iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: IX Month of publication: September 2025

DOI: https://doi.org/10.22214/ijraset.2025.74381

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IX Sep 2025- Available at www.ijraset.com

Cryptography based Network Security Analysis using Secure Hashed Identity Message Authentication

Asst. Prof. Nagarathna C[1], Prabhat Rai[2], Prajwal Patel AN[3], S Shrisha[4], Shreyas S[5]
Dept. of CSE Sapthagiri College of Engineering

Abstract: Network security in resource-constrained environments has become a critical challenge due to limited memory, power restrictions, and vulnerabilities to encryption attacks. Traditional approaches, such as Proxy Re-Encryption (PRE) and Lightweight Symmetric Asymmetric Encryption (LSAE), often sufferfrom computational overhead, latency, and inefficiency in real-timesystems. To address theseconcerns, this workproposesaSecureHashedIdentityMessageAuthentication (SHIMA) model that ensures data integrity, authentication, and efficient end-to-end encryption.Theproposed schemeintegrates SHIMAwithimprovedalgorithmssuchasAdvancedEncryption RSA (AERSA), Mono-alphabetic key substitution, and a modifiedCaesarcipher,therebyachievingenhancedsecurityand reduced latency. Simulation results demonstrate that SHIMA minimizes time complexity, improves packet delivery ratio, and increases throughput when compared to conventional schemes like PRE and LSAE. This framework provides a robust foundation for efficient, scalable, and secure communication across networked environments.
Keywords: SHIMA, Proxy Re-Encryption (PRE), Lightweight Symmetric Asymmetric Encryption (LSAE), Advanced Encryption RSA, Network Security, Authentication

I. INTRODUCTION

With the rapid expansion of computer networks and cloud-based communication, ensuring secure and efficient data transfer has become a major challenge. Traditional encryption methods, although strong in theory, often fail in practical environments due to high computation costs, key management issues, and vulnerabilityto adaptiveattacks. Inparticular, identity- based encryption (IBE) has emerged as an attractive primitive,reducingtherelianceontraditionalpublickey infrastructure by associating private keys with user identities. ThismakesIBE highly relevantfor real-world applicationssuchasemail,intranetcommunication,and distributed network systems. Despite these advantages, the growing sophistication of cyberattacks highlights the need for more robust security mechanisms.

Standard symmetric and asymmetric cryptographic algorithms are still prone to delays, re-encryption overheads, and vulnerabilities such as ciphertext leakage and insider attacks. Proxy Re-Encryption (PRE) and Lightweight Symmetric Asymmetric Encryption(LSAE), though efficient in some aspects, introduce latency and computational bottlenecks that hinder their adoption in large-scale, real-time systems.

To overcome these challenges, this work introduces the SecureHashedIdentityMessageAuthentication(SHIMA) framework,whichleverageshashing-basedauthentication along with advanced cryptographic primitives to strengthen data confidentiality, integrity, and authentication. SHIMA operates by assigning unique hashed identities for secure communication sessions, thereby reducing re-encryption delays and ensuring lightweight yet robust security.

The proposed scheme integrates multiple cryptographic layers such as Advanced Encryption RSA (AERSA), mono-alphabeticsubstitution,andmodifiedCaesarcipher toenhanceresilienceagainstbrute-forceandcryptanalytic attacks. Simulation results show that SHIMA improves latency,packetdeliveryratio,andthroughputcomparedto existing PRE and LSAE schemes. This makes SHIMA highly suitable for resource-constrained and real-time environments such as IoT networks, wireless communication, anddistributedcomputingsystems.

II. BACKGROUND AND MOTIVATION

A. *Importance of Secure Communication*

Withthegrowinguseofcloudcomputing,wirelessnetworks,and distributed systems, ensuring confidentiality, authentication, and integrity of transmitted data has become critical. Sensitive informationtravelingacrossopennetworksishighlyvulnerableto tampering, eavesdropping, and forgery if robust cryptographic mechanisms are not applied.

B. *Limitations of Conventional Schemes*

Conventional encryption models such as Proxy Re-Encryption (PRE) and Lightweight Symmetric Asymmetric Encryption (LSAE)aimtoreducecomputationcostsbutoftensufferfromhigh latency, re-encryption overheads, and scalability issues. Additionally,thesesystemsarepronetoadaptiveleakageattacks, insiderthreats,andbrute-forceattempts,makingtheminsufficient for modern high-performance applications.

