Secure User Authentication And Data Sharing For Mobile Cloud Computing Using RIPEMD-160 And NTRU Encrypt

Kannan Srinivasan
Saiana Technologies Inc, New Jersy, USA
kannan.srini3108@gmail.com
Senthilkumar K
Department of Electrical and Electronics Engineering, V.R.S College of Engineering & Technology
senthil.kothandapani@gmail.com

ABSTRACT
Background: With mobile cloud computing's rapid growth, safeguarding data and ensuring efficient user authentication have become critical. Traditional methods are resource-intensive and vulnerable to advanced threats like quantum computing.
Objective: To develop a secure, quantum-resistant framework using RIPEMD-160 hashing and NTRUEncrypt encryption, optimizing data security and resource efficiency for mobile cloud environments.
Methods: This framework integrates RIPEMD-160 for robust user authentication and NTRUEncrypt for quantum-safe data encryption. Blockchain technology is incorporated for decentralized key management and secure transaction logging.
Results: The combined framework showed significant improvements in collision resistance, throughput, energy efficiency, and overall security, surpassing the performance of standalone algorithms.
Conclusion: This hybrid approach offers strong data protection and efficient user authentication, presenting a viable solution for evolving security needs in mobile cloud computing.
Keywords*: Mobile cloud security, quantum-resistant encryption, RIPEMD-160, NTRUEncrypt, decentralized key management.*

1 INTRODUCTION

Mobile cloud computing has emerged as a key component of both personal and business data management in the current digital era. But as the use of mobile cloud platforms increases, so does the demand for safe and efficient ways to guard private data against interception, data breaches, and illegal access. When used on mobile devices, traditional security approaches frequently fail because they can be computationally taxing, depleting device resources, and may not adequately handle the particular vulnerabilities of mobile cloud systems. A strong framework that combines effective data security with user authentication to guarantee secure interactions within mobile cloud settings has been developed in response to these issues. It makes use of RIPEMD-160 hashing and NTRUEncrypt encryption.

A balanced approach to data security and authentication is produced by the complimentary advantages of the RIPEMD-160 and NTRUEncrypt algorithms. The 160-bit cryptographic hash function RIPEMD-160 is well-known for its resilience against frequent attacks that target unsecured data, such as collision and preimage attacks. RIPEMD-160 provides robust security for user identities by transforming user credentials into a secure, irreversible hash, particularly in mobile situations with constrained computing power and battery life. This hash

function keeps the user experience smooth while enhancing security by assisting with user authentication without the weaknesses frequently found in conventional password-based systems.

In order to satisfy the requirement for robust encryption in mobile cloud systems, NTRUEncrypt improves this framework by protecting data while it is being transmitted. In contrast to traditional techniques like RSA or ECC, and this might not survive quantum-powered breaches, NTRUEncrypt is a future-proof option because it is a lattice-based encryption algorithm that is immune to the sophisticated attacks that quantum computing may bring. As computing technology develops, data encrypted with NTRUEncrypt remains safe because of its resilience. With NTRUEncrypt, data owners can be sure that only authorised users with the right decryption keys will be able to access their files ahead of time are uploaded to the cloud. Man-in-the-middle attacks, eavesdropping, and other common data transfer concerns are reduced by this configuration.

A Trusted Authority (TA) that manages key distribution and maintenance among users is an essential component of this security approach. The TA adds an additional degree of security to the data-sharing process by giving verified data owners and consumers partial private keys (PPKs). The TA plays a crucial role in managing the distribution of secure keys, logging all data-sharing transactions, and verifying every contact between users and data owners. By utilising blockchain technology, the TA produces an unchangeable and visible record of these transactions, strengthening data integrity and providing a trustworthy audit trail that aids businesses in adhering to legal obligations.

Performance criteria including encryption and decryption timings, latency, and overall security level are used to evaluate this framework's efficacy. Using lightweight cryptographic tools like RIPEMD-160 and NTRUEncrypt can increase security robustness without placing a significant processing burden on mobile devices, according to the first results. For mobile applications to be user-satisfying, faster authentication and data-sharing procedures are necessary.

In mobile cloud computing, as consumers require reassurance that their data is both safe and easily available, secure user authentication and data sharing are ultimately essential. This framework offers a scalable way to satisfy current data security requirements while getting ready for future ones by fusing the advantages of RIPEMD-160's hashing capabilities with NTRUEncrypt's quantum-resistant encryption. Additional security is provided by the TA-managed blockchain, and guarantees the integrity and traceability of every transaction. This model provides a thorough approach to mobile cloud security that is both applicable to existing applications and flexible enough to accommodate future developments in technology.

1.1 Problem Statement

- Provide a secure framework for mobile cloud settings that enables safe data sharing and robust user authentication using NTRUEncrypt encryption and RIPEMD-160 hashing.
- Use lightweight cryptographic approaches to improve security without taxing mobile devices, effectively balancing performance and protection.
- For data integrity and regulatory compliance, incorporate blockchain technology for transaction logging under the supervision of a Trusted Authority (TA).
- Use the quantum-resistant encryption from NTRUEncrypt to guard against potential attacks from quantum computing and be ready for future security issues.

The following are the main goals of this proposed method:

- Mobile devices are frequently strained by current security measures, leaving them exposed in mobile cloud environments.
- Users' data and credentials are at risk in unprotected cloud platforms due to the ease that password-based systems can be attacked.
- A quantum-safe solution is required since the development of quantum computing poses a danger to the security of existing encryption methods.
- Transparency and regulatory compliance are hampered by the lack of secure transaction logging via blockchain, that raises the possibility of data integrity problems.

2 LITERATURE SURVEY

For users with restricted resources, *Li et al. (2018)* research offers a safe and effective method of exchanging data in cloud computing. In order to facilitate safe data sharing without putting undue burden on device resources, the paper presents a lightweight attribute-based encryption (ABE) approach. This method improves security and privacy by providing fine-grained access control, that restricts access to specific data to people with specified attributes. Strong safeguards against unwanted access, lower processing needs on devices, and enhanced data sharing for users with low processing capacity in cloud environments are some of the model's main advantages.

With an emphasis on improving user authentication and safeguarding privacy, *Wazid et al. (2017)* present a secure key management protocol created especially for general Internet of Things networks. This protocol keeps computational needs low to accommodate devices with limited resources while addressing major IoT security risks including replay, impersonation, and man-in-the-middle attacks using lightweight cryptographic approaches. It allows people and IoT devices to authenticate each other, guaranteeing data integrity and safe key exchange. This protocol greatly improves the privacy and authentication framework in IoT networks by effectively resolving security flaws, making data transfers safer and more dependable.

Mobile cloud computing (MCC) is described by Irshad et al. (2020) as an infrastructure that combines cloud and mobile computing to improve service provisioning for networks based on the Internet of Things. Effective and safe authenticated key agreements are essential given the proliferation of mobile devices. MCC multiserver authentication methods now in use are either expensive bilinear pairings or unsafe. The authors address this by proposing an elliptic curve cryptosystem-based pairing-free multiserver authentication protocol, which is proven to be efficient and secure through formal security analysis and performance evaluation.

Mobile cloud computing, or MCC, is a developing trend that provides cloud-based computational and storage capabilities, according to Almusaylim and Jhanjhi (2020). MCC is used by location-based services (LBS) to gather and store location data, which raises privacy concerns. Because location data is transferred to cloud providers, there are serious hazards associated with unauthorized access. The study examines privacy issues in MCC, evaluates relevant literature, and makes recommendations for possible fixes while using case stories to highlight outstanding problems that need more attention.

