ISSN 2319-5991 www.ijerst.com

Peer Reviewed, Referred & Indexed Journal

Research Paper

INFORMATION-THEORETIC SECURE USER AUTHENTICATION VIA SECRET SHARING COMPUTATION

BIRU SHIVA [1], MULINTI VINAY [2], KADIRA LOKESH REDDY [3], KAMMARI BHANU PRASAD [4], KATTA SHASHANK [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— When using an insecure communication channel, the initial step involves authenticating the user (verifying the other party) to ensure the legitimacy of the communication partner, followed by encrypted communication. With the advancement of quantum computers, many conventional cryptographic techniques are at risk of being deciphered. While post-quantum cryptographic approaches are under development, they often demand substantial computational resources, making them difficult to implement in resource-constrained environments such as the Internet of Things (IoT). This study proposes a user authentication and secure communication system that guarantees information-theoretic security by leveraging secure computation based on a computationally lightweight (k, n)-threshold secret sharing scheme. The proposed authentication approach utilizes constantly changing information to prevent replay attacks and enhance security. It is further demonstrated that secure communication with information-theoretic guarantees can be achieved without the need to distribute a large volume of true random numbers, relying instead on secret sharing-based secure computation. The proposed methods are particularly suitable for IoT applications due to their minimal processing overhead and efficient performance.

Index Terms – User authentication, secure communication, threshold secret sharing,

(k, n)-threshold scheme, secure computation, information-theoretic security, post-quantum cryptography, Internet of Things (IoT), replay attack prevention, lightweight cryptography, quantum-resistant security, resource-constrained devices.

I. INTRODUCTION

In communication over an insecure channel, the initial step involves performing entity authentication (user authentication) to verify the legitimacy of the parties involved. The purpose of user authentication is to confirm the identity of a person. Password-based identification is the most commonly used method of user authentication. Passwords are commonly used for user authentication over communication channels and the Internet, where an encrypted password is transmitted and remains unchanged until it is updated. Consequently, if an attacker intercepts an encrypted password, they can potentially pose as a legitimate user. Therefore, it is advisable to regularly update the passwords. For user authentication alternatives to passwords, the known methods involve shared secret information (excluding those that utilize physical tokens such as identification cards or biometric traits). Several approaches have been discussed, including token-based authentication challenge-and-response (C-R) protocols using symmetric key encryption and digital signatures. However, the token-based method requires a device that coordinates and produces random numbers, known as tokens, between the claimant and the verifier. This device must also be physically carried as required. The C-R method remains secure provided that the password is securely exchanged between the claimant and the verifier, thereby eliminating the need to transmit the password directly over the communication channel. However, this method requires a minimum of two communication phases, challenge and response. Furthermore, there are concerns that the existing cryptographic codes can be readily decrypted with the advent of quantum computing. The Vernam cipher, recognized for its perfect information theoretical security, was deemed secure. However, its practical application is hindered by the necessity of exchanging a substantial volume of random numbers as keys between the claimant and the verifier. Because the conventional C-R method employs a combination of a password and a hash function that provides computational security, it provides only computational security. Moreover, although digital signatures are implemented using public key

encryption, they are secured only under computational security assumptions and lack information-theoretic security. Computational security implies that the security can be compromised if an adversary has unlimited computing resources. However, information-theoretic security remains secure, even when an adversary has infinite computational power. The threat that digital signatures based on traditional public key encryption may be vulnerable to quantum-computing attacks has recently become more pronounced. Consequently, there has been extensive research into a type of cryptography known as post-quantum cryptography, which remains secure against quantum computing attacks; however, it requires significant computational resources and effort. In contrast, the (k, n)-threshold secret sharing scheme is recognized for its information-theoretic security. This method transforms a single secret into n distinct values, known as shares. This enables the reconstruction of the original secret by collecting any k of the n shares. Furthermore, possessing fewer than k shares does not yield knowledge of the secret. Examples include Shamir's (k, n) method, Blakley's method, and additive secret sharing method. These methods are commonly used in applications such as secure information storage and management across multiple server environments, multiparty computation and searchable encryption. They are yet to be applied to user authentication in communication channels, to the best of our knowledge. Conversely, the Vernam cipher demands substantial storage space because of the pre-sharing of numerous true random numbers between the sender and the receiver, which renders it impractical for lightweight devices such as Internet of Things (IoT) devices. Looking ahead to Society 5.0, it is crucial to have user (or device) authentication and secure communication in IoT environments, which require lightweight and highly secure methods.

II. RELATED WORK

A. Improved protocols for secure multiplication using secret sharing scheme

The project "Improved Protocols for Secure Multiplication Using Secret Sharing Scheme" focuses on developing an enhanced and efficient approach for performing secure multiplications in a distributed environment without exposing any private data of the participants. In traditional secure computation, ensuring data privacy during arithmetic operations

like multiplication is a major challenge, especially when dealing with multiple parties or servers. This project aims to overcome such challenges by improving the (k, n)-threshold secret sharing scheme, which divides a secret into multiple shares distributed among different entities, ensuring that no single party can reconstruct the secret alone.

The improved protocol enhances computational efficiency, communication cost, and fault tolerance while maintaining information-theoretic security, meaning the data remains protected even against adversaries with unlimited computational power. It ensures that secure multiplication can be performed collaboratively using shared values, without revealing the underlying secrets. The proposed method is designed to be lightweight and scalable, making it suitable for IoT systems, cloud computing, and secure data outsourcing applications.

Additionally, the protocol minimizes the number of communication rounds required for multiplication, thereby increasing performance in real-time applications. Overall, the project aims to achieve secure, efficient, and privacy-preserving computation by optimizing secret sharing techniques for modern distributed systems.

B. A block chain-based approach to ensuring the security of electronic data

The project "A Block Chain-Based Approach to Ensuring the Security of Electronic Data" aims to develop a decentralized and tamper-proof framework that guarantees the integrity, confidentiality, and authenticity of digital information. With the increasing volume of electronic data exchange across networks, traditional centralized security models face challenges such as data breaches, unauthorized access, and single points of failure. This project leverages the immutable and transparent nature of block chain technology to overcome these limitations. By storing data or its cryptographic hashes across distributed nodes, the system ensures that any unauthorized alteration is easily detectable. Smart contracts are integrated to automate verification and access control, enabling trust less and secure transactions without intermediaries.

The project also incorporates cryptographic techniques like hashing and digital signatures to enhance data privacy and authenticity. Furthermore, it supports data traceability and auditability, allowing users to verify the complete history of information changes. The framework is particularly beneficial for applications like healthcare,

finance, and government data management, where trust and data accuracy are critical.

Overall, this project provides a secure, transparent, and decentralized solution that protects electronic data from tampering, fraud, and unauthorized manipulation in modern digital ecosystems.

C. Privacy preserving multi-party multiplication of polynomials based on (k, n) threshold secret sharing

The project "Privacy-Preserving Multi-Party Multiplication of Polynomials Based on (k, n) Threshold Secret Sharing" focuses on developing a secure and efficient protocol that enables multiple parties to jointly perform polynomial multiplication without revealing their private inputs. In many collaborative computations, such as data analytics or cryptographic systems, participants need to compute on sensitive data while maintaining confidentiality. This project leverages the (k, n) threshold secret sharing scheme, where a secret is divided into n shares and only k or more shares are required to reconstruct it, ensuring information-theoretic security even against powerful adversaries. The proposed system allows each participant to perform computations on their shares independently, enabling secure polynomial multiplication through shared computations without disclosing individual coefficients. The protocol ensures that no single party gains access to the original data while still achieving accurate collective results. It is designed to minimize communication rounds, computational complexity, and storage overhead, making it suitable for resource-constrained and distributed environments. Furthermore, the system enhances privacy, scalability, and fault tolerance in multiparty computation frameworks. The project's main objective is to achieve privacy-preserving collaborative computation while maintaining high efficiency and security, which can be applied in domains like secure data aggregation, cloud computing, and encrypted machine learning.

D. Secure user authentication and key agreement scheme for IoT device access control based smart home communications

The project "Secure User Authentication and Key Agreement Scheme for IoT Device Access Control Based Smart Home Communications" focuses on developing a robust and lightweight authentication framework to ensure secure communication and access control among IoT devices in smart home environments. With the rapid

growth of smart home technologies, numerous interconnected devices exchange sensitive data, making them vulnerable to unauthorized access, replay attacks, and data breaches. This project proposes a mutual authentication and key agreement mechanism that verifies both users and devices before granting access. The system generates session keys dynamically to establish secure communication channels, ensuring confidentiality and integrity of transmitted data. It uses lightweight cryptographic operations suitable for resource-constrained IoT devices, thereby reducing computational and communication overhead. The protocol resists common network threats such as man-in-the-middle, impersonation, and eavesdropping attacks, ensuring privacy preservation. Additionally, it supports scalability and interoperability among diverse IoT devices through efficient key management and secure session initiation. The scheme enhances trust and reliability within smart home networks by integrating authentication with real-time key agreement. Overall, the project aims to provide a secure, efficient, and user-friendly IoT access control solution that safeguards smart home communications against evolving cyber threats while maintaining system performance.

III. PROPOSED METHODOLOGY

The proposed system introduces a secure user authentication and communication method that provides information-theoretic security by leveraging a lightweight (k, n)-threshold secret sharing scheme combined with secure computation techniques.

Instead of relying on traditional encryption or computational hardness assumptions, the system divides sensitive authentication data into multiple shares and distributes them among different entities. Only a subset (k out of n) of these shares is required to reconstruct the original data, ensuring that partial exposure of shares does not compromise security.

The authentication process utilizes dynamically changing information, such as session-based values or timestamps, to prevent replay attacks and improve robustness. Moreover, secure communication between entities is achieved without the need to distribute large quantities of random keys or perform heavy cryptographic operations, making the system highly suitable for resource-constrained environments like IoT devices. This design ensures both strong security and practical efficiency in real-world applications.

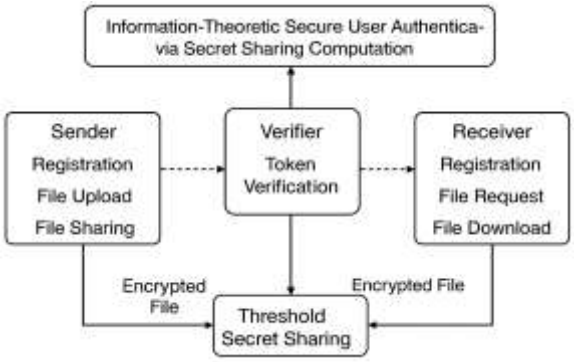


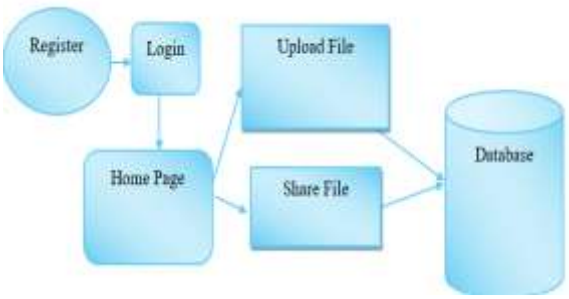
Fig. 1: System Overview

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. Sender (Data Upload)

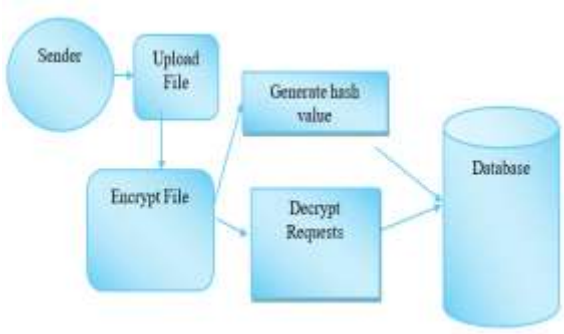
The Sender module is responsible for initiating the secure data-sharing process within the system. When a sender registers, a unique hash value is generated using the SHA-256 algorithm to ensure identity integrity and prevent tampering. Along with this, a public and private key pair is generated using the RSA encryption algorithm to enable secure encryption and decryption operations. Once the registration details are verified by the Verifier module, a token ID is assigned to the sender to validate his authenticity within the network. After successful verification, the sender can upload files, which are then encrypted using RSA, ensuring that only the intended receiver can decrypt the data. A unique secret key is generated for each uploaded file to enhance confidentiality. Additionally, the sender has access to verify and manage decryption requests received from receivers, approving them to securely distribute the secret key necessary for file access.



3. SHA-256

The SHA-256 module is used to generate a unique cryptographic hash value for each user during registration. As part of the

Secure Hash Algorithm (SHA-2) family, SHA-256 produces a 256-bit hash that is practically impossible to reverse-engineer or duplicate, ensuring strong identity protection. In this project, it is employed to verify user integrity and prevent impersonation or replay attacks. Since even a minor modification in the input data results in a completely different hash output, SHA-256 ensures that every sender and receiver maintains a distinct and tamper-proof identity. This module forms the foundation of trust and authentication within the system, guaranteeing that all registration data remains secure and immutable throughout the communication process.



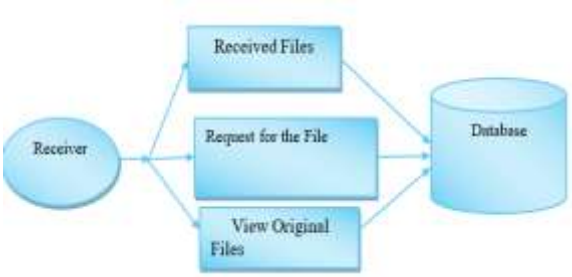
4. Threshold Secret Sharing Scheme

The Threshold Secret Sharing Scheme module enhances the information-theoretic security of the system by enabling secure computation and key management without exposing sensitive data. Based on the (k, n)-threshold scheme, the secret (such as a cryptographic key) is divided into n shares, and only k or more shares are required to reconstruct the original secret. Possessing fewer than k shares reveals no information, ensuring absolute confidentiality even if some shares are compromised. In this project, this mechanism strengthens the key distribution and verification process, ensuring that the secret key used for file decryption is securely managed and shared only with authorized entities. This approach makes the system quantum-resistant and suitable for IoT and lightweight environments, providing privacy-preserving authentication and secure communication that remains robust against both classical and quantum attacks.

5. RSA

The RSA module forms the core encryption and decryption component of the project, ensuring confidentiality and secure data transmission. During registration, each user (sender and receiver) is assigned a unique RSA public and private key pair. The public key is shared for encryption, while the private key is securely retained for

decryption. When a sender uploads a file, it is encrypted using the receiver's public key, ensuring that only the intended receiver can decrypt it with their corresponding private key. RSA also plays a vital role in digital authentication, confirming that data originates from verified users. By using asymmetric cryptography, the system achieves strong protection against unauthorized access, man-in-the-middle attacks, and data interception, ensuring secure end-to-end communication between sender and receiver.



6. JSP Dashboard

Displays the uploaded encrypted data along with file details and timestamps. It also shows the transaction status, verification results, pending registration details, and overall project modules. The dashboard acts as the user interface for monitoring stored data, status, and user details etc.

7. MySQL Database

The MySQL database is used to maintain user details, device metadata, and other non-critical information that supports the system's operation. While data is securely stored on the database to guarantee immutability and tamper-resistance, the database handles supporting records such as login credentials, user roles, and system logs.

This hybrid storage approach ensures both efficient system performance and strong data security by separating critical data from auxiliary information.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

The experimental results show that the proposed secret sharing-based authentication scheme provides information-theoretic security while maintaining low computational overhead. The use of (k, n)-threshold secret sharing and dynamically changing authentication information effectively prevents replay attacks and enables secure communication without distributing large amounts of random data. The lightweight design makes the scheme well suited for IoT and other resource-constrained environments.

Fig. 2: Home Page

Fig. 3: Registration

Fig. 4: Shared Files

Fig. 5: Encrypted Data

V. CONCLUSION

The Conclusion of the project "Information-Theoretic Secure User Authentication via Secret Sharing Computation" emphasizes the successful development of a lightweight, secure, and quantum-resistant communication framework. The proposed system ensures information-theoretic security by integrating SHA-256 hashing, RSA encryption, and the (k, n)-threshold secret sharing scheme, providing robust authentication and secure file transmission between the Sender, Receiver, and Verifier. Unlike conventional cryptographic systems that rely on computational hardness, this approach guarantees protection even against quantum attacks. The Verifier effectively authenticates users by validating hash values and public keys, ensuring only legitimate entities participate in communication. The Sender can encrypt and share files securely, while the Receiver can request and decrypt files upon approval, maintaining end-to-end confidentiality. The system also minimizes the need for heavy computation, making it suitable for IoT and edge-based environments. By employing threshold secret sharing, the proposed model distributes trust and prevents single points of compromise. Overall, this project demonstrates an efficient and secure user authentication mechanism that achieves

privacy, integrity, and authentication with minimal computational cost, paving the way for future advancements in post-quantum secure communication frameworks.

REFERENCES

[1] C.-L. Lin and T. Hwang, "A password authentication scheme with secure password updating," *Comput. Secur.*, vol. 22, no. 1, pp. 68–72, Jan. 2003.

[2] I.-E. Liao, C.-C. Lee, and M.-S. Hwang, "A password authentication scheme over insecure networks," *J. Comput. Syst. Sci.*, vol. 72, no. 4, pp. 727–740, Jun. 2006.

[3] S. K. Sood, A. K. Sarje, and K. Singh, "Cryptanalysis of password authentication schemes: Current status and key issues," in *Proc. Int. Conf. Methods Models Comput. Sci. (ICM2CS)*, Dec. 2009, pp. 1–7.

[4] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," *Proc. IEEE*, vol. 91, no. 12, pp. 2021–2040, Dec. 2003.

[5] M. Dammak, O. R. M. Boudia, M. A. Messous, S. M. Senouci, and C. Gransart, "Token-based lightweight authentication to secure IoT networks," in *Proc. 16th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2019, pp. 1–4.

[6] H. Bojinov and D. Boneh, "Mobile token-based authentication on a budget," in *Proc. 12th Workshop Mobile Comput. Syst. Appl. (HotMobile)*, 2011, pp. 14–19.

[7] K. Rhee, J. Kwak, S. Kim, and D. Won, "Challenge-response based RFID authentication protocol for distributed database environment," in *Security in Pervasive Computing (SPC)*, vol. 3450, D. Hutter and M. Ullmann, Eds. Berlin, Germany: Springer, 2005, pp. 70–84, doi: 10.1007/978-3-540-32004-3_9.

[8] A. Hiltgen, T. Kramp, and T. Weigold, "Secure internet banking authentication," *IEEE Secur. Privacy*, vol. 4, no. 2, pp. 21–29, Mar./Apr. 2006.

[9] Y. Shoukry, P. Martin, Y. Yona, S. Diggavi, and M. Srivastava, "PyCRA: Physical challenge-response authentication for active sensors under spoofing attacks," in *Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, 2015, pp. 1004–1015.

[10] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978.

AUTHORS Profile

Mr. BIRU SHIVA has received his B. Tech in CSE from JNTUH, Hyderabad in 2013, M. Tech in Computer Science and Engineering from JNTUH, Hyderabad in 2016 and He has been dedicated to the teaching field for the last 6 years. At present he is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India.

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

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

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

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