C. *Motivation*

Thisworkismotivatedbytheneedforalightweight,scalable,and secure encryption model that ensures both computational efficiency and strong authentication, particularly in real-time, resource-constrained environments such as IoT devices, wireless clients, and cloud servers. The proposed Secure Hashed Identity Message Authentication (SHIMA) introduces unique hashed identitiesforeachsessiontomaintainintegrityandresistreplayor forgery attacks, while reducing time complexity and latency by minimizing re-encryption delays. By integrating AERSA, mono- alphabetic substitution, and a modified Caesar cipher, SHIMA enhances authentication, throughput, and resilience against cryptanalysis without overloading end-user devices, making it suitableforbothsmall-scaleandlarge-scalenetworkapplications, while ensuring adaptability, trustworthiness, and reliable data security across diverse communication infrastructures.

III. LITERATURE SURVEY

A. *X.DuanandX.Wang(2015):AuthenticationHandoverand Privacy Protection in 5G HetNets*

METHODOLOGY: Proposed an authentication handover scheme using software-defined networking to provide secure communication in heterogeneous 5G networks. It ensures seamless mobility and privacy by dynamically managing identities.

LIMITATIONS: Although efficient, the model has high implementationcomplexityinreal-worldnetworks.Scalability remains an issue with multiple heterogeneous environments and large user bases.

B. *Y. Feng and C. Zhaohui (2016): Overview of SM9 Identification and Cryptography Algorithm*

METHODOLOGY: Introduced the SM9 identity-based cryptography standard, which provides identity-driven encryption and digital signatures. It reduces reliance on traditional certificate-based infrastructures.

LIMITATIONS:The system's reliance on a private key generator (PKG) introduces trust issues and potential single pointsoffailure.Italsofacesefficiencychallengeswhenscaled to large user networks.

C. *S. R. Shree et al. (2019): Efficient RSA Cryptosystem using Cuckoo Search Optimization*

METHODOLOGY: Enhanced RSA encryption by applying cuckoo search optimization for selecting strong keys, thereby improving resistance against cryptanalysis.

LIMITATIONS: While stronger, the model increases computation cost in key generation. Applicability in resource- constrained systems is limited.

D. *W. Jiajia et al. (2019): LTE Decryption Method Based on Air Interface*

METHODOLOGY:Developed methods for decrypting LTE communication at theairinterface, focusingon secure key retrieval mechanisms to prevent interception.

LIMITATIONS:HighlyspecifictoLTEenvironmentsand may not apply universally across all wireless protocols. Vulnerable to advanced 5G and beyond-network threats.

E. *Liu et al. (2020): Network Security using PCA and BP Neural Networks*

METHODOLOGY: Applied principal component analysis (PCA) with backpropagation neural networks for anomaly detection in network traffic to identify malicious behavior. LIMITATIONS:Performance depends on dataset quality. Highfalsepositivesindynamicenvironmentsreduce reliability.

F. Chen et al. (2019): Blockchain-Based Searchable Encryption in Cloud-Assisted Vehicular Social Networks

METHODOLOGY**:** Combined blockchain with searchable public key encryption to achieve forward and backward privacy in vehicular communication networks. LIMITATIONS**:**Blockchainintroducesoverheadinstorage and latency. Practical deployment in real-time vehicular systems is challenging.

G. Sujan et al. (2021): Multicarrier Radar Signal Optimization

METHODOLOGY:Proposed methods for joint reduction of sidelobe and PMEPR in radar signals to enhance secure transmission.
LIMITATIONS:Focusesmoreonsignaloptimizationrather than direct cryptographic network security. Limited adaptability to general-purpose communication networks.

H. B. Chen et al. (2019): Lightweight Searchable Public- Key Encryption with Forward Privacy

METHODOLOGY: Introduced a lightweight encryption scheme for Industrial IoT environments, enabling forward privacy and efficient data outsourcing.
LIMITATIONS: Vulnerable to insider keyword-guessing attacks. Lacks robustness for large-scale data environments.

I. S.-F. Sun et al. (2018): Practical Backward-Secure Searchable Encryption

METHODOLOGY:Designedsearchableencryptionbasedon puncturable encryption, ensuring backward security by invalidating previously compromised keys.
LIMITATIONS: High computational complexity and increased memory consumption in large datasets.

J. Nalla and Chalavadi (2015): Sparse Representation- Based Iris Classification.

METHODOLOGY:Used online dictionary learning for iris- based biometric authentication and secure deduplication in large-scale storage systems.
LIMITATIONS: Specialized to biometric applications, limiting broader application in generic network security.