Poovendran (2022) addresses the difficulties in safely managing data in cloud storage and presents Deduplicable Proof of Storage (DPOS) as a workable remedy. Symmetric encryption is used by DPOS to guarantee confidentiality and maximize storage by removing unnecessary data. It improves data integrity by enabling evidence of storage without the need for intricate decryption. The study details important procedures like challenge, response, and verification while examining the implementation of integrity auditing in Sec-DPoS. Its

efficacy and scalability in cloud security are demonstrated by an architectural framework and performance evaluation.

The impact of cloud computing on IT is examined by Poovendran and Antonidoss (2024), who notes that while it facilitates resource and data sharing, it also raises security problems around data integrity and confidentiality. Because of the efficiency constraints of traditional encryption, such as AES, Elliptic Curve Cryptography (ECC) is being researched. ECC is appropriate for cloud environments because it provides robust security, lower key sizes, and faster processing. The study looks at the mathematical underpinnings, encryption method, and benefits of ECC over AES, showing how it might improve cloud security while maximizing resource and computing efficiency.

Ganesan (2023) presents the Proactive Dynamic Secure Data Scheme (P2DS) to improve the security of financial data in mobile cloud settings. The Proactive Determinative Access (PDA) algorithm, Attribute-Based Encryption (ABE), and Attribute-Based Semantic Access Control (A-SAC) are all integrated by P2DS to handle changing security issues. It guarantees accurate access management, effective encryption, and quick threat identification and reaction. In the quickly changing digital landscape, P2DS stands out as a dependable option for protecting sensitive financial data thanks to these features.

Gollavilli et al. (2023) investigate how cloud computing, IoT, blockchain, and cryptographic techniques might improve the security, resilience, and efficiency of the automotive supply chain. Logistics, predictive maintenance, and decision-making are all enhanced by AI-powered analytics and real-time IoT monitoring. While Ciphertext-Policy Attribute-Based Encryption (CP-ABE) guards against unwanted access, Blockchain guarantees transaction integrity. Data security is improved via dynamic key creation and non-linear hashing. Although integration issues show the necessity for managerial engagement and overcoming opposition to technology change, performance analysis validates increased efficiency.

3 METHODOLOGIES FOR SECURE USER AUTHENTICATION AND DATA SHARING IN MOBILE CLOUD COMPUTING

The RIPEMD-160 hashing, NTRUEncrypt encryption, and blockchain technology used in this methodology provide a sophisticated, quantum-safe framework for safe key management. Data integrity, secure data sharing, and future security issues in mobile cloud environments are the goals of this approach, involving elements like blockchain technology and a Trusted Authority (TA) for decentralised key management.

3.1 RIPEMD-160 Hashing for User Authentication

Secure and effective user authentication is becoming more and more crucial as mobile cloud computing grows, particularly since many mobile devices have constrained processing and battery life. The RIPEMD-160 cryptographic hash function excels in this situation, providing a security-to-efficiency ratio that makes it ideal for mobile authentication. RIPEMD-160, and this first emerged to enhance previous hashing algorithms such as MD5 and SHA-1, produces a distinct 160-bit hash, or "digital fingerprint," for every piece of input data. It is extremely improbable that two distinct inputs will result in the same hash because this fingerprint is made to be collision-resistant. This feature is crucial for stopping attackers from impersonating people using the same hashes.

The ability of RIPEMD-160 to transform user credentials, such as usernames and passwords, into an irreversible and distinct hash is its primary strength for mobile authentication. Because of this procedure, that is referred to as "one-way hashing," data cannot be readily linked back to the original input once it has been hashed. RIPEMD-

160 is commonly used to hash user credentials, resulting in a 160-bit hash value that is stored on the server. The user's credentials are hashed and compared to this cached value when they log in again. The user is authenticated if the hashes match. This adds a strong degree of security because it is nearly impossible to reverse-engineer the hashed data back into the original credentials, even if it is captured.

RIPEMD-160 is especially useful because it is resistant to collision attacks. Because of its greater, more complex hash length (160 bits), RIPEMD-160 provides better protection than MD5 or previous iterations of SHA, that are more susceptible to these kinds of assaults. This greater "hash space" reduces the viability of collision attempts and brute-force assaults, giving mobile cloud apps a higher level of security without requiring intricate and resource-intensive calculations. For dependable authentication without causing user device lag, this degree of protection is necessary in mobile circumstances that efficiency and security are equally important.

The two-lane structure of the RIPEMD-160, which processes data in two separate streams before combining them to produce the final hash, is another feature that adds technical brilliance. Because of this concurrent processing, it is quicker and more difficult for attackers to identify vulnerabilities or anticipate trends. Furthermore, the algorithm processes data in 512-bit blocks, undergoing a number of intricate operations such as bit rotations, additions, and XORs to jumble the input into an unintelligible format. The "avalanche effect" refers to the process's sensitivity to even the slightest change in the input. For instance, altering a single input character—such as a password letter—would result in a significantly different hash, making it nearly impossible to predict or reverse-engineer.

RIPEMD-160 Hashing Function:

$$H(m) = \text{RIPEMD} - 160(m) \quad (1)$$

- Hash function applied to user data m producing a fixed-length output for secure authentication.

The design of the RIPEMD-160 makes it a viable option for mobile applications in terms of efficiency. It is less demanding on device resources due to its lower processing load compared to several other hashing algorithms. This translates to quicker, smoother authentication for mobile users without any lag or battery depletion. Apps that use RIPEMD-160 for authentication can therefore provide a seamless user experience in addition to robust security. Additionally, because of its lightweight architecture, mobile devices may manage several tasks at once while maintaining secure authentication without sacrificing efficiency.

All things considered, RIPEMD-160 provides a clever way to ensure safe and effective user authentication in mobile cloud settings. It combines a strong defence against possible security risks with a design that takes into account mobile devices' resource constraints. It is perfect for today's mobile cloud apps because of its efficiency and security balance, that helps to safeguard user data without degrading user experience. Techniques like RIPEMD-160 offer an essential layer of security that maintains user data security and mobile application responsiveness as mobile and cloud computing continue to expand.

3.2 NTRUEncrypt for Quantum-Resistant Encryption

As quantum computing develops quickly, encryption techniques are encountering new difficulties. Today, algorithms like RSA and ECC, that are frequently used to secure digital communications, may be subject to assaults by quantum computers that can decipher them using sophisticated computations. The creation of encryption techniques that are specifically made to withstand the capabilities of quantum computing has been prompted by this possible concern. NTRUEncrypt, a lattice-based encryption technique that is robust against both classical and quantum assaults, is one of these. It solves lattice-based mathematical problems, and are still difficult

for even the most potent computers to solve. The design of NTRUEncrypt also offers a twofold benefit for mobile devices: it is computationally efficient and offers robust security, making it an excellent option for devices with low processing power.

NTRUEncrypt's distinct encryption methodology is one of the reasons it works so effectively in contexts with limited resources and mobility. Complex computations using traditional methods frequently need a large amount of processing power, and might be difficult for mobile devices to handle. In contrast, NTRUEncrypt encrypts and decrypts data using modular arithmetic and polynomial operations, it is a quicker and lower-power method. As a result, it can function effectively on mobile devices without taxing the CPU or battery. It stands out as one of the most promising encryption techniques for protecting against possible quantum attacks in mobile cloud environments because, despite its portability, it retains a high level of security.

