iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** III **Month of publication:** March 2026

DOI: https://doi.org/10.22214/ijraset.2026.78202

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

Mercury

Aftab Mohamed Thayyil[1], Muhammed Aman[2], Fathimathul Amana Sulaiman[3], Shibila Shirin[4], Asst. Prof. Athira Balachandran
Department of Computer Science and Engineering Sree Narayana Guru College of Engineering and Technology Kerala, India

Abstract: ***Decentralized communicationplatformsoftenop- erate independently, limiting interoperability and reliable data exchangeacrossapplications.Traditionalmessagingsystemsrely on isolated infrastructures and centralized identity management. To address these challenges, this paper presents the Mercury Framework, a decentralized messaging model that uses wallet-based addressing, where blockchain wallet identities replace traditional usernames for secure and user-controlled identity verification. The framework integrates edge computing with a libp2p relay network to enable distributed message routing, caching, and encryption, improving scalability and reducing latency.Securemulti-partycommunicationissupportedthrough theDoubleRatchetencryptionprotocolandadelegationscheme, ensuring forward secrecy and efficient group synchronization. Overall, the Mercury Framework provides a secure, scalable,and interoperable approach for decentralized communication.***
Index Terms: ***Decentralized communication, blockchain iden- tity,wallet-basedaddressing,libp2prelaynetwork,edgecomput-ing,DoubleRatchetprotocol,securemessaging,interoperability.***

I. INTRODUCTION

Traditionalcommunicationsystemsarepredominantlybuilt on centralized architectures in which user data and message transactions are processed through a limited number ofservers managed by a single authority. Although this structure simplifies system administration and monitoring, it introduces several concerns related to privacy, security, and reliability. Sensitiveuserinformationandcommunicationmetadata maybeexposedtosurveillance,misuse,ordatabreaches.

Inaddition,centralizedinfrastructurescreatesinglepoints of failure, where disruptions, cyberattacks, or infrastructure breakdowns can affect the entire communication network. Anotherlimitationofcentralizedsystemsisthelackof user autonomy and control over digital identities and data ownership.Sinceauthenticationandidentitymanagement are typically handled by centralized service providers, users must rely on external platforms to verify and manage their identities. This dependency increases the risk of censorship, unauthorizeddataaccess,andmanipulationofcommunication records. As digital communication becomes more integrated withdistributedtechnologies,thereisagrowingdemand for architectures that prioritize privacy, transparency, and resilience.

Decentralizedcommunicationframeworksaimtoaddress these challenges by distributing communication responsibilitiesacrossa networkofindependentnodes. Insuchsystems,messagetransmissionandvalidationoccurcollaborativelyamongpeersratherthanrelyingon a central authority. The Mercury Framework adopts this decentralized approach to improve network reliability and privacy protection. By distributing data across multiplenodes, the system minimizes centralized control and enhances resistance to tampering, surveillance, and denial-of-service attacks.AkeyfeatureoftheMercuryarchitectureisthe useofwallet-basedaddressing,wheretraditionalidentifiers such as usernames, email addresses, or phone numbers are replaced by cryptographic wallet addresses. Each address is linked to a public–private key pair stored securely on the user's device, allowing secure authentication and encrypted communication. This approach also enables integration with blockchain technology, which supports decentralized identity management through immutable identity records, secure key updates, and revocation mechanisms.

Tofurtherenhanceperformanceandscalability,theMercury framework incorporates edge computing within its communi- cation infrastructure. Edge nodes, including relay devices and local gateways, can process and temporarily store message data closer to users. This reduces communication latency and network congestion while ensuring that message delivery can continue even under unstable or limited connectivity condi- tions. Such capabilities are particularly beneficial in remoteor resource-constrained environments. Finally, the reliability of the decentralized network is reinforced through lightweight consensus mechanisms that verify the behavior of relay nodes andmaintaincommunicationintegrity.Theseprotocolsensure that only trusted nodes participate in message routing and validation, preventing malicious activity within the network. By combining decentralized messaging, wallet-based identity management, edge computing, and consensus validation, the Mercury Framework establishes a secure, scalable, and au- tonomous communication model suitable for next-generation decentralized applications.