K. Y. Miao et al. (2018): Verifiable Multi-Keyword Search over Encrypted Cloud Data

METHODOLOGY: Developed searchable encryption allowing multiple keyword queries with verifiability, improving efficiency in encrypted cloud databases.
LIMITATIONS: Performance suffers when handling very large datasets and high-frequency queries.

L. M.Naveedetal.(2015):InferenceAttacksonEncrypted Databases

METHODOLOGY: Demonstrated how property-preserving encrypteddatabasescanbeattackedusingstatisticalinference and access pattern leaks.
LIMITATIONS: Highlights vulnerabilities but does not propose complete countermeasures.

M. L.Sunetal.(2018):SecurePublicKeyEncryptionAgainst Keyword Guessing Attacks

METHODOLOGY: Proposed encryption methods using indistinguishability obfuscation to resist insider keyword- guessing attacks.
LIMITATIONS: Computationally expensive and impractical for lightweight or real-time applications, especially in resource-constrained environments requiring efficiency, scalability, and secure communication.

N. HemanthKumarandRamesh(2019):PowerReductionin IoT Devices

METHODOLOGY: Designed energy-efficient encryption strategies to extend IoT device lifetime while maintaining secure data transfer.
LIMITATIONS: Focuses mainly on power optimization, lacking comprehensive analysis of strong cryptographic resistance.

O. Lightweight Authenticated-Encryption Scheme for IoT (2019)

METHOLOGY:Proposedapublish-subscribecommunication model with lightweight authenticated encryption suitable for IoT data exchange.
LIMITATIONS: Limited to specific IoT environments. Scalability across large, heterogeneous networks remains uncertain.

P. ConstructionBasedonLWE(v19)–ZiqingWangYear2024

METHODOLOGY: Wang et al. suggest two lattice-based PAEKS schemes based on the Learning with Errors (LWE) problem-one in the random oracle model and the other in the standard model-to be resistant to inside keyword guessing attacks while providing post-quantum security.

LIMITATIONS: The work is mainly theoretical, with no publicly known implementation nor real-world benchmarks offered,sopracticalperformanceandscalability aresomewhat in doubt. Although the schemes minimize certain sizes and computation costs, the use of LWE-based lattice constructions could still be efficiency-constraining, especially in resource- limited environments.

Q. FenWang-"Key-UpdatablePEKSwithCiphertextSharing"Year:2022

METHODOLOGY: Public Key Encryption with Keyword Search(PEKS)mechanisms.StandardPEKSispronetodanger when secret keys are revealed and is inflexible when the encryptedkeywordciphertextsneedtobeupdatedorshared.To solve this, the authors designed a Key-Updatable Ciphertext Sharing PEKS (KU-CS-PEKS) scheme. This model enables public and secret keys to be updated during system run to minimize risks of key leakage, and it incorporates ciphertext sharingfunctionality,whichwasnotaddressedinpreviousKU- PEKS frameworks.

LIMITATIONS: It fails to completely examine the computational or communication overhead of ciphertext updating, creating doubt regarding efficiency on a massive scale. Although it enhances privacy, the scheme continues to possess assumptions about secure transmission of search tokens, potentially creating vulnerabilities. The security analysis primarily considers ciphertext and token privacy but doesn't extensively discuss stronger adversary models such as collusion or active keyword-guessing attacks.

R. BoQin-LightweightPublicKeyEncryptionwithKeyword Search for IoT Devices Year: 2022

METHODOLOGY: attempting to close the gap between limited device capabilities and the demand for secure, searchable encryption. The scheme makes use of computationally efficient cryptographic primitives—like elliptic curvemethods, performant trapdoor functions,or light hashstructures—toachieveminimalcomputationalburdenand memory consumption, making it viable for low-energy, low- storage environments. Its most significant advantages are efficientkeymanagement,minimizedciphertextandtrapdoor sizes, and support for keyword search with negligible overhead, thus facilitating the practical deployment in battery-constrained sensors or edge modules.

LIMITATIONS: No large-scale performance metrics. Restricted security model (e.g., lacks side-channel, keyword-guessing protection). Trust assumptions that can restrict real-world resilience.