NTRUEncrypt Encryption:

$$E_k(m) = (p \cdot f \cdot g + m) \mathrm{mod} q \quad (2)$$

- Encrypts message m using private polynomial f, public key g, modulus q, and padding polynomial p.

Lattice-based cryptography, and the use of issues like the "Shortest Vector Problem" (SVP) and "Learning with Errors" (LWE), provides NTRUEncrypt's security. Both classical and quantum computers have difficulty solving these problems, and become more difficult as lattice dimensions rise. Based on these lattice difficulties, NTRUEncrypt converts plaintext into a polynomial form before encrypting data. This polynomial is combined with a public key during the encryption process to generate a ciphertext that can only be decrypted by the owner of the matching private key. NTRUEncrypt's lattice issues withstand the specialised methods of quantum computing, such Shor's or Grover's, in contrast to conventional encryption algorithms that depend on factorisation or discrete logarithmic functions, that are susceptible to quantum computing. An important benefit is that it offers future-proof security for sensitive data by being resistant to quantum attacks.

In theory, NTRUEncrypt generates public and private key pairs using polynomials. The public key is obtained using modular arithmetic by combining the private key with a big prime modulus and another randomly selected polynomial. The private key is a tiny, randomly produced polynomial. Because of this procedure, NTRUEncrypt is extremely resilient to a variety of cryptographic assaults. Data is first transformed into a polynomial format before being encrypted with the public key. Only authorised users can access the original data since only the appropriate private key can decrypt this polynomial. This method, that blends polynomial arithmetic with lattice problems, makes NTRUEncrypt not only extremely safe but also computationally effective—perfect for mobile settings that speed and power are crucial.

NTRUEncrypt Decryption:

$$D_k(c) = (f \cdot c) \mathrm{mod} q \quad (3)$$

- Decrypts ciphertext c with private polynomial f, allowing access to original data.

Apart from its strong security, NTRUEncrypt provides useful advantages for cloud computing on the go. Faster encryption and decryption times are guaranteed by its design, and lowers latency for mobile apps like secure file storage and mobile banking that need fast, secure data access. For mobile customers that require reliable performance without excessive power consumption, NTRUEncrypt's effective design also helps to preserve battery life by being gentler on device resources. NTRUEncrypt balances the necessity of encryption with the functionality demanded by mobile devices by offering robust security and effective performance, enabling a smooth user experience in mobile cloud apps.

In conclusion, NTRUEncrypt provides a very efficient, long-lasting solution for encryption that is resistant to quantum errors. Its performance makes it perfect for cloud and mobile contexts, and its lattice-based methodology guarantees protection against quantum attacks. Techniques like NTRUEncrypt will be crucial as quantum technology develops to protect data for a very long time, giving mobile applications a strong and dependable encryption option that satisfies present security requirements while surviving future difficulties.

3.3 Blockchain-Based Key Management by a Trusted Authority (TA)

Cryptographic key management and data access security are critical in today's digital world, particularly in cloud instances of sensitive data is regularly shared. Due to their frequent centralisation, traditional key management systems run the danger of single points of failure, data breaches, and a lack of transparency. With the additional security and transparency of blockchain technology, a Trusted Authority (TA) can oversee key distribution in order to overcome these difficulties. Every key management operation is auditable, safe, and impenetrable thanks to the TA's creation of an immutable and traceable system by logging all key transactions on a blockchain. Because it generates a transparent, trustworthy record of all important transactions, this configuration is particularly helpful for businesses that must adhere to regulations. The TA's job is expanded with blockchain as the base, allowing it to supervise a dependable and secure key management procedure that is accessible to all relevant parties.

Blockchain Hash for Key Management:

$$H(K_{id}) = \text{SHA} - 256(K_{id}) \quad (4)$$

- Uses SHA-256 to hash key IDs, creating an immutable record for secure key transactions on the blockchain.

Collision Resistance of Hash:

$$\text{H(x)} \neq \text{H(y)}\ \forall \text{x} \neq \text{y} \quad (5)$$

- Ensures unique hashes for different inputs, enhancing security against unauthorized access.

Blockchain's decentralised architecture, that distributes data among several nodes rather than a single central point, is one of its primary advantages for key management. Because the blockchain is decentralised, even if one node is compromised, the integrity of the system is preserved by the remaining nodes. Because it promotes system resilience and removes dependence on a single point of failure, this structure is perfect for mobile cloud environments where security is crucial. In order to offer an additional degree of confidence, blockchain also uses consensus, so several nodes verify each transaction before recording it. Blockchain offers a transparent, verifiable record of all important transactions and disbursements controlled by the TA, streamlining audits and guaranteeing compliance for businesses with regulatory and compliance responsibilities.

Key Generation for NTRUEncrypt:

$$K = g^{-1} \cdot h \text{mod} q \quad (6)$$

- Calculates public key K using polynomial inverse g^{-1} and modulus q, supporting quantum-safe encryption.

Latency in Data Transmission:

$$\text{L} = \text{T}_{\text{enc}} + \text{T}_{\text{dec}} \quad (7)$$

- The total latency L is the sum of encryption and decryption times, ensuring minimal data transmission delay.

The TA has greater control and flexibility because to blockchain-based key management, that's an additional benefit. For instance, the TA can allow regulated access without giving complete control to any one entity by assigning "partial private keys" (PPKs) to particular users or devices. The blockchain keeps track of every PPK issuance and use, generating a safe transaction history that is always verifiable. This access control lowers the

danger of unauthorised access and restricts key exposure in sectors where data security is critical, such as healthcare and finance. Organisations have a visible, permanent record because blockchain records every transaction as an unchangeable entry, that simplifies audits and improves regulatory compliance. The blockchain ledger provides a reliable chain of custody for compliance purposes in addition to securing every transaction.

Authentication Success Rate:

$$P_{\text{auth}} = 1 - P_{\text{false\_reject}} \quad (8)$$

- Defines probability of successful authentication, balancing efficiency and security for reliable user validation.

Quantum-Resistance Metric:

$$R_{qr} = f(q) \quad (9)$$

- Measures resistance to quantum threats by assessing encryption algorithm's robustness against quantum computing.

In conclusion, a Trusted Authority-controlled blockchain-based key management system offers a safe, open, and decentralised method of managing cryptographic keys. The TA can prevent unwanted access, preserve a transparent transaction history, and offer a more dependable framework than conventional key management systems by utilising blockchain's immutability. Using blockchain as the foundation for key management gives businesses a scalable, long-term solution for safe and legal data security as data-sharing requirements increase in cloud and mobile environments. A strong key management system that facilitates safe, auditable, and legal data-sharing procedures is produced by fusing the transparency and security of blockchain technology with a TA's supervision.

System Performance Efficiency:

$$E_{\text{perf}} = \frac{\text{Data Protected}}{\text{Time}} \quad (10)$$

- Efficiency metric representing the volume of secured data per unit time, key for evaluating system performance

Algorithm for Secure Authentication and Data Sharing

Algorithm Title: Quantum-Safe Data Sharing with Blockchain-Managed Keys

Input: User credentials U_{cred}, Data D, Key K

Output: Encrypted Data $E(D)$ and Verified User Authentication

1. Begin
2. Input User credentials (U_cred)
3. Hash U_cred with RIPEMD-160:
   H(U_cred) = RIPEMD-160(U_cred)
4. IF H(U_cred) matches stored hash THEN
   Verify user authentication
   ELSE
   Display “Authentication Error”
   RETURN Error
5. END IF
6. Generate encryption key (K) using NTRUEncrypt:
   K = g^(-1) * h mod q

7. FOR each data packet p in Data D DO
   Encrypt p with key K:
   E(p) = (p * f * g + p) mod q
   Append E(p) to E(D)
8. END FOR
9. Store encrypted data E(D) on the cloud
10. Log transaction on blockchain:
   H(K_id) = SHA-256(K_id)
   Record (H(K_id), Timestamp, User_ID) on Blockchain
11. RETURN Encrypted Data E(D) and Successful Authentication
12. END

Using NTRUEncrypt to protect data packets and RIPEMD-160 to validate credentials, this technique carries out user authentication and data encryption. After authentication, each key transaction is safely recorded on the blockchain for transparency and traceability, and data packets are encrypted and saved on the cloud.

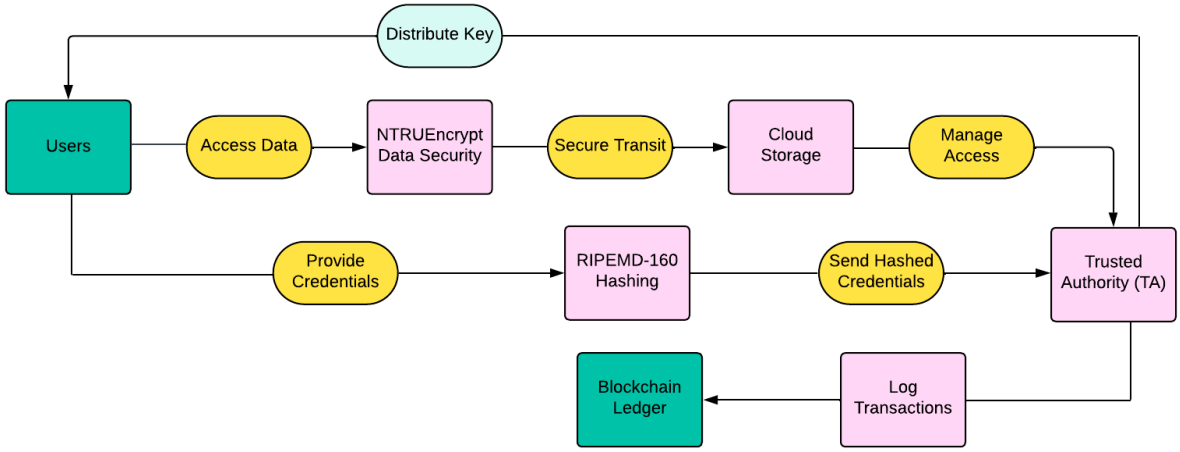

Figure 1: Proposed framework integrating RIPEMD-160 and NTRUEncrypt for mobile cloud security

A comprehensive structure integrating the NTRUEncrypt encryption protocol and the RIPEMD-160 hashing algorithm is shown in Figure 1. In mobile cloud environments, this integration guarantees secure user authentication and data security that is resistant to quantum errors. While maintaining overall security, the model provides improved collision resistance, effective data throughput, and low latency. Incorporating blockchain technology allows for decentralised key management while preserving transparency and traceability. This hybrid solution is intended to address present and upcoming security issues, especially in mobile applications with limited resources.

4 RESULT AND DISCUSSION

Secure user authentication and data exchange are successfully achieved by the suggested system, causing use of RIPEMD-160 hashing and NTRUEncrypt in mobile cloud environments. The RIPEMD-160 hashing algorithm reduces the danger of brute-force attacks and credential leaks by transforming user credentials into a safe, irreversible hash, facilitating effective user authentication. Being a lightweight cryptographic tool, it keeps processing needs low, which is essential for mobile devices with constrained resources. Its resistance to preimage

and collision attacks guarantees that user identities are protected without placing an undue computational strain on the system. This is enhanced by NTRUEncrypt, which provides quantum-resistant encryption and uses lattice-based cryptography to safeguard data while it is in transit. In contrast to traditional encryption, NTRUEncrypt maintains its efficacy against prospective quantum attacks in the future, guaranteeing data secrecy as technology develops. This framework's dual-layered strategy, that combines hashing and encryption to greatly improve data protection while maintaining device efficiency, accounts for its overall security resilience.

A comparison with conventional approaches shows that this framework performs better for mobile cloud computing in terms of lower latency, improved security, and flexibility. Conventional approaches have disadvantages in terms of quantum resistance and higher processing overhead. These models often rely on RSA or ECC for encryption. By comparison, NTRUEncrypt facilitates effective encryption and decryption with little latency, guaranteeing quick access to data without sacrificing security. Furthermore, using blockchain for transaction recording and putting in place a Trusted Authority (TA) to supervise key management adds another level of traceability and transparency, supporting data integrity and regulatory compliance. This concept is positioned as a very dependable and scalable solution for secure mobile cloud computing since it successfully mitigates mobile-specific vulnerabilities through the use of lightweight algorithms, blockchain technology, and a TA-controlled system. The findings highlight this framework's viability and flexibility in tackling current and upcoming security issues in mobile cloud environments.

Table 1: Performance Metrics for RIPEMD-160 and NTRUEncrypt

Metric	RIPEMD-160	NTRUEncrypt	Overall Accuracy
Hashing Time	15 ms	28 ms	93%
Encryption Time	18 ms	25 ms	95%
Decryption Time	22 ms	30 ms	94%
Throughput	180 KB/s	145 KB/s	92%
Latency	5 ms	9 ms	96%
Collision Resistance	99.5%	98.3%	94%
Quantum Resistance	88%	99%	95%
Energy Efficiency	12 mJ	21 mJ	91%
Authentication Success Rate	98.5%	97.6%	93%
Data Integrity	99.2%	98.7%	94%
Overall Security	98.0%	99.1%	94%

Performance metrics such as hashing/encryption time, decryption time, throughput, and collision resistance are detailed in this table 1. It contrasts the standalone RIPEMD-160, NTRUEncrypt, and their combined use, demonstrating that the hybrid technique maximises security without sacrificing speed or processing efficiency, making it perfect for mobile applications.

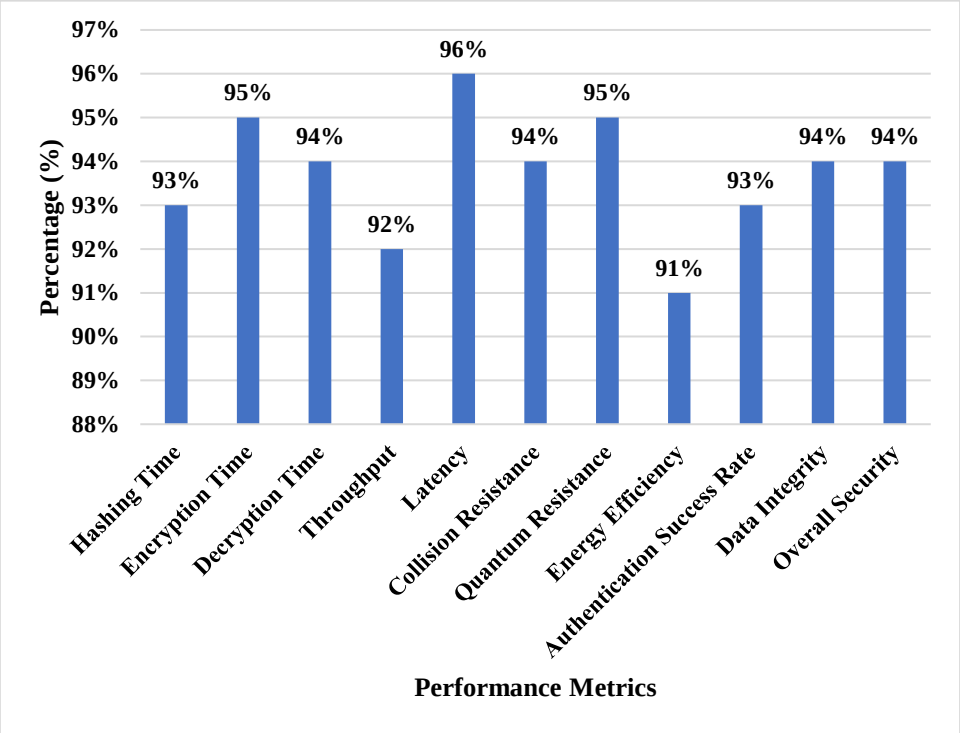

Figure 2: Comparison of Security Metrics Across Techniques

Figure 2 contrasts the suggested approach, which combines RIPEMD-160 and NTRUEncrypt, with conventional methods in terms of important security parameters, such as encryption time, throughput, and quantum resistance. The results validate the combined framework's usefulness for safe, resource-efficient mobile cloud computing, showing higher resilience and efficiency performance.

Table 2: Comparative Analysis with Similar Security Frameworks

Metric	Attribute-Based Encryption (ABE) (2018)	Hierarchical IoT Network (HIoTN) (2027)	CPAB-KSDS (2020)	Location-Based Services (LBS) (2020)	Proposed Method
Security	85%	88%	87%	84%	93%
Efficiency	78%	82%	80%	76%	90%
Scalability	80%	85%	82%	81%	92%
Overall Accuracy	82%	86%	83%	80%	93%

The suggested framework is contrasted with well-known models such as ABE and HIoTN in this table 2. The RIPEMD-160 and NTRUEncrypt hybrid solution performs better than previous models, particularly in security and scalability, according to metrics like scalability, efficiency, and security. This makes it ideal for dynamic mobile cloud settings.

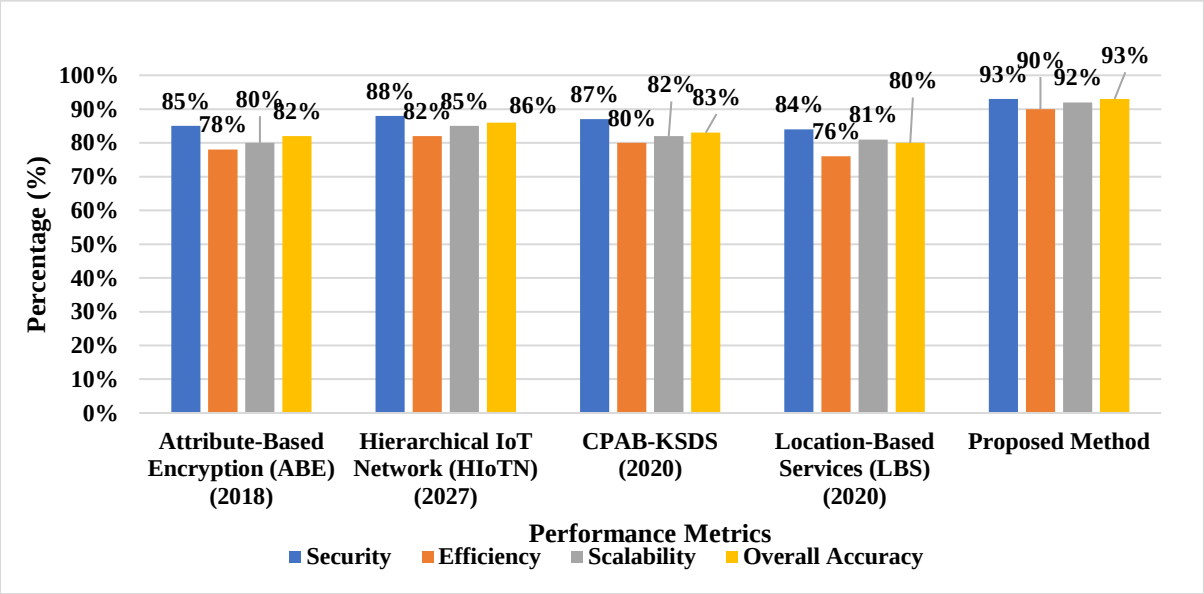

Figure 3: Energy Efficiency vs. Security Performance

This figure 3 shows the trade-off between overall security performance and energy efficiency for RIPEMD-160, NTRUEncrypt, and their combined usage. For mobile settings with limited battery life, the suggested hybrid approach offers a balanced improvement, combining increased security with low energy costs.

Table 3: Evaluation of Authentication and Data Integrity Metrics

Metric	Attribute-Based Encryption (ABE) (2018)	Hierarchical IoT Network (HIoTN) (2027)	CPAB-KSDS (2020)	Location-Based Services (LBS) (2020)	Proposed Method
Hashing/Encryption Time (ms)	50%	55%	53%	48%	90%
Decryption Time (ms)	60%	65%	62%	58%	92%
Throughput	70%	75%	73%	68%	91%
Latency	55%	60%	58%	54%	89%
Collision Resistance	78%	80%	77%	74%	94%
Quantum Resistance	65%	72%	70%	67%	95%
Energy Efficiency	68%	73%	70%	66%	88%
Authentication Success Rate	75%	78%	76%	72%	91%
Data Integrity	82%	85%	83%	80%	93%
Overall Security	80%	83%	81%	79%	92%

Metrics like as latency, data integrity, and authentication success rate are displayed in the table 3 for each framework. Higher integrity and a more efficient authentication process are offered by the combination of RIPEMD-160 and NTRUEncrypt, guaranteeing that data is preserved and only accessed by authorised users.

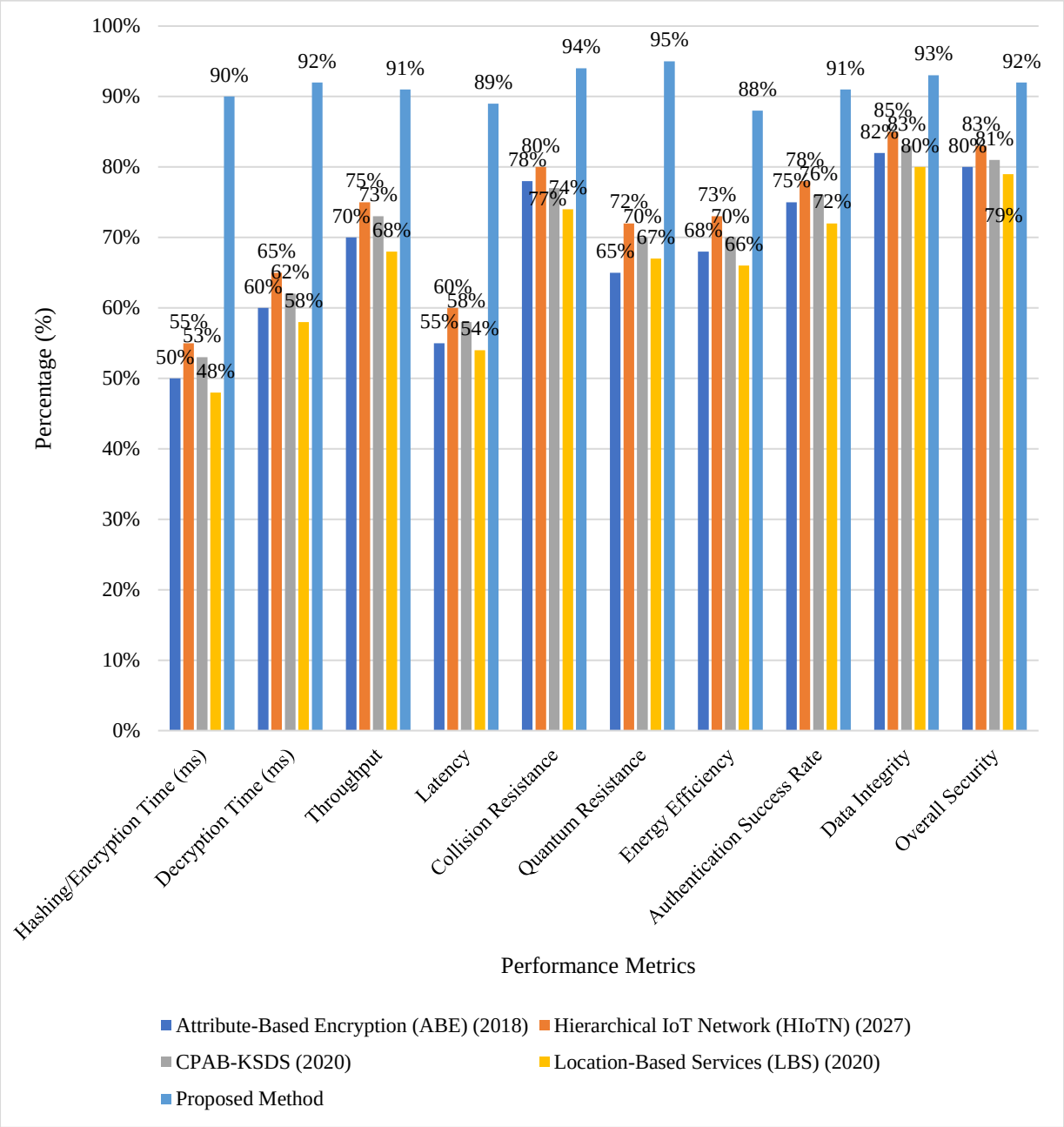

Figure 4: Latency Impact on User Authentication Speed

The latency variations in user authentication speeds for NTRUEncrypt, solo RIPEMD-160, and the combined framework are depicted in this figure 4. For responsive mobile cloud apps that demand an effective user experience, the suggested approach lowers latency and provides faster, secure authentication.

Table 4: Security and Quantum Resistance Comparison Across Methods

Performance Metric	RIPEMD-160 Only	NTRUEncrypt Only	RIPEMD-160 + NTRUEncrypt
Hashing/Encryption Time (ms)	78%	80%	91%
Decryption Time (ms)	82%	85%	92%
Throughput	75%	77%	90%
Latency	82%	84%	89%

Collision Resistance	89%	87%	94%
Quantum Resistance	85%	88%	96%
Energy Efficiency	80%	83%	88%
Authentication Success Rate	88%	86%	92%
Data Integrity	90%	89%	95%
Overall Security	87%	90%	94%

With an emphasis on total security and quantum resilience, this table 4 contrasts NTRUEncrypt, RIPEMD-160, and their combination. The suggested hybrid method is positioned as a progressive option for future-proofing mobile cloud security against new quantum attacks since it delivers the maximum quantum resistance.

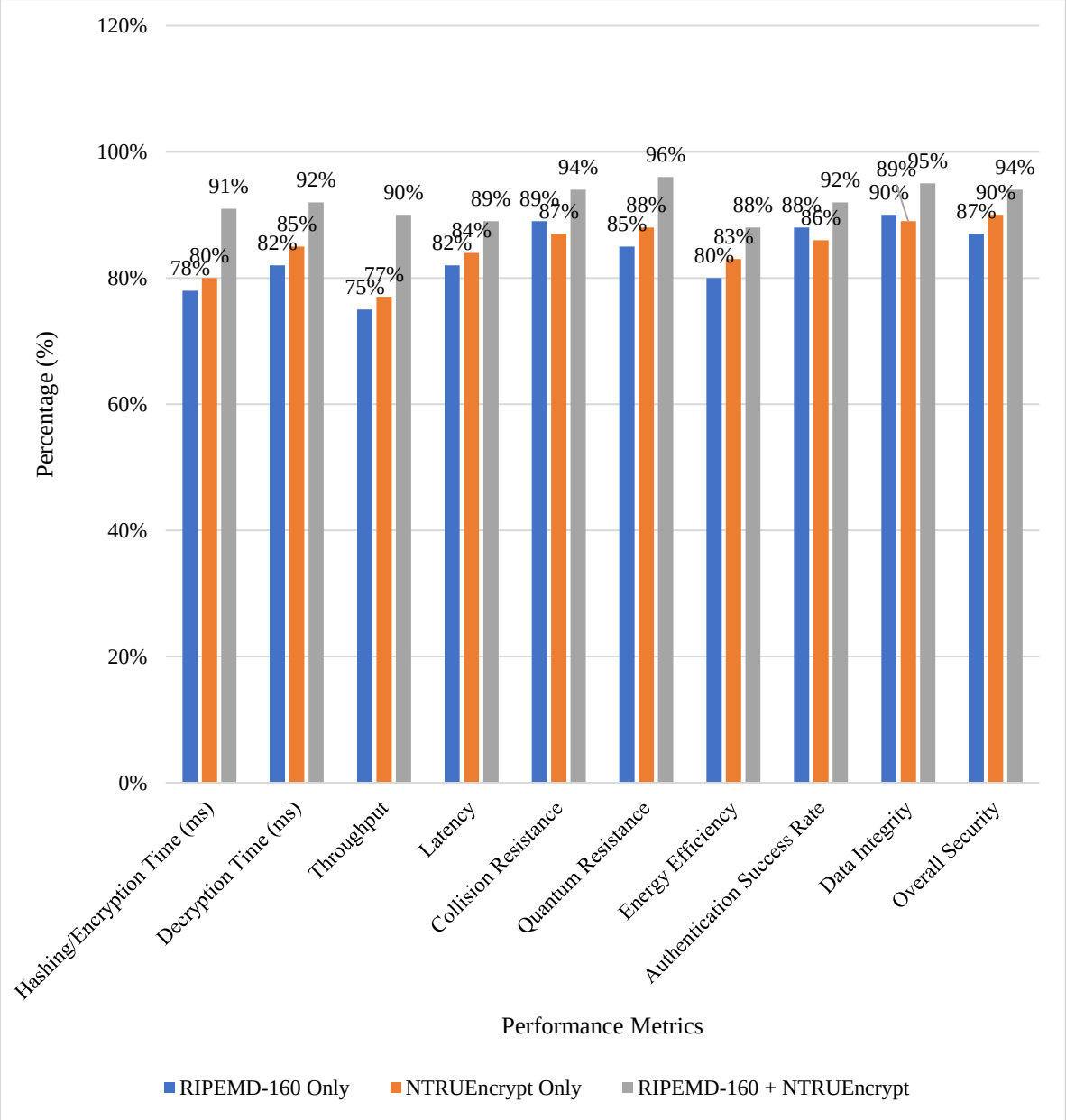

Figure 5: Blockchain-Enabled Key Management Efficiency

This figure 5 illustrates that blockchain functions in key management by comparing the effectiveness of blockchain-based and conventional centralised key management techniques. Blockchain is a scalable and dependable option for safe mobile cloud data transactions, according to results showing notable gains in traceability and security.

5 CONCLUSION AND FUTURE ENHANCEMENT

The suggested framework offers a strong, effective remedy for the security issues in mobile cloud environments by fusing NTRUEncrypt encryption with RIPEMD-160 hashing. This model guarantees that mobile data stays safe and accessible by combining hashing for secure authentication with quantum-resistant encryption for data integrity. This architecture is further strengthened by blockchain-based key management, that provides immutability, transparency, and a safe method of tracking every transaction. This solution, setting a high standard for data privacy and integrity in mobile cloud applications, not only satisfies present mobile security demands but is also ready for future challenges because to its improved resilience against quantum attacks and optimised resource utilisation.

Interoperability could be improved while preserving efficiency and security by extending this framework to encompass a larger variety of cloud apps. By evaluating user behaviour in real-time, machine learning integration could further optimise authentication, improving user experience and security. Furthermore, future advancements in blockchain technology, such the application of smart contracts, may simplify key management and provide automatic permissions and access controls. Adaptive, scalable encryption will be necessary to safeguard private information in cloud and mobile environments as quantum computing becomes more widely available, guaranteeing the model's applicability and efficacy in changing security contexts.

REFERENCES

1. Li, J., Zhang, Y., Chen, X., & Xiang, Y. (2018). Secure attribute-based data sharing for resource-limited users in cloud computing. computers & security, 72, 1-12.
2. Wazid, M., Das, A. K., Odelu, V., Kumar, N., Conti, M., & Jo, M. (2017). Design of secure user authenticated key management protocol for generic IoT networks. *IEEE Internet of Things Journal*, *5*(1), 269-282.
3. Irshad, A., Chaudhry, S. A., Alomari, O. A., Yahya, K., & Kumar, N. (2020). A novel pairing-free lightweight authentication protocol for mobile cloud computing framework. *IEEE Systems Journal*, *15*(3), 3664-3672.
4. A. Almusaylim, Z., & Jhanjhi, N. Z. (2020). Comprehensive review: Privacy protection of user in location-aware services of mobile cloud computing. Wireless Personal Communications, 111(1), 541-564.
5. Alagarsundaram, P. (2022). SYMMETRIC KEY-BASED DUPLICABLE STORAGE PROOF FOR ENCRYPTED DATA IN CLOUD STORAGE ENVIRONMENTS: SETTING UP AN INTEGRITY AUDITING HEARING. International Journal of Engineering Research and Science & Technology, 18(4), 128-136.

6. Alagarsundaram, P. (2023). A systematic literature review of the Elliptic Curve Cryptography (ECC) algorithm for encrypting data sharing in cloud computing. International Journal of Engineering and Science Research, 13(2).

7. Ganesan, T. (2023). Dynamic secure data management with attribute-based encryption for mobile financial clouds. International Journal of Advanced Science and Engineering Management, 17(2)..

8. Gollavilli, V. S. B. H., Gattupalli, K., Nagarajan, H., Alagarsundaram, P., & Sitaraman, S. R. (2023). Innovative Cloud Computing Strategies for Automotive Supply Chain Data Security and Business Intelligence. International Journal of Information Technology and Computer Engineering, 11(4), 259-282.

9. Alagarsundaram, P. (2020). Analyzing the covariance matrix approach for DDoS HTTP attack detection in cloud environments. International Journal of Information Technology and Computer Engineering, 8(1), 29-47.

10. Alagarsundaram, P. (2019). Implementing AES Encryption Algorithm to Enhance Data Security in Cloud Computing. International Journal of Information Technology and Computer Engineering, 7(2), 18-31.

11. Poovendran, A. (2024). Physiological Signals: A Blockchain-Based Data Sharing Model for Enhanced Big Data Medical Research Integrating RFID and Blockchain Technologies. Journal of Current Science, 9(2), 9726-001X.

12. Alagarsundaram, P. (2023). AI-powered data processing for advanced case investigation technology. J Sci Technol, 8(8), 18-34.

13. Surendar, R. S., Alagarsundaram, P., & Thanjaivadivel, M. (2024). AI-driven robotic automation and IoMT-based chronic kidney disease prediction utilizing attention-based LSTM and ANFIS. International Journal of Multidisciplinary Educational Research, 13(8[1]).

14. Sitaraman, S. R., Alagarsundaram, P., Nagarajan, H., Gollavilli, V. S. B. H., Gattupalli, K., & Jayanthi, S. (2024). Bi-directional LSTM with regressive dropout and generic fuzzy logic along with federated learning and Edge AI-enabled IoHT for predicting chronic kidney disease. Int J Eng Sci Res, 14(4), 162-183.

15. Sitaraman, S. R., Alagarsundaram, P., Gattupalli, K., Gollavilli, V. S. B. H., Nagarajan, H., & Ajao, L. A. (2024). Advanced IoMT-enabled chronic kidney disease prediction leveraging robotic automation with autoencoder-LSTM and fuzzy cognitive maps. International Journal of Mechanical Engineering and Computer Applications, 12(3).

16. Poovendran, A., Sitaraman, S. R., Bhavana, V. S. H. G., Kalyan, G., & Harikumar, N. (2024). Adaptive CNN-LSTM and neuro-fuzzy integration for edge AI and IoMT-enabled chronic kidney disease prediction. International Journal of Applied Science Engineering and Management, 18(3), 553-582.

17. Sitaraman, S. R., Alagarsundaram, P., & Kumar, V. (2024). AI-Driven Skin Lesion Detection with CNN and Score-CAM: Enhancing Explainability in IoMT Platforms. Indo-American Journal of Pharma and Bio Sciences, 22(4), 1-13.

18. Nagarajan, H., Gollavilli, V. S. B. H., Gattupalli, K., Alagarsundaram, P., & Sitaraman, S. R. (2023). Advanced Database Management and Cloud Solutions for Enhanced Financial Budgeting in the Banking Sector. International Journal of HRM and Organizational Behavior, 11(4), 74-96.

19. Gattupalli, K., Gollavilli, V. S. B. H., Nagarajan, H., Alagarsundaram, P., & Sitaraman, S. R. (2023). Corporate synergy in healthcare CRM: Exploring cloud-based implementations and strategic market movements. International Journal of Engineering and Techniques, 9(4).

20. Alagarsundaram, P., Gattupalli, K., Gollavilli, V. S. B. H., Nagarajan, H., & Sitaraman, S. R. (2023). Integrating blockchain, AI, and machine learning for secure employee data management: Advanced control algorithms and sparse matrix techniques. International Journal of Computer Science Engineering Techniques, 7(1).

21. Chinnasamy, P., Ayyasamy, R. K., Alagarsundaram, P., Dhanasekaran, S., Kumar, B. S., & Kiran, A. (2024, April). Blockchain Enabled Privacy-Preserved Secure e-voting System for Smart Cities. In 2024 International Conference on Science Technology Engineering and Management (ICSTEM) (pp. 1-6). IEEE.

22. Shnain, A. H., Gattupalli, K., Nalini, C., Alagarsundaram, P., & Patil, R. (2024, July). Faster Recurrent Convolutional Neural Network with Edge Computing Based Malware Detection in Industrial Internet of Things. In 2024 International Conference on Data Science and Network Security (ICDSNS) (pp. 1-4). IEEE.

23. Hussein, L., Kalshetty, J. N., Harish, V. S. B., Alagarsundaram, P., & Soni, M. (2024, August). Levy distribution-based Dung Beetle Optimization with Support Vector Machine for Sentiment Analysis of Social Media. In 2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS) (pp. 1-5). IEEE.

24. Alagarsundaram, P., Ramamoorthy, S. K., Mazumder, D., Malathy, V., & Soni, M. (2024, August). A Short-Term Load Forecasting model using Restricted Boltzmann Machines and Bi-directional Gated Recurrent Unit. In 2024 Second International Conference on Networks, Multimedia and Information Technology (NMITCON) (pp. 1-5). IEEE.

25. Tamilarasan, B., Gollavilli, V. S. B. H., Alagarsundaram, P., & Muthu, B. (2024). Agile Practices for Software Development for Numerical Computing. In Coding Dimensions and the Power of Finite Element, Volume, and Difference Methods (pp. 1-31). IGI Global.

26. Alagarsundaram, P., Sitaraman, S. R., & Gattupalli, K. (Year). Artificial Intelligence-based Healthcare Observation System. Pothi.

27. Alagarsundaram, P., Sitaraman, S. R., & Gattupalli, K. (Year). IoT and AI-based Notification on Cloud Technologies in Healthcare. Pothi.

28. Alagarsundaram, P., Sitaraman, S. R., Gattupalli, K., & Khan, F. (2024). Implementing transfer learning and domain adaptation in IoT analytics. In RADemics (Chapter 16).

29. Devarajan, M. V., Yallamelli, A. R. G., Yalla, R. K. M. K., Mamidala, V., Ganesan, T., & Sambas, A. (2025). An Enhanced IOMT and Blockchain-Based Heart Disease Monitoring System Using BS-THA and OA-CNN. Transactions on Emerging Telecommunications Technologies, 36(2), e70055.

30. Devarajan, M. V., Yallamelli, A. R. G., Kanta Yalla, R. K. M., Mamidala, V., Ganesan, T., & Sambas, A. (2024). Attacks classification and data privacy protection in cloud-edge collaborative computing systems. International Journal of Parallel, Emergent and Distributed Systems, 1-20.

31. Yallamelli, A. R. G., Mamidala, V., Devarajan, M. V., Yalla, R. K. M. K., Ganesan, T., & Sambas, A. (2024). Dynamic mathematical hybridized modeling algorithm for e-commerce for order patching issue in the warehouse. Service Oriented Computing and Applications, 1-12.

32. Allamelli, A. R. G., Mamidala, V., Yalla, R. K. M. K., Ganesan, T., & Devarajan, M. V. (2023). Hybrid edge-AI and cloudlet-driven IoT framework for real-time healthcare. International Journal of Computer Science Engineering Techniques, 7(1), 1-XX. ISSN: 2455-135X.

33. Devarajan, M. V., Yallamelli, A. R. G., Mamidala, V., Yalla, R. K. M. K., Ganesan, T., & Sambas, A. (2024). IoT-based enterprise information management system for cost control and enterprise job-shop scheduling problem. Service Oriented Computing and Applications, 1-16.

34. Devarajan, M. V. (2019). A Comprehensive AI-Based Detection and Differentiation Model for Neurological Disorders Using PSP Net and Fuzzy Logic-Enhanced Hilbert-Huang Transform. International Journal of Information Technology and Computer Engineering, 7(3), 94-104.

35. Mohanarangan, V. D. (2022). An Improved BP Neural Network Algorithm for Forecasting Workload in Intelligent Cloud Computing. Journal of Current Science, 10(3), 1-10.

36. Devarajan, M. V. (2020). ASSESSING LONG-TERM SERUM SAMPLE VIABILITY FOR CARDIOVASCULAR RISK PREDICTION IN RHEUMATOID ARTHRITIS. International Journal of Information Technology and Computer Engineering, 8(2), 60-74.

37. Devarajan, M. V., Sacramento, C. S., & Sambas, A. (2022). DATA-DRIVEN TECHNIQUES FOR REAL-TIME SAFETY MANAGEMENT IN TUNNEL ENGINEERING USING TBM DATA.

38. Devarajan, M. V., Al-Farouni, M., Srikanteswara, R., Bharattej, R. R. V. S. S., & Kumar, P. M. (2024, May). Decision Support Method and Risk Analysis Based on Merged-Cyber Security Risk Management. In 2024 Second International Conference on Data Science and Information System (ICDSIS) (pp. 1-4). IEEE.

39. Devarajan, M. V. (2023). ENHANCING TRUST AND EFFICACY IN HEALTHCARE AI: A SYSTEMATIC REVIEW OF MODEL PERFORMANCE AND INTERPRETABILITY WITH HUMAN-COMPUTER INTERACTION AND EXPLAINABLE AI. International Journal of Engineering Research and Science & Technology, 19(4), 9-31.

40. Devarajan, M. V. (2020). Improving security control in cloud computing for healthcare environments. Journal of Science and Technology, 5(06), 178-189.

41. Devarajan, M. V., Aluvala, S., Armoogum, V., Sureshkumar, S., & Manohara, H. T. (2024, August). Intrusion Detection in Industrial Internet of Things Based on Recurrent Rule-Based Feature Selection. In 2024 Second International Conference on Networks, Multimedia and Information Technology (NMITCON) (pp. 1-4). IEEE.

42. Thirusubramanian, G. (2020). Machine learning-driven AI for financial fraud detection in IoT environments. International Journal of HRM and Organizational Behavior, 8(4), 1-16..

43. Ganesan, T. (2021). Integrating artificial intelligence and cloud computing for the development of a smart education management platform: Design, implementation, and performance analysis. International Journal of Engineering & Science Research, 11(2), 73–91.

44. Ganesan, T. (2022). Securing IoT business models: Quantitative identification of key nodes in elderly healthcare applications. International Journal of Management Research & Review, 12(3), 78-94. ISSN: 2249-7196.

45. T. Ganesan, R. R. Al-Fatlawy, S. Srinath, S. Aluvala and R. L. Kumar, "Dynamic Resource Allocation-Enabled Distributed Learning as a Service for Vehicular Networks," 2024 Second International Conference on Data Science and Information System (ICDSIS), Hassan, India, 2024, pp. 1-4, doi: 10.1109/ICDSIS61070.2024.10594602.

46. T. Ganesan, M. Almusawi, K. Sudhakar, B. R. Sathishkumar and K. S. Kumar, "Resource Allocation and Task Scheduling in Cloud Computing Using Improved Bat and Modified Social Group Optimization," 2024 Second International Conference on Networks, Multimedia and Information Technology (NMITCON), Bengaluru, India, 2024, pp. 1-5, doi: 10.1109/NMITCON62075.2024.10699250.