©IJRASET: All Rights are Reserved

II. RELATED WORKS

A. *Decentralized Encrypted Communication Systems Based on Blockchain*

Recent studies have explored the use of blockchain technology to develop secure and decentralized communication platforms. The work titled "Decentralized Encrypted Communication Systems Based on Blockchain" investigates how blockchain, end-to-end encryption (E2EE), and decentralized storage can be combined to enhance the security of digital communication. The proposed approach utilizes distributed ledger technology and public key cryptography to protect user privacy and reduce dependence on centralized servers. In this model, decentralized identity verificationandPublicKeyInfrastructure(PKI)areused forkeygeneration,whilemessagesareencryptedusingthe recipient's public key before being transmitted across blockchain networks such as Ethereum. This design ensures message confidentiality, integrity, and resistance to tampering duringtransmission.However,thestudymainlyfocuseson the architectural design and security concepts of thesystem. Practical considerations such as scalability, latency, regulatory constraints, and real-world deployment challenges arenotextensivelyaddressed.Consequently,issuesrelated to performance optimization and the ability to support large-scaleuseradoptionremainopenareasforfurtherinvestigation.

B. *An Improving Secure Communication Using Multipath Malicious Avoidance Routing Protocol in Underwater Sensor Network*

Thestudy"AnImprovingSecureCommunication UsingMultipathMaliciousAvoidanceRoutingProtocol in Underwater Sensor Network" presents a secure andenergy-efficient communication approach for Underwater WirelessSensorNetworks(UWSNs).Theauthorspropose a multipath routing strategy designed to mitigate malicious nodebehaviorwhilemaintainingreliabledatatransmission in challenging underwater environments. The framework integrates the Multipath Malicious Avoidance Routing Protocol(M2ARP)withlightweightencryptionmethods andoptimizationtechniquestoaddressissuessuchas high propagation delay, limited bandwidth, and security vulnerabilities. Additional components, including FM-PRFRS encryption, energy-efficient node selection, and CuckooSearchOptimizationforclusterheadselection, areintroducedtoimprovenetworksecurityandextend the operational lifetime of sensor nodes. Experimental simulations demonstrate improvements in secure datadelivery and energy efficiency. However, the study primarily emphasizes protocol design and simulation-based evaluation. Practical considerations such as real-world underwater deployment challenges, hardware constraints, scalability, and long-term reliability in harsh marine environments are not extensively discussed, leaving these aspects open for further investigation.

C. *EnhancingReliabilityandStabilityofBLEMeshNetworks Through Multipath Optimized AODV Protocol*

The study explores improvements in routing mechanisms for Bluetooth Low Energy (BLE) mesh networks used in Internet of Things (IoT) environments. The study highlights the limitations of existing routing approaches, particularly flooding-basedroutingandthetraditionalAdhocOn-Demand DistanceVector(AODV)protocol.Whilefloodingtechniques can achieve a high Packet Delivery Ratio (PDR), they often introduce significant network overhead and communication delays. On the other hand, AODV reduces overhead but may compromise reliability in dynamic network conditions. To address these challenges, the authors propose a Multipath Optimized AODV (M-O-AODV) protocol that establishes alternative routing paths during the route discovery phase.This multipath strategy improves network robustness and enablesfasterlinkrecoverywhencommunicationpathsfail. Experimental evaluations demonstrate improvements in reliabilityandroutingperformance.However,thestudymainly relies on controlled experimental environments with a limited number of nodes. As a result, aspects such as large-scale deploymentperformance,long-termenergyconsumption, and adaptability in highly dynamic IoT environments require further investigation.

D. *Blockchain-AwareDecentralizedIdentityManagementand Access Control (BADIMAC) Mode*

A blockchain-based decentralized identity management approach known as the BADIMAC (Blockchain-Aware Decentralized Identity Management and Access Control) model has been proposed to address the security limitationsoftraditionalcentralizedidentitymanagementsystems.Inconventionalsystems,identityinformationisstoredincentralizeddatabases,whicharehighlyvulnerableto databreaches,identitytheft,andunauthorizedaccess. The BADIMAC framework shifts identity ownership from service providers to individual users by utilizing blockchain technology to create a transparent and tamper-resistantidentity management structure. Instead of storing complete identity data on the blockchain, the model records only encrypted hashes of identity documents, while sensitive information remains stored off-chain to preserve privacy.

Users manage their identities through private key ownership and policy-based access control mechanisms, enabling secure authentication and controlled data sharing. Although this approach improves user autonomy and privacy protection, challenges related to large-scale implementation, transaction costs, system performance, and interoperability with existing identity infrastructures remain areas that require further investigation.

E. Blockchain for Secure and Decentralized Artificial Intelli- gence in Cybersecurity

Blockchain technology has also been explored as a foun- dation for secure and decentralized artificial intelligence in cybersecurity systems. By combining blockchain with de- centralized AI (D-AI), security frameworks can benefit from both distributed data processing and tamper-resistant data management. In such architectures, blockchain provides an immutableledgerthatrecordstransactionsandsecurityevents, while decentralized AI enables collaborative analysis and decision-makingacrossmultiplenodeswithoutrelyingona central authority. This integration improves transparency, strengthens trust among participating entities, and reduces vulnerabilities associated with centralized security infrastruc- tures, such as single points of failure or unauthorized data modification.Additionally,blockchain-basedmechanismscan supportsecuredatasharing, modelvalidation,andauditability within distributed AI environments. Despite these advantages, manyexisting approaches remainlargely conceptual,focusing on architectural models and theoretical classifications rather than practical deployment. Challenges such as implemen- tation complexity, computational overhead, and integration with existing cybersecurity infrastructures still require further investigation.

III. CONCLUSION FROM LITERATURE SURVEY

The reviewed literature highlights the increasing impor- tance of decentralized technologies in improving the security, reliability,andtransparencyofmoderncommunicationand computing systems. Across the examined works, a common observationisthelimitationoftraditionalcentralizedarchitec- tures, which often suffer from single points of failure, privacy risks, and vulnerability to cyberattacks or data manipulation. To overcome these challenges, recent research has focused on integrating blockchain technology with advanced mechanisms such as encryption techniques, decentralized identity manage- ment, optimized routing protocols, and distributed artificial intelligence.

Blockchain technology plays a significant role in many of these proposed solutions because of its inherent properties, including immutability, transparency, and decentralized trust management. When combined with techniques such as End- to-End Encryption (E2EE), Public Key Infrastructure (PKI), multipath routing strategies, and decentralized AI processing, these frameworks aim to improve confidentiality, data in- tegrity,andsystemresilience.Applicationsoftheseapproaches have been explored in different domains, including IoT net- works, underwater sensor networks, decentralized communi- cationplatforms, andcybersecurityinfrastructures,wherethey demonstrate potential improvements in reliability, secure data transmission, and fault tolerance.

Despite these advancements, many existing studies primar- ilyemphasizeconceptualarchitecturesorsimulation-based evaluations.Keypracticalaspects—suchasscalability,net-worklatency,transactionoverhead,interoperabilitywithexist- ingsystems, andhardware limitations—areoftennotexamined indepth.Furthermore,large-scaleimplementationandlong- term performance assessments in real-world environments re- main limited, leaving several practical challenges unresolved. Overall,theliteraturesuggeststhatdecentralizedandblockchainbasedframeworkshavestrongpotentialtoreshapesecurecommunicationan dcybersecuritysystems.However,futureresearchshouldplacegreateremphasisonrealworldexperimentation,scalabilityoptimization,ands eamlessin- tegrationwithexistinginfrastructuresinordertotranslate theseconceptualmodelsintopracticalandwidelydeployablesolutions.

IV. SYSTEM ARCHITECTURE

The proposed Decentralized Multi-Path Encrypted Messaging Systemisdesignedtoprovidesecure,reliable,andscalable communication in decentralized environments. The architectureintegratesblockchain-basedidentitymanagement, end-to-end encryption, adaptive routing mechanisms, and distributed networking to ensure confidentiality, integrity, and efficient data transmission. By combining these components, the system enables secure communication without relying on centralized infrastructure.

At the initial stage, the user interface serves as the primary interaction point where users compose and send encrypted messages. Identity management within the system is handled throughablockchain-basedidentityframework,whereuser identities are associated with public cryptographic keys stored in a decentralized registry.

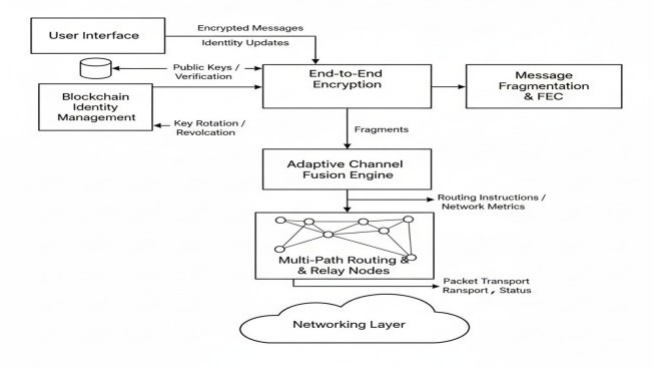


Fig. 1.Proposed Decentralized Multi-Path Encrypted Messaging SystemArchitecture.

When a message is initiated, the senderretrievesandverifiestherecipient'spublickeythrough the blockchain identity management module. This mechanism ensuressecureauthenticationwhileenablingfeaturessuch askeyrotationandrevocation, whichallow compromised or outdated keys to be updated without affecting the overall security of the network.

After identity verification, the message is processedthroughtheend-to-endencryption(E2EE)layer.Inthis stage, the sender encrypts the message using the recipient's public key so that only the intended receiver can decrypt the content using their private key. This encryption ensures that even if messages pass through multiple intermediate nodes,theactualcontentremains confidential.Onceencrypted,the message proceeds to the processing stage where it is preparedforreliable transmission.Toenhancereliability and network efficiency, the encrypted message undergoes message fragmentation and Forward Error Correction (FEC). The message is divided into smaller fragments, which allows the system to transmit them simultaneously through different network paths. The use of FEC ensures that the original messagecanstillbereconstructedevenifsomefragments are lost or delayed during transmission. These fragments are then managed by the Adaptive Channel Fusion Engine, which dynamically evaluates network conditions and determines the most suitable communication channels based on available routing information and network metrics.

Thefragmentedmessagesarethentransmittedthrough a multi-path routing mechanism supported by relay nodes. Instead of relying on a single communication route, thesystem distributes fragments across multiple relay nodes within the decentralized network. This multi-path routing strategy improves fault tolerance, enhances transmission reliability, and reduces the risk of message interception ordata loss. Finally, the networking layer manages packet transportandmonitorsdeliverystatus.Atthedestination,the receivedfragmentsarereassembled,verified,anddecrypted to reconstruct the original message securely.

Overall, the proposed architecture integrates decentralized identity verification, strong encryption mechanisms, adaptive channel management, and multi-path routing to establish a robust and secure communication framework. This design improvesprivacy,resilience,andreliability,makingitsuitablefor decentralized messaging systems and next-generation secure communication networks.

V. RESULTS AND DISCUSSIONS

TheimplementationoftheMercurySecureCommunication Framework was evaluated through a series of functional and performance tests conducted in a controlled network environment. The objective of these tests was to analyze the effectiveness of the proposed architecture in terms of secure communication, reliability, latency, and system scalability. The results indicate that the integration of decentralized networking, blockchain-based identity management, and multi-path encrypted communication significantly improves thesecurityandrobustnessofthemessagingsystem. One of the primary observations from the experimental evaluationistheimprovementinsecuremessagedelivery. By implementing end-to-end encryption mechanisms combinedwithdecentralizedidentityverification,the system ensures that only authenticated nodes can participatein communication. The blockchain-based identity layer successfullyhandledpublickeyregistration,verification, and revocation without relying on centralized authentication servers. This decentralized trust model enhanced system security and reduced the risk of identity spoofing or unauthorized access.

The multi-path communication mechanism also demonstrated significant improvements in communication reliability. Messages were fragmented and transmitted across multiple communication channels such as Wi-Fi, BLE, and LoRa.

Evenwhencertainchannelsexperiencedpacketloss or network congestion, the Forward Error Correction (FEC) mechanismenabledsuccessfulreconstructionofmessages at the receiver side. Experimental tests showed improved messagedeliverysuccessratescomparedtotraditional single-path communication approaches, particularly under unstable network conditions. Performance analysis further indicated that the use of adaptive channel selection androuting algorithms helped optimize network utilization. The system dynamically monitored parameters such as bandwidth availability, latency, and packet loss to select the mostefficient communication path. This adaptive routing approach reduced overall transmission delay and improved throughput in comparison with static routing strategies.

Intermsofsecurityevaluation,penetrationtestingandthreat modeling confirmed the effectiveness of the implemented encryptionandauthenticationmechanisms.Thecombinationoflayeredencryption,MessageAuthenticationCodes(MAC),andreplayprotection mechanismsensureddataconfidentiality and integrity during communication. Additionally, blockchain immutability enabled reliable verification of identity records and communication metadata, further strengthening trust within the network. Energy efficiency tests were also conducted to evaluate the suitability of the system for resource-constrainedenvironmentssuchasIoTdevices.The results showed that adaptive scheduling and optimized message handling reduced unnecessary communication overhead, thereby lowering energy consumption across wireless interfaces. This makes the Mercury framework suitable for deployment in decentralized and mobile communication environments.

Overall, the experimental results demonstrate that the pro- posed Mercury framework provides a secure, reliable, and scalabledecentralizedcommunicationsystem.Theintegration ofblockchain-basedidentitymanagement,multi-pathcommu- nication, and adaptive routing significantly enhances system resilience against network failures and security threats. How- ever, further research and large-scale real-world deployments are necessary to evaluate long-term performance, scalability, and interoperability with existing communication infrastruc- tures.

VI. CONCLUSION

The Mercury Project introduces a decentralized andprivacy-focused communication framework designed to address the limitations of traditional centralized messaging systems.Conventionalcommunicationplatformsoften relyoncentralizedservers, whichcreateriskssuchasdatabreaches,privacyviolations,andsinglepointsof failure. In contrast, the Mercury framework adopts a decentralized architecture based on a peer-to-peer mesh network, enabling direct communication between nodes without dependence on centralized infrastructure. This design enhances system resilience, improves reliability, and ensures thatcommunicationcancontinueevenunderunstablenetwork conditions.

To strengthen communication security, the framework integrates advanced end-to-end encryption mechanisms, including the X3DH key exchange protocol and the Double Ratchet algorithm. These cryptographic techniques ensure secure key establishment and continuous key updates during communication, thereby maintaining strong confidentialityandprotection againstunauthorizedaccess. Inaddition,the incorporation of blockchain-based identity management providesadecentralizedmethodforauthenticatingusers and managing cryptographic keys. By recording identity information and key references on the blockchain, the system ensures transparency, tamper resistance, and secure peer authentication.

AnotherimportantfeatureoftheMercuryframeworkis the use of adaptive routing and multi-path communication strategies. Messages are fragmented and transmitted across multiple channels such as Wi-Fi, Bluetooth Low Energy (BLE), and LoRa, allowing the system to dynamically select themostefficientcommunicationpath.Theintegration of Forward Error Correction (FEC) further improvesreliability by enabling message reconstruction even if some fragmentsarelostduringtransmission.Thisapproach reducescommunicationdelays,improvesfaulttolerance, and optimizes energy consumption in resource-constrained environments.

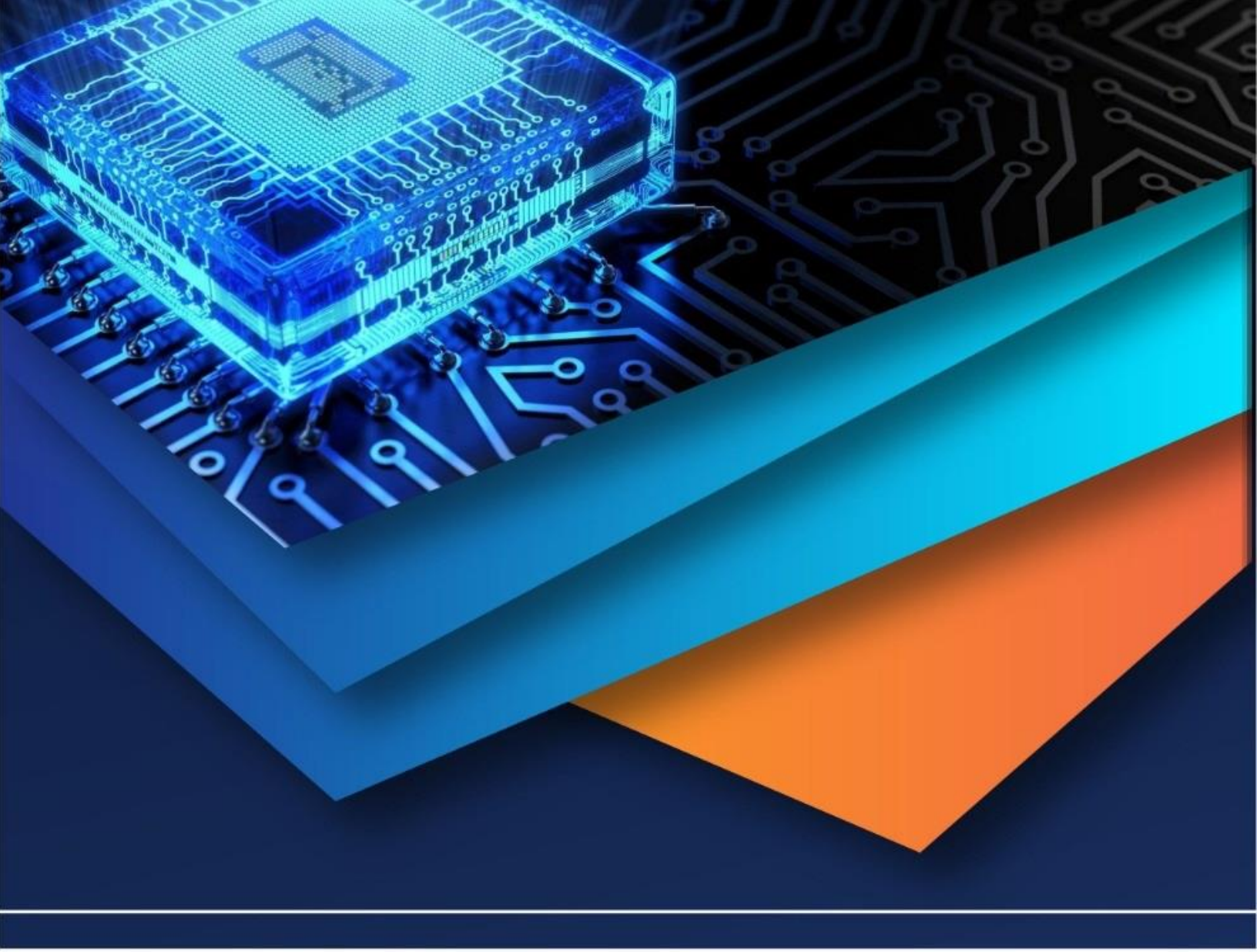
Overall, the Mercury framework provides a scalable, se- cure, and energy-efficient communication solution suitablefor next-generation decentralized applications. By combining decentralizednetworking,strongcryptographicprotection,and blockchain-basedtrustmechanisms,thesystemestablishesa reliable infrastructure for secure digital communication. Future research may focus on large-scale deployment, en- hanced routing optimization, and integration with emerging decentralizedtechnologiest ofurther improveperformanceand interoperability.

REFERENCES

[1] H.Shao,“DecentralizedEncryptedCommunication:AnInvestigationofthe Current Landscape and Future Prospect,” in Proc. 1st InternationalConference on Data Science and Engineering (ICDSE), 2024, pp.275–280, doi: 10.5220/0012821000004547.
[2] V. P. Natarajan et al., “An Improving Secure Communication UsingMultipath Malicious Avoidance Routing Protocol in Underwater SensorNetworks,” Sensors, 2024, doi: 10.3390/s24227330.

[3] M. R. Ghori et al., “Enhancing Reliability and Stability of BLE MeshNetworks Through Multipath Optimized AODV Protocol,” Sensors,vol. 24, 2024, doi: 10.3390/s24175561.
[4] H. Agrawal, M. Karyakarte, G. Chavhan, M. Patil, R. Talware, and L.Kulkarni, “Blockchain Aware Decentralized Identity Management andAccess Control System,” Measurement Sensors, vol. 31, p. 101032,2024, doi: 10.1016/j.measen.2024.101032.
[5] A.M.S.Salehetal.,“BlockchainforSecureandDecentralizedArtificialIntelligence in Cybersecurity,” Journal of Information Security andApplications, 2024, doi: 10.1016/j.jisa.2024.103746.
[6] M. B. Imtiaz and R. Kamran, “Mitigating Transmission Errors: AForwardErrorCorrection-BasedFrameworkforEnhancingVideoQual-ity,” IEEE Access, vol. 13, pp. 83261–83276, 2025, doi: 10.1109/AC-CESS.2025.3572489.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)