S. SALEHIBRAHIM,ALAA-"ANew12-BitChaoticImage Encryption Scheme Using a 12 × 12 Dynamic S-Box"Year:2024

METHODOLOGY: Saleh Ibrahim and Alaa M. Abbas proposed a new 12-bit chaotic image encryption algorithm in 2024 specifically designed for medical imaging, utilizing a key- dependent 12 × 12 dynamic S-box to provide both improved security and efficiency in processing high-precision grayscale data. Their design provides much stronger confusion and key sensitivity compared to traditional 8-bit S-box designs while reaching encryption rates of up to 300 MB/s, roughly 3.3 times faster, and consistently passing standard security tests.

LIMITATIONS: In spite of these positives, security analysis of the scheme seems restricted to simple tests with no mention of defensibility against sophisticated cryptanalysis like chosen- plaintext,differential,orside-channelattacks.Moreover,useofa 12-bit S-box structure could impose greater implementation complexity and hardware or memory requirements, which might debar incorporation onto resource-limited platforms. Furthermore, although the performance claims are quite strong, the reported testsarenarrow in scopeto controlled environmentsalone,leaving doubt regarding robustness and scalability across varied, real- world medical imaging contexts.

T. Zhangetal-"SurveyonPEKSinCloud(v20)"Year:2023

METHODOLOGY:PublicKeyEncryptionwithKeywordSearch (PEKS) in cloud storage environments. They classify past PEKS schemesbasedon their cryptographic foundationincluding those based on public key infrastructure, identity-based encryption, attribute-based encryption, predicate encryption, certificateless systems, and proxy re-encryption methods.

LIMITATIONS:Inspiteofitscomprehensiveness,thesurveyhas some limitations. Firstly, having been published in 2020, it does not encompass more recent developments — e.g., advancements in PEKS-ABE systems, blockchain incorporation, or quantum-resistant versions that materialized after 2020

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IX Sep 2025- Available at www.ijraset.com

IV. METHODOLOGY

TheproposedmethodologyintroducestheSecureHashedIdentity Message Authentication (SHIMA) framework to strengthen network security by ensuring data confidentiality, integrity, and authentication while minimizing re-encryption overhead in dynamic communication environments. The system integrates Advanced Encryption RSA (AERSA), Mono-alphabetic substitution, and a modified Caesar cipher, working together seamlesslytoimproveefficiency,scalability,andresiliencewhile effectively resisting various forms of cryptographic attacks.

A. SystemInitializationandKeyGeneration

In this phase, a key generator module produces RSA-based public and private keys. SHIMA then assigns a unique hashed identity to each communication session using secure hash functions. Session keys are derived from identity hashing to enable lightweight encryption and authentication.

.

B. AdvancedEncryptionRSA(AERSA)

The objective of AERSA is to improve encryption performance by optimizing RSA key generation using non- prime randomization. The process involves generating the modulusM=p×qM=p/timesqM=p×qusingoptimized non-prime selection, computing the private/public key pair forencryption,andencryptingnetworkpacketswithAERSA beforetransmission.Theoutcomeisstrongprotectionagainst brute-force attacks while reducing key computation time.

C. TrapdoorGenerationandSHIMAIdentityHashing

EachmessagerequestishashedwithSHIMA’s160-bitidentity function. Message blocks are padded to 512-bit segments and processed through 80 rounds of hash functions. This generates a secure digest that authenticates the sender’s identity and preventsreplayorforgerybyensuringeachrequestisuniquely bound to the sender’s identity.

D. Mono-AlphabeticSubstitution

This phase adds a lightweight character substitution layer for additional obfuscation. Plaintext characters are replaced with fixed substitutes (e.g., A→U, B→N, C→I), which enhances confusion and reduces predictability in transmitted data. It is usedasapreprocessingstepbeforeSHIMAhashingtoprovide added complexity.

E. ModifiedCaesarCipher

Inthisstep,ashiftingmechanismisappliedtothecharactersof encryptedtext. Key-dependentshiftsensurethatevenrepeated characters produce different ciphertext outputs, thereby providing additional resistance against frequency analysis attacks.

F. SecureDataTransmission

Encrypted packets are transmitted across the network with SHIMA-based authentication. At the receiver side, SHIMA validates the hashed identity before decrypting, ensuring that only authenticated clients can access the transmitted information.

G. PerformanceandAttackResistance

Finally, the scheme resists brute-force and cryptanalysis by combiningmultipleencryptionlayers.SHIMAhashingintroduces non-deterministic trapdoors that prevent replay and identity forgery. Compared to PRE and LSAE, SHIMA reduces latency, improves throughput, and enhances the packet delivery ratio.

