The suggested model will have the capacity to use the Key-Split Threshold Decryption protocol to achieve enhanced security as well as to spread the trust among the several parties comprising the scheme. The offered mechanism will separate the decryption key into n shares and the threshold of t shares. In order to avoid each party gaining access to the data separately to ensure the security against the insider attacks as well as the unauthorized access threshold cryptography is applied. Such a distributed trust is typically used to conduct a multi-party computation in order to offer security to sensitive information [4], [5]. Dissection and advancement of multi party homomorphic secret sharing schemes to give security to the calculation activity have lately attracted a compilation of attention to craft enhanced multi-party techniques to the homomorphic secret sharing of information by multiple parties with enhanced security attributes [13].

D. *Security and Scalability Considerations*

The protection and scalability of the structure is superior compared to the conventional ways of secure data sharing. This is because in his model the data is encrypted and solely once instead of the ciphertext shares key shares whereby the communications costs are decreased. The lattice-based encryption on its part allows the security to be assured even during quantum attacks. The modular construct is also used in the assurance that the original data does not require re-encryption because there is a possibility of new parties entering the system and, consequently, eradicating them, which is why modular construct can be utilized in the IoT model with the parties requiring it continuing to change.

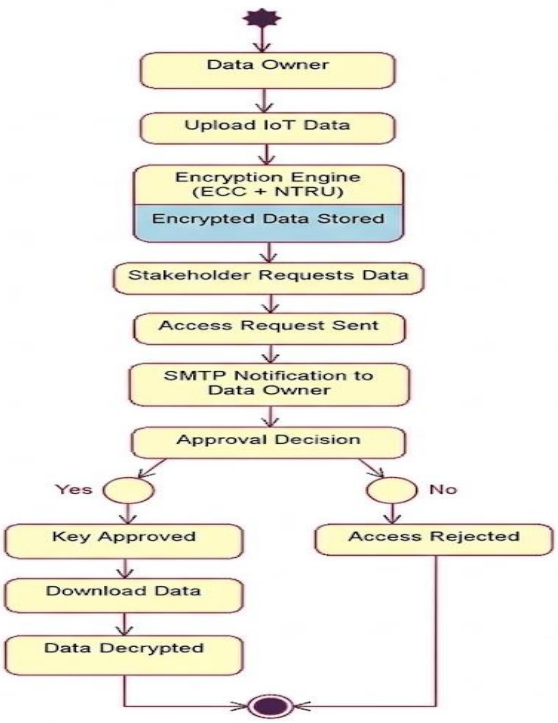

Fig. 1: Flow Chart of the proposed procedure of distributing the IoT Data in a safe manner.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13382

Therefore, the suggested architecture can be applied to the IoT applications, making sure that the security, scaling, and effectiveness of data sharing within the distributed systems.

VI. RESULTS AND DISCUSSION

This part will discuss the results of implementing the proposed framework of the secure IoT data sharing based on the outcomes of the experiment carried out. In this regard it has implemented the system as a web based system with the inclusion of the NTRU encrypted secret sharing methods, ECC based key management and proxy re-encryption techniques. The given section primarily serves to outline the proposed secure IoT data sharing framework experimental results and findings.

A. System Implementation and Interface

At this stage the proposed data sharing framework of the secure IoT was implemented as web-based platform and different parties could interact with the system through application of varied interfaces including data owners, parties and system administrators. Figure 2- system home page reveals the home page of the installed system of IoT SecureShare in the ionic environment sharing the data in a safe way. The system interface allows users to input different modules in the system which comprise data owner log in, stakeholders and cloud dashboard. The system has also provided a special interface where the data owner can upload the data on the cloud and encrypt the data before being deposited in the cloud.

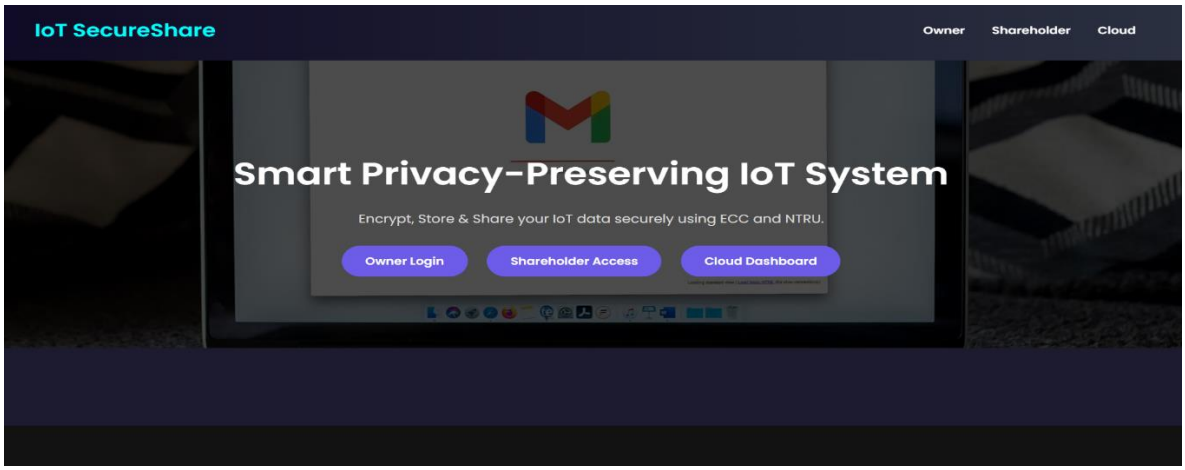

Fig. 2: Homepage of the IoT SecureShare platform

B. Data Encryption Process

The system has provided the facility of encrypting the IoT information using the ECC and NTRU algorithm before the data is stored in the cloud. Figure 3 provides an image of the encryption interface on which the user was able to add the sensor data and encrypt the data. The system has also provided the possibility of storing the encrypted data and keys after the encryption already has been made. This is a hint that is the sensitive IoT that the system is effectively encrypting.

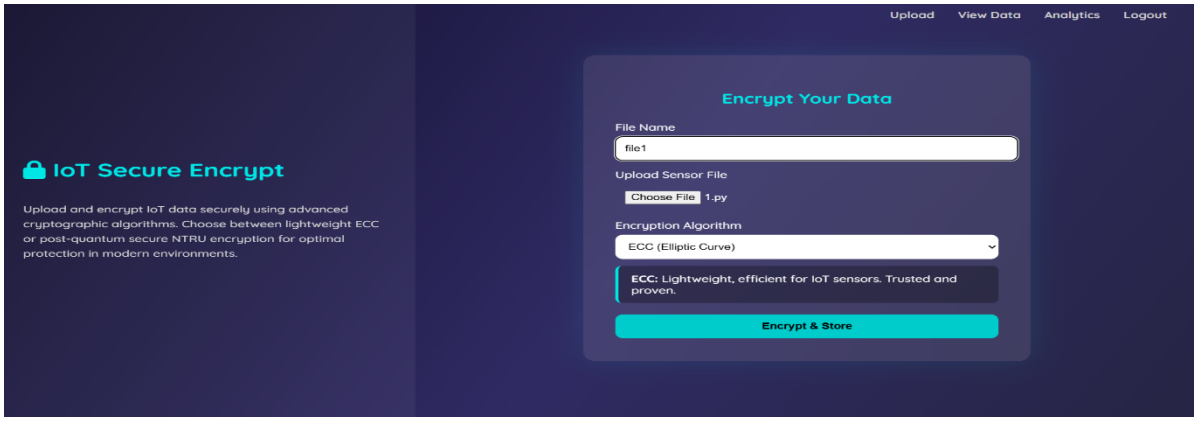

Fig. 3: Human IOT Data Encryption Interface with ECC and NTRU

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13382

C. *Secure Data Access Workflow*

Secure Data Access Workflow provides consideration of the various stages that are involved in this protection efforts. Once the encrypted data is stored to the system, the authorized stakeholders will be capable of searching the available data in the IoT and force retrieval of the data. Figure 4 below is the interface of the search data through which the stakeholders searched and ordered the encrypted IoT data in the system.

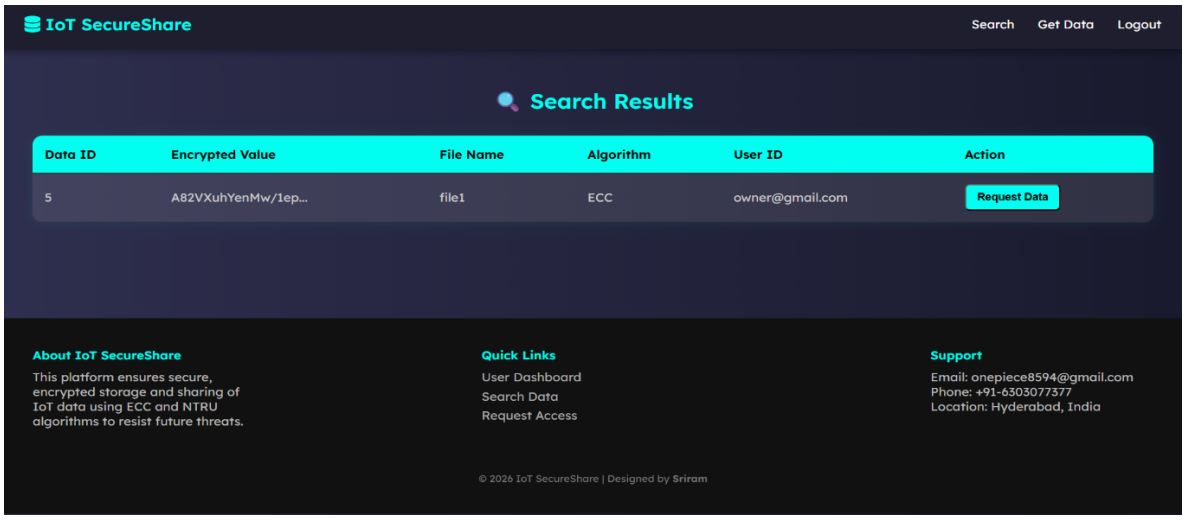

Fig. 4: Search Interface for Encrypted IoT Data

The owner of data will be informed of the success of the request of the data by the stakeholders through the system through SMTP protocol service that will send the approval message. This will offer the secure admission of the information.

D. *Access Control and Approval Mechanism*

The process of approval will merely ensure that the encrypted data is only distributed to the relevant stakeholders. The approval received in the email as provided in Figure 5 demonstrates the email approval that the data owner will receive to inform him/her that the system had approved him/her. The data in the system can be downloaded by the stake holders and the data can be accessed with the permission of the data owner to the data access request as well as using the authorized key.

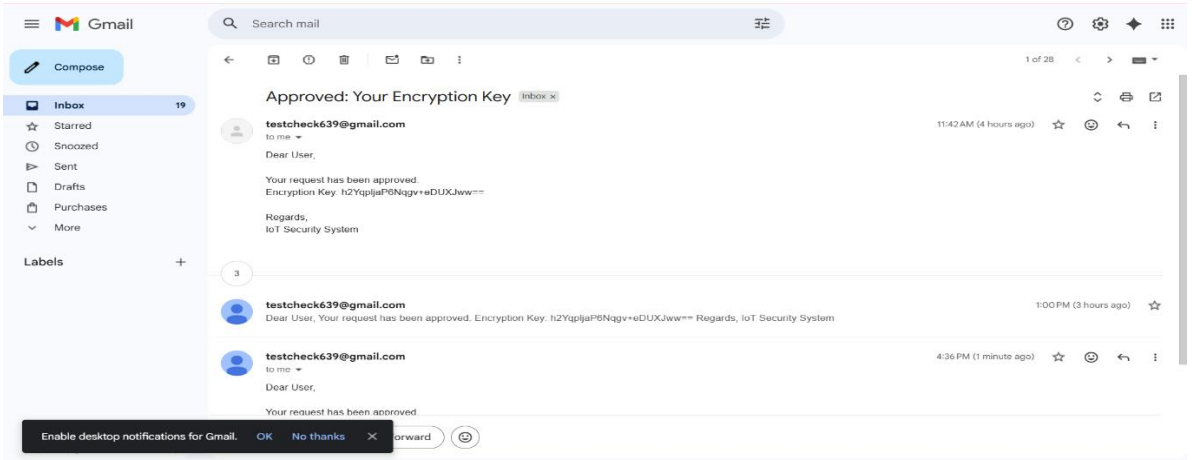

Fig. 6: Analytics and monitoring dashboard of the proposed system

E. *System Monitoring and Performance Analysis*

The dashboard is cloud-based displaying mechanisms of the performance monitoring of the system in the forms of encryption analytics, user monitoring and the performance analysis. The description of the analytics dashboard Figure 6 is the dashboard that is used to watch the process of uploading encrypted data in the IoT and system performance.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13382

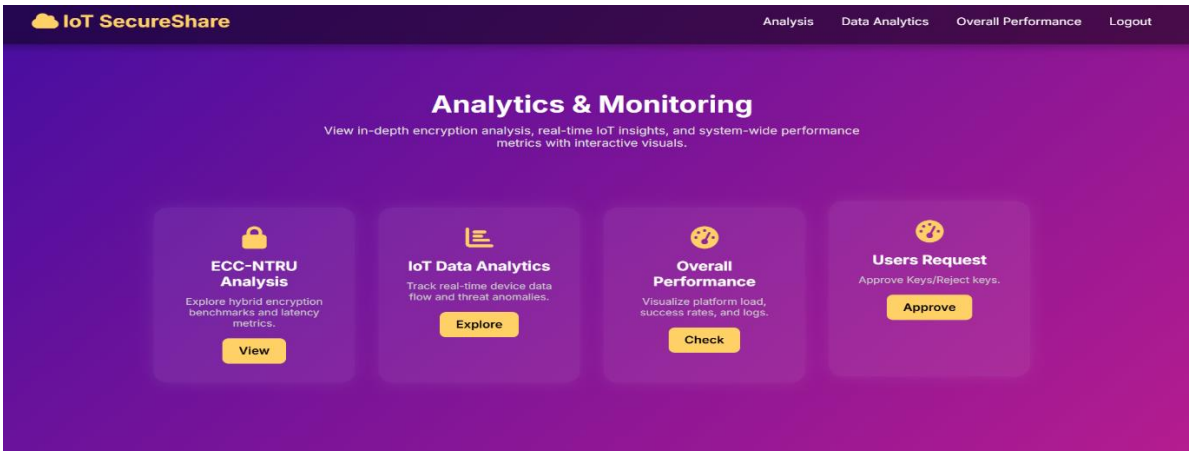

Fig. 6: Analytics and monitoring dashboard of the proposed system

F. *Discussion*

According to the outcomes of the experiments, it can be assumed that the encrypted system and access control integration made in the proposed system has been undertaken successfully. The NTRU algorithm of encryption is applied, providing the best encryption speed to the proposed system as an element of the IoT-related application. Also the secret sharing mechanism has been utilized to provide powerful security to decryption keys to unauthorized access. Besides, proxy re encryption scheme is also effective in access security. According to the results of the experiment, it becomes obvious that the suggested system can provide effective security and efficiency in regards to maintenance of privacy in the disclosure of the IoT data.

VII. CONCLUSION AND FUTURE SCOPE

Through ECC, NTRU, secret sharing, and proxy re encryption technologies, this paper has suggested a safe and scalable framework which can form a method of sharing IoT data in a privacy-saving manner. The proposed system eliminates issues of sharing and securing data through legacy methods of data sharing which entails many encrypted trans missions by the low resource IoT devices. The suggested technique encrypts the data only once and transmits the decryption key to the interested parties through the threshold technique that reduces the communication cost and offers optimum security level to the information. The experiment has effectively demonstrated the applicability and feasibility of the suggested framework by utilizing the suggested framework by the deployment of the suggested web application that could be applied in uploading, encrypting and decrypting the information through the suggested strategy. It is possible to shape the further work to the more advanced cryptographic methods and intelligent data management systems that can be employed in the future work. In this system, some of the examples include its flexibility in a large-scale IoT network, which makes use of some advanced key management systems or threshold policies. A transparent audit trail on access requests and approvals can be delivered by using a blockchain technology integration. Moreover, the monitoring systems can be enhanced through the application of machine learning-based anomaly detection systems or by employing advanced data analysis tools of the IoT in this framework. All of this can be applied to make this framework more practical in the real-life situation and at the same time provide the privacy and security assurance.

REFERENCES

[1]. P. P. Ray, “A survey of iot cloud platforms,” Future Computing and Informatics Journal, vol. 1, no. 1-2, pp. 35–46, 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, no. 3, pp. 269–284, 2016.

[3]. 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, 2020.

[4]. D. Evans, V. Kolesnikov, and M. Rosulek, A Pragmatic Introduction to Secure Multi-Party Computation. Now Publishers, 2018.

[5]. I. Damg˚ard, V. Pastro, N. Smart, and S. Zakarias, “Multiparty computation from somewhat homomorphic encryption,” in Advances in Cryptology– CRYPTO. Springer, 2012, pp. 643–662.

[6]. A. Marandi, P. G. M. R. Alves, D. F. Aranha, and R. H. Jacobsen, “Lattice-based homomorphic encryption for privacy-preserving smart meter data analytics,” The Computer Journal, 2023.

DOI: 10.17148/IARJSET.2026.13382

[7]. Z. Qin, H. Xiong, S. Wu, and J. Batamuliza, "A survey of proxy re encryption for secure data sharing in cloud computing," IEEE Transactions on Services Computing, 2016.

[8]. C. Marcolla, V. Sucasas, M. Manzano, R. Bassoli, F. Fitzek, and N. Aaraj, "Survey on fully homomorphic encryption: Theory and ap plications," Proceedings of the IEEE, vol. 110, no. 10, pp. 1572–1609, 2022.

[9]. M. Burkhart, M. Strasser, D. Many, and X. Dimitropoulos, "Sepia: Privacy-preserving aggregation of multi-domain network events and statistics," in USENIX Security Symposium, 2010, pp. 223–240.

[10]. 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, no. 3, pp. 3555–3572, 2023.

[11]. Q. Zhang, C. Xin, and H. Wu, "Privacy-preserving deep learning based on multiparty secure computation: A survey," IEEE Internet of Things Journal, vol. 8, no. 13, pp. 10412–10429, 2021.

[12]. R. Canetti and S. Hohenberger, "Chosen-ciphertext secure proxy re encryption," in ACM Conference on Computer and Communications Security. ACM, 2007, pp. 185–194.

[13]. I. Chillotti, E. Orsini, P. Scholl, N. P. Smart, and B. Van Leeuwen, "Scooby: Improved multi-party homomorphic secret sharing based on fhe," in Security and Cryptography for Networks. Springer, 2022, pp. 540–563.

[14]. 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, no. 12, pp. 9259–9267, 2022.

[15]. J. Herranz, A. Ruiz, and G. Saez, "New results and applications for multi-secret sharing schemes," Designs, Codes and Cryptography, vol. 73, no. 3, pp. 841–864, 2014