V. CONCLUSION

Withtheincreasingrelianceonnetworkedcommunicationsystems, the need for secure, efficient, and scalable encryption mechanisms has become more critical than ever. Conventional methods such as Proxy Re-Encryption (PRE) and Lightweight Symmetric Asymmetric Encryption (LSAE) offer certain advantages but are limited by latency, computational complexity, and vulnerability to adaptive attacks.

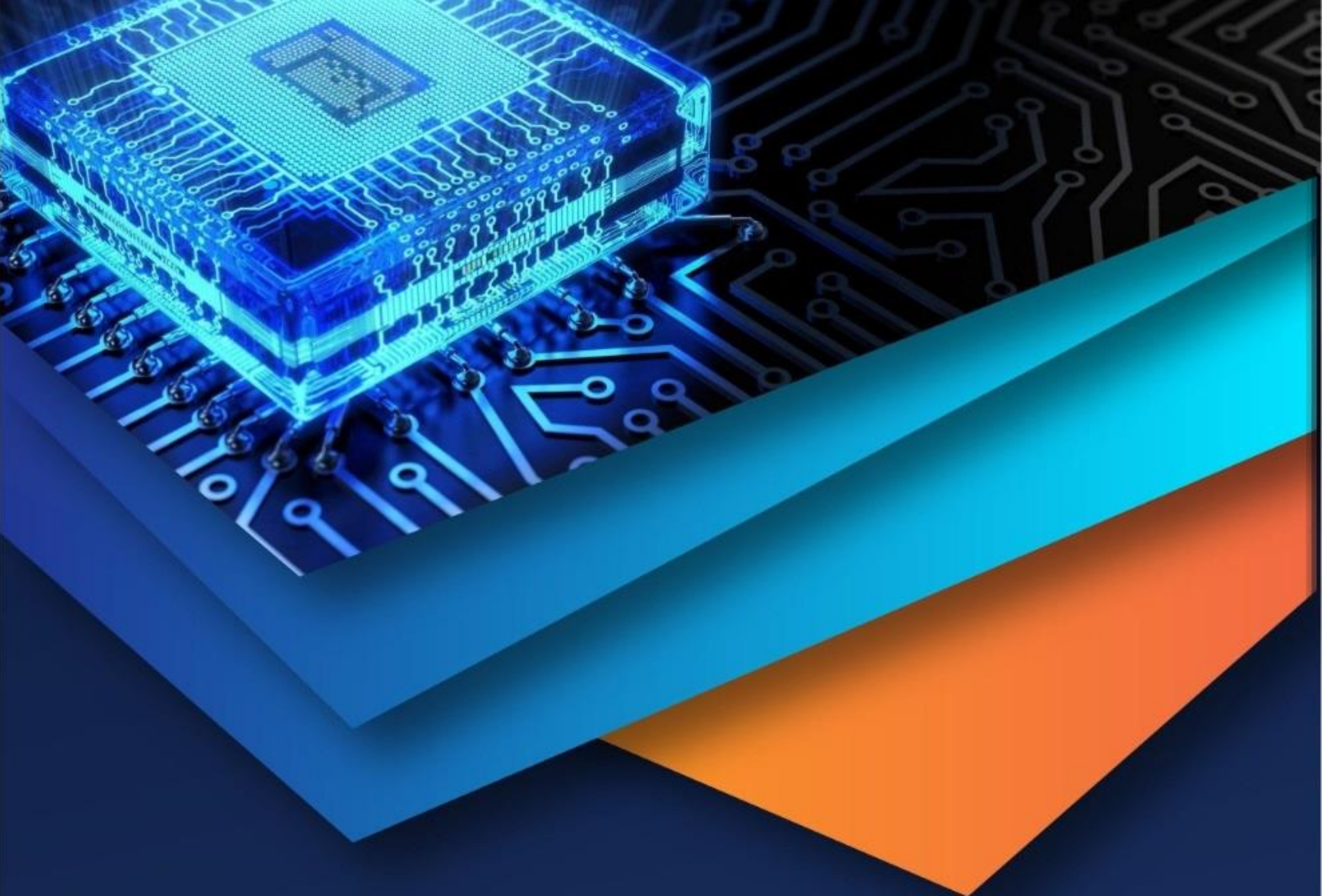
The proposed Secure Hashed Identity Message Authentication (SHIMA) framework addresses these challenges by combining identity-based hashing with layered cryptographic techniques such as AERSA, mono-alphabetic substitution, and modified Caesar cipher. This integration ensures that transmitted data maintains its confidentiality,authenticity,andintegritywhilealsominimizingre-encryption delays.

Simulation results validate that SHIMA outperforms existing models by achieving lower latency, reduced time complexity, higher packet delivery ratios, and improved throughput performance. Furthermore, its lightweight design makes it suitable for resource-constrained devices in IoT and wireless environments as well as for larger-scale distributed cloud systems.

Thus, SHIMA provides a balanced solution that combines robustness with practicality, making it a strong candidate for next-generation secure communication frameworks.

REFERENCES

[1] X. Duan and X. Wang, “Authentication handover and privacy protection in 5G HetNets using software-defined networking,” IEEE Communications Magazine, vol. 53, no. 4, pp. 28–35, Apr. 2015.
[2] Y.Feng and C. Zhaohui, “Overview of SM9 identification and cryptography algorithm,” Information Security Research, vol. 2, no. 11, pp. 1008–1027, 2016.
[3] S.R.Shree,A.C.Chelvan,andM.Rajesh,“AnefficientRSA cryptosystem by applying cuckoo search optimization algorithm,” Concurrency and Computation: Practice and Experience, vol. 31, no. 12, Jun. 2019.
[4] W. Jiajia, Y. Chuanwei, W. Lei, and S. Jiaqi, “Research on LTE decryptionmethodbasedonairinterface,”Electronics Products World, vol. 26, no. 8, pp. 40–42, 2019.
[5] F.Liu,W.Huo,Y.Han,S.Yang,andX.Li,“Studyonnetwork security based on PCA and BP neural network under green communication,” IEEE Access, vol. 8, pp. 53733–53749, 2020.
[6] B. Chen, L. Wu, H. Wang, L. Zhou, and D. He, “A blockchain-based searchable public-key encryption with forward and backward privacy for cloud-assisted vehicular social networks,” IEEE Transactions on Vehicular Technology, pp. 1–1, 2019.
[7] L. J. L. Sujan, V. D. Telagadi, C. G. Raghavendra, B. M. J. Srujan,R.B.VinayPrasad,B.D.Parameshachari,andK.L. Hemalatha, “Joint reduction of sidelobe and PMEPR in multicarrierradarsignal,”inCognitiveInformaticsandSoft Computing:ProceedingsofCISC2020,SpringerSingapore, 2021, pp. 457–464.
[8] B. Chen, L. Wu, N. Kumar, K.-K. R. Choo, and D. He, “Lightweightsearchablepublic-keyencryptionwithforward privacy over IIoT outsourced data,” IEEE Transactions on Emerging Topics in Computing, 2019.
[9] S.-F. Sun, X. Yuan, J. K. Liu, R. Seinfeld, A. Sakzad, V. Vo, and S. Nepal, “Practical backward-secure searchable encryption from symmetric puncturable encryption,” in Proceedings of the 2018 ACM SIGSAC Conference on ComputerandCommunicationsSecurity,pp.763–780,2018.
[10] P. R. Nalla and K. M. Chalavadi, “Iris classification based on sparse representations using on-line dictionary learning for large-scale de-duplication applications,” SpringerPlus, vol. 4, no. 238, 2015.
[11] Y. Miao, J. Weng, X. Liu, K.-K. R. Choo, Z. Liu, and H. Li, “Enablingverifiablemultiplekeywordsearchoverencrypted clouddata,”InformationSciences,vol.465,pp.21–37,2018.
[12] M.Naveed,S.Kamara,andC.V.Wright,“Inferenceattacks on property-preserving encrypted databases,” in Proceedings of the 22nd ACM SIGSAC Conference on ComputerandCommunicationsSecurity,pp.644–655,2015.
[13] L.Sun, C. Xu, M. Zhang, K. Chen, and H. Li, “Secure searchable public key encryption against insider keyword guessing attacks from indistinguishability obfuscation,”
[14] G.HemanthKumarandG.P.Ramesh,“Reducingpower feasting and extend network life time of IoT devices through localization,”InternationalJournalofAdvancedScienceand Technology, vol. 28, no. 12, pp. 297–305, 2019.
[15] “Lightweight authenticated-encryption scheme for Internet of Things based on publish-subscribe communication,” IEEE Access, pp. 60539–60551, 2019.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY