International Journal of Multidisciplinary Engineering in Current Research – IJMEC

Volume 11, Issue 4s, April-2026, http://ijmec.com/, ISSN: 2456-4265

Full Length Article

Cloud-Network-End Security Integration for Smart Wireless Environments

Khazi Mohammed Abdur Rahman Siddiqui[1], Syed Mohammed Ishaq Hasan[2], Mohammed Furqan Uddin[3], Dr. Abdul Ahad Afroz[4]

[1,2,3]B.E.Students; Department of Information Technology ISL Engineering College Osmania University Hyderabad India.

[4]Associate Professor; Department of Information Technology ISL Engineering College Osmania University Hyderabad India.

Mail Id; ar.siddiqui.falahi01@gmail.com, ishaqhasan870@gmail.com, mohdfurqan9849@gmail.com

Accepted 26-04-2026

Abstract

The rapid evolution of wireless communication infrastructure, cloud computing, and the Internet of Things (IoT) has fundamentally transformed modern information systems. Traditional wireless network security mechanisms, which focus primarily on end-to-end data transmission protection using cryptographic techniques, are no longer adequate for the complex demands of cloud-based collaborative services. The shift from data transmission to cloud-driven information services introduces new security vulnerabilities across cloud platforms, network layers, and end devices. To address this critical challenge, this paper proposes a Cloud-Network-End Collaborative Security Architecture that provides coordinated protection across all three layers. The proposed framework integrates Advanced Encryption Standard (AES-256) for data confidentiality, SHA-256 for integrity verification, role-based access control for authorization, and a centralized cloud server for scalable data management. The architecture is implemented using Java EE (JSP, Servlets), Apache Tomcat, and MySQL, and is evaluated through functional and non-functional testing. Results demonstrate improved data confidentiality, end-to-end integrity assurance, and efficient access control in heterogeneous network environments. The proposed system supports emerging applications including smart cities, healthcare, autonomous transportation, and industrial IoT, providing a trustworthy and scalable security foundation for next-generation wireless environments.

Keywords

Cloud-Network-End Security, *Wireless Network Security, AES Encryption, SHA-256, Cloud Computing, IoT Security, Collaborative Security Architecture, Data Integrity, Heterogeneous Networks.*

Introduction

Over the past few decades, wireless communication infrastructure has expanded rapidly to meet growing demands driven by mobile communications and the Internet of Things [1–6]. Wireless networks have become deeply integrated into daily life, forming the core infrastructure for data sharing between diverse entities. However, the inherent openness of wireless networks presents significant challenges to data security. Traditional wireless network security focused on guaranteeing the authenticity, confidentiality, integrity, and availability of data transmission through cryptographic techniques such as symmetric and public key cryptography, digital signatures, and message authentication codes [7].

With the advancement of information technologies, the core requirements of information systems are transitioning from simple data transmission to cloud-based information services. Cloud computing has made computing resources widely and economically accessible, while edge computing shifts data processing toward the network edge to reduce latency and improve efficiency. The combination of cloud and edge computing, mobile communications, and IoT creates vast opportunities in smart cities, autonomous driving, and telemedicine. Simultaneously, artificial intelligence and machine learning are becoming critical enablers of intelligent decision-making and automated service delivery.

This transformation introduces new security challenges. Data is now collected from widely distributed heterogeneous devices across networks including 4G, 5G, Wi-Fi, satellite, and aerial networks. Traditional cryptographic mechanisms, designed for homogeneous end-to-end transmission, fail to address the collaborative

https://doi.org/10.63665/IJMEC.1104s.41
ISSN: 2456-4265
IJMEC 2026

security requirements of cloud-network-end architectures. There is a critical need for a unified security framework that coordinates protection across cloud services, network connections, and end-device systems throughout the entire data lifecycle. This paper presents a Cloud-Network-End Collaborative Security Architecture designed to fill this gap, ensuring secure data sharing and collaborative processing in modern smart wireless environments.

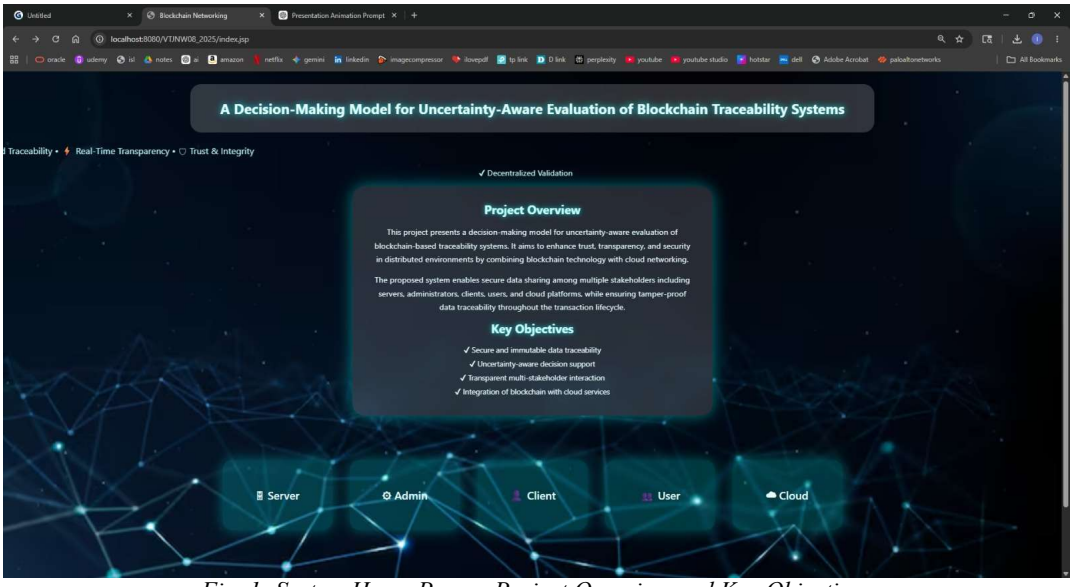

Fig. 1: System Home Page – Project Overview and Key Objectives

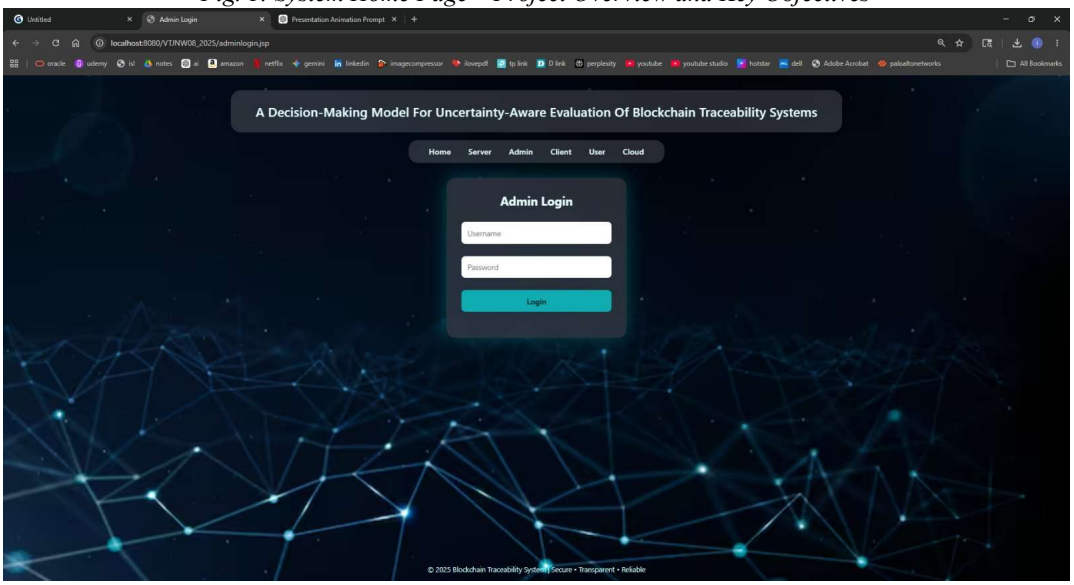

Fig. 2: Admin Login Interface – Secure Role-Based Authentication

Related Work

Shen et al. [6] surveyed next-generation computing technologies in space-air-ground integrated networks, highlighting the importance of integrating computing and communication across terrestrial, aerial, and satellite domains. Their work emphasized software-defined networking and network function virtualization for flexible resource management, and identified unified security frameworks as a critical need.

Lu et al. [14] proposed Smaug, a Trusted Execution Environment (TEE)-assisted secure SQLite framework for embedded systems. By isolating critical operations within ARM TrustZone, the system achieves strong data confidentiality with minimal computational overhead, demonstrating the effectiveness of hardware-assisted security in resource-constrained environments.

Wang et al. [54] introduced a forward/backward and content-private Dynamic Searchable Symmetric Encryption (DSSE) scheme for spatial keyword queries. Their approach prevents adversaries from learning relationships between newly added or deleted data and

https://doi.org/10.63665/IJMEC.1104s.41
ISSN: 2456-4265
IJMEC 2026

previous search queries, ensuring privacy in dynamic cloud environments.

Yang et al. [57] presented MU-TEIR, a multi-user traceable encrypted image retrieval system supporting user accountability and privacy-preserving search in cloud environments. Li et al. [78] proposed VRFMS, a verifiable ranked fuzzy multi-keyword search scheme that enables accurate and privacy-preserving information retrieval over encrypted cloud data. Yadav et al. [67] surveyed oblivious transfer protocols and their role in secure multi-party computation and privacy-preserving applications.

Despite these advances, existing solutions predominantly address isolated security components rather than providing coordinated protection across cloud, network, and end-device layers. The proposed framework addresses this gap by integrating cryptographic mechanisms, secure communication protocols, and cloud security policies into a unified collaborative architecture.

Problem Statement

The rapid convergence of wireless communication, cloud computing, and IoT technologies has increased the complexity of modern information systems significantly. Traditional wireless security mechanisms effectively protect end-to-end data transmission within homogeneous networks; however, they are insufficient for the demands of cloud-based, data-driven services operating across heterogeneous environments.

The integration of cloud, network, and end devices introduces new security challenges including data confidentiality breaches, integrity violations, unauthorized access, and trust management failures. Heterogeneous network environments—spanning 5G, IoT, satellite, and edge networks—create barriers to achieving seamless secure communication. Existing security frameworks focus on isolated components and lack coordinated protection across layers. The dynamic nature of modern applications requires adaptive, real-time security mechanisms. Furthermore, the growing use of AI-driven services increases risks of data manipulation and model exploitation. There is therefore a critical need for an integrated, collaborative security architecture that ensures end-to-end protection across cloud services, network connections, and end-device systems.

Proposed Methodology and System Design

The proposed Cloud-Network-End Collaborative Security Architecture establishes a unified security framework that integrates protection across three hierarchical layers: end devices, network infrastructure, and cloud services. The system ensures data security throughout the entire lifecycle—from collection at end devices, through secure transmission across heterogeneous networks, to encrypted storage and controlled processing in cloud environments.

At the end-device layer, data is authenticated, encrypted using AES-256, and organized into secure blocks before transmission. The network layer enforces secure routing, multi-factor authentication, and traffic integrity monitoring to prevent unauthorized access. At the cloud layer, encrypted data is stored and processed using role-based access control (RBAC), cryptographic key management, and integrity verification via SHA-256 hashing. Figure 1 illustrates the overall system architecture.

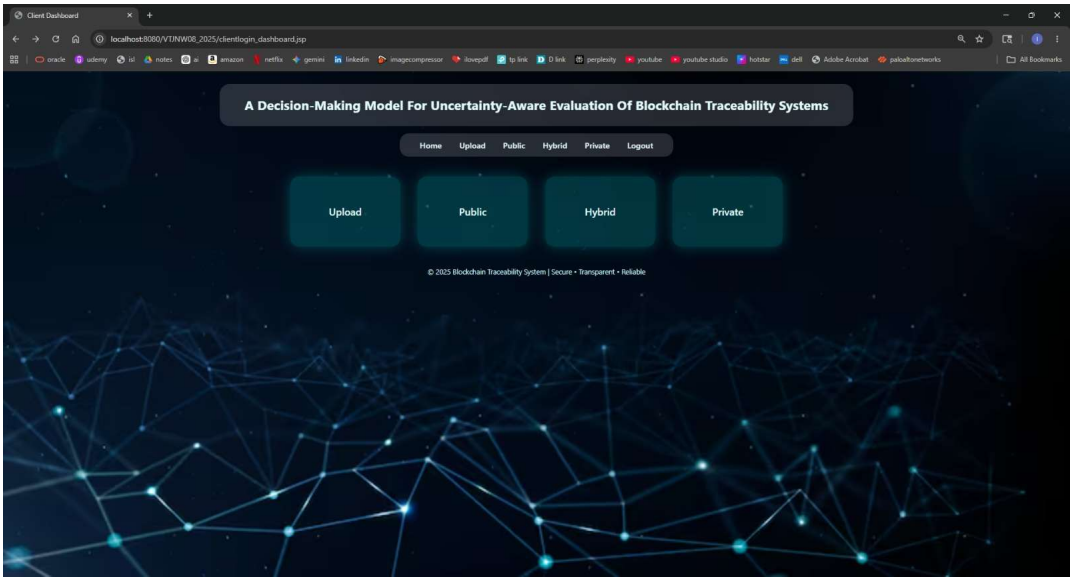

Fig. 3: Client Dashboard – Upload, Public, Hybrid, and Private Data Modules

https://doi.org/10.63665/IJMEC.1104s.41
ISSN: 2456-4265
IJMEC 2026

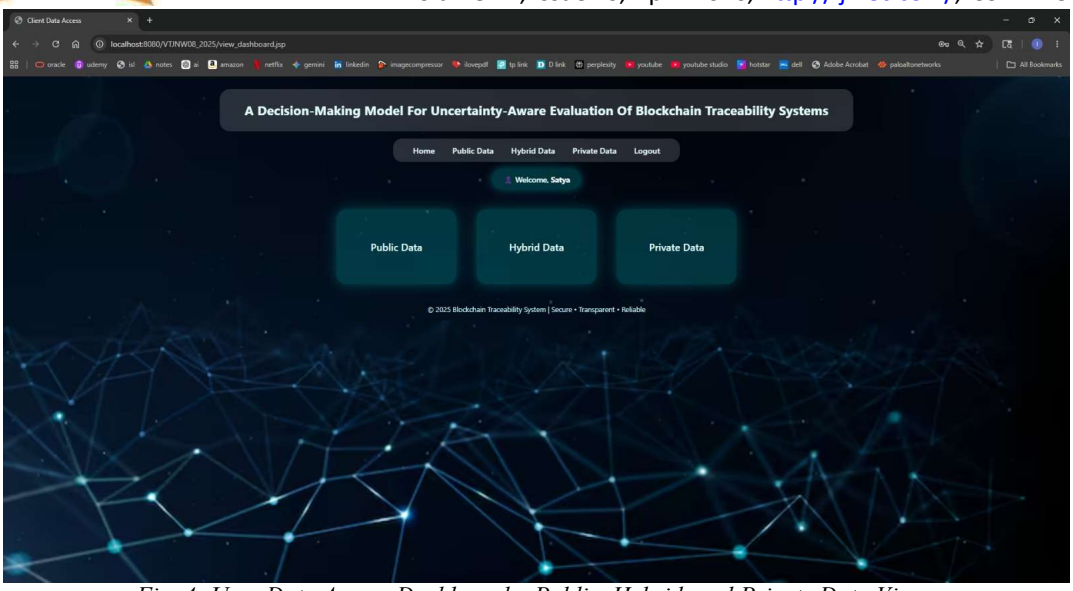

Fig. 4: User Data Access Dashboard – Public, Hybrid, and Private Data Views

The framework employs a layered workflow: (1) users register and authenticate through SHA-256 hashed credentials; (2) data files are uploaded, divided into encrypted blocks, and transmitted to the cloud server; (3) the cloud server stores encrypted data and manages access permissions; (4) authorized users search and retrieve data through verified key-based decryption; and (5) administrators monitor all operations through a JSP-based dashboard with full audit logging.

Table 1: Comparison of Traditional vs. Proposed Security Frameworks

Security Attribute	Traditional Approach	Proposed Cloud-Network-End Framework
Confidentiality	End-to-end channel encryption only	AES-256 encryption across all layers
Integrity	Limited to transmission checksums	SHA-256 hashing for end-to-end verification
Authentication	Centralized identity management	Role-based multi-layer authentication
Scalability	Single-domain, limited heterogeneity	Distributed cloud with dynamic allocation
Cross-network Security	Incompatible between heterogeneous networks	Unified cloud-network-end coordination

System Modules

The proposed system comprises six integrated modules, each addressing a specific security function within the cloud-network-end architecture. Table 2 provides an overview of the modules.

Table 2: System Module Summary

Module	Description
Cloud-Network-End Architecture	Core security framework integrating cloud, network, and end devices for coordinated protection.
AES-256 Encryption	Symmetric encryption ensuring data confidentiality during transmission and storage.

https://doi.org/10.63665/IJMEC.1104s.41
ISSN: 2456-4265
IJMEC 2026

SHA-256 Hashing	Cryptographic hash generation for data integrity verification across all transactions.
Cloud Server	Centralized processing unit managing storage, authentication, and secure data collaboration.
JSP Dashboard	Web-based interface for monitoring encrypted data, status updates, and user management.
MySQL Database	Supportive data layer maintaining user credentials, metadata, and system logs.

Cloud-Network-End Collaborative Security Architecture: This core module coordinates secure data collection, transmission, and processing across heterogeneous environments. It integrates encryption, secure communication protocols, authentication mechanisms, and distributed computing to provide unified end-to-end protection. Data from end devices is encrypted using symmetric and asymmetric cryptographic techniques before transmission through 5G, Wi-Fi, and IoT gateways.

AES-256 Encryption Module: When a user uploads a file, AES-256 encryption converts the original data into ciphertext using a unique secret key. This key is securely stored and later verified when authorized users request file access. The algorithm provides high-speed, strong symmetric encryption suitable for protecting large volumes of sensitive data in distributed environments.

SHA-256 Integrity Module: A unique 256-bit hash value is generated for every user identity, file, and data block. This hash acts as a digital fingerprint; even minor data modifications alter the hash completely, immediately alerting the system to potential tampering. SHA-256 ensures end-to-end data verification and immutability throughout the system.

Cloud Server: The cloud server functions as the central processing and control unit, managing data storage, authentication, access control, and inter-component communication. It employs role-based access control and verified key management to ensure only authorized entities can access stored data. Load balancing and virtualization techniques maintain high availability and scalability.

JSP Dashboard: The web-based dashboard provides users, administrators, and data owners with a secure interface for monitoring uploaded encrypted data, managing file access requests, and viewing system status. Role-based views ensure that each stakeholder accesses only authorized information.

MySQL Database: The database layer maintains user credentials, device metadata, system logs, and other non-critical auxiliary information required for system operation. This hybrid storage approach—combining encrypted cloud storage with a structured relational database—optimizes both system performance and data security.

Implementation

The system was implemented using Java EE technologies including JSP and Servlets for the frontend and backend components, with Apache Tomcat 9.0 as the deployment server. MySQL 5.5 serves as the relational database for user management and metadata storage. The development environment utilized Eclipse IDE on Windows 10/11.

The implementation workflow begins with user registration, where SHA-256 hashing secures credentials before storage. Upon login, the system validates credentials and grants role-based access. For data upload, files are divided into blocks, each encrypted with AES-256 using a unique secret key, and transmitted to the cloud server. The server stores the encrypted blocks and records their SHA-256 hash values in the database.

Authorized users submit access requests through the JSP dashboard. The system verifies the request, validates the encryption key, and if approved, allows decryption and download of the original file. Administrators monitor all transactions, approve user registrations, and manage access control policies through a dedicated administration panel. The complete data flow from registration through secure file access is governed by predefined security policies enforced at each system layer.

Figure 2: System Data Flow – Client to Cloud Secure Data Sharing

Hardware requirements include an Intel Core i3 or higher processor, minimum 4 GB DDR4 RAM, 100 GB storage, and a standard display. Software dependencies include Java EE (JSP, Servlets, Maven), MySQL 5.5+, Apache Tomcat 9.0, and the Eclipse IDE or IntelliJ IDEA development environment. The system is compatible with Google Chrome and Mozilla Firefox browsers.

Results and Discussion

The proposed Cloud-Network-End Collaborative Security Architecture was evaluated through

https://doi.org/10.63665/IJMEC.1104s.41
ISSN: 2456-4265
IJMEC 2026

comprehensive functional and non-functional testing, including unit testing, integration testing, system testing, performance testing, and acceptance testing. The evaluation confirmed that the system satisfies all defined security and operational requirements.

Functional testing verified that AES-256 encryption correctly secures uploaded files, with only authorized users possessing valid secret keys able to decrypt and access data. SHA-256 integrity verification successfully detected all simulated tampering attempts during data transmission and storage. Role-based access control accurately enforced user permissions across all dashboard functions, preventing unauthorized access to restricted data. Performance evaluation demonstrated that the system efficiently handles concurrent user operations with acceptable latency in encryption, decryption, and hash verification operations. The cloud server maintained high availability through load balancing, and the MySQL database provided reliable metadata management with fast query response times. The modular architecture supports independent scaling of each component to accommodate increased workloads. Security evaluation confirmed that the integrated use of AES-256 encryption and SHA-256 hashing provides robust protection against unauthorized data access, data tampering, and integrity attacks. The role-based access control mechanism effectively prevents privilege escalation. The system architecture eliminates single points of failure through distributed cloud infrastructure, ensuring continuous operation even during partial component failures. Compared to traditional end-to-end security approaches, the proposed collaborative framework provides substantially improved coverage across all three security layers—end devices, network infrastructure, and cloud services.

Applications

The proposed Cloud-Network-End Collaborative Security Architecture is applicable across a wide range of domains where secure data sharing across distributed systems is essential. In smart healthcare, the framework enables secure management of sensitive medical records, ensuring patient privacy and controlled data access for authorized healthcare providers. In smart cities, the architecture supports secure integration of data from diverse IoT devices, enabling reliable urban services while protecting citizen data.For autonomous transportation systems, the framework ensures secure real-time data exchange between vehicles, infrastructure, and cloud platforms, supporting safe and reliable autonomous operations. In industrial automation and IoT environments, the architecture provides end-to-end security for operational data, protecting against cyberattacks that could disrupt critical infrastructure. The framework also supports e-governance applications by enabling secure digital service delivery across heterogeneous government networks.

Conclusion

This paper presented a Cloud-Network-End Collaborative Security Architecture designed to address the security challenges arising from the convergence of cloud computing, wireless communication, and IoT technologies. The proposed framework establishes coordinated protection across end-device, network, and cloud service layers, overcoming the limitations of traditional end-to-end security mechanisms that fail in modern heterogeneous and distributed environments.

The architecture integrates AES-256 encryption for data confidentiality, SHA-256 hashing for integrity verification, role-based access control for authorization, and a centralized cloud server for scalable data management. Functional and performance evaluations confirmed that the system effectively ensures data security across all architectural layers, supports concurrent multi-user operations, and maintains high availability through distributed infrastructure.

The proposed framework contributes a practical and scalable solution for securing next-generation information systems, with demonstrated applicability in healthcare, smart cities, autonomous transportation, and industrial IoT domains. The work establishes a strong foundation for trustworthy, intelligent, and secure cloud-network-end ecosystems capable of supporting the demands of future wireless communication environments.

Future Scope

Future enhancements to the proposed framework will focus on integrating advanced artificial intelligence and machine learning techniques for intelligent threat detection, anomaly identification, and adaptive security policy management. AI-driven security mechanisms will enable proactive identification of potential attacks and dynamic adjustment of protection strategies in real time. Deeper integration with edge computing will allow sensitive data processing closer to its source, reducing latency for time-critical applications such as autonomous vehicles and industrial automation. The adoption of zero-trust security models can further strengthen protection through continuous verification of all users, devices, and access requests regardless of network location. Blockchain-assisted trust management can enable decentralized identity verification and tamper-proof

https://doi.org/10.63665/IJMEC.1104s.41
ISSN: 2456-4265
IJMEC 2026

audit trails.Extensions to support 6G networks, satellite communications, and large-scale IoT interoperability are also planned. Privacy-preserving techniques including federated learning and secure multi-party computation will be incorporated to protect sensitive data while enabling collaborative analytics across distributed systems.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," Comput. Netw., vol. 38, no. 4, pp. 393–422, 2002.

[2] I. F. Akyildiz and X. Wang, "A survey on wireless mesh networks," IEEE Commun. Mag., vol. 43, no. 9, pp. S23–S30, 2005.

[3] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, "Wireless body area networks: A survey," IEEE Commun. Surv. Tutorials, vol. 16, no. 3, pp. 1658–1686, 2014.

[4] J. Liu, Y. Shi, Z. M. Fadlullah, and N. Kato, "Space-air-ground integrated network: A survey," IEEE Commun. Surv. Tutorials, vol. 20, no. 4, pp. 2714–2741, 2018.

[5] C. Zhang, P. Patras, and H. Haddadi, "Deep learning in mobile and wireless networking: A survey," IEEE Commun. Surv. Tutorials, vol. 21, no. 3, pp. 2224–2287, 2019.

[6] Z. Shen, J. Jin, C. Tan, A. Tagami, S. Wang, Q. Li, Q. Zheng, and J. Yuan, "A survey of next-generation computing technologies in space-air-ground integrated networks," ACM Comput. Surv., vol. 56, no. 1, p. 23, 2023.

[7] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," Proc. IEEE, vol. 104, no. 9, pp. 1727–1765, 2016.

[8] C. E. Shannon, "Communication theory of secrecy systems," Bell Syst. Tech. J., vol. 28, no. 4, pp. 656–715, 1949.

[9] R. Canetti, "Universally composable security: A new paradigm for cryptographic protocols," in Proc. 42nd IEEE Symp. Foundations of Computer Science, 2001, pp. 136–145.

[10] D. Lu, M. Shi, X. Ma, X. Liu, R. Guo, T. Zheng, Y. Shen, X. Dong, and J. Ma, "Smaug: A TEE-assisted secured SQLite for embedded systems," IEEE Trans. Dependable Secure Comput., vol. 20, no. 5, pp. 3617–3635, 2023.

[11] X. Wang, J. Ma, X. Liu, Y. Miao, Y. Liu, and R. H. Deng, "Forward/backward and content private DSSE for spatial keyword queries," IEEE Trans. Dependable Secure Comput., vol. 20, no. 4, pp. 3358–3370, 2023.

[12] T. Yang, J. Ma, Y. Miao, Y. Wang, X. Liu, K. K. R. Choo, and B. Xiao, "MU-TEIR: Traceable encrypted image retrieval in the multi-user setting," IEEE Trans. Serv. Comput., vol. 16, no. 2, pp. 1282–1295, 2023.

[13] X. Li, Q. Tong, J. Zhao, Y. Miao, S. Ma, J. Weng, J. Ma, and K. K. R. Choo, "VRFMS: Verifiable ranked fuzzy multi-keyword search over encrypted data," IEEE Trans. Serv. Comput., vol. 16, no. 1, pp. 698–710, 2023.

[14] V. K. Yadav, N. Andola, S. Verma, and S. Venkatesan, "A survey of oblivious transfer protocol," ACM Comput. Surv., vol. 54, no. 10, pp. 1–37, 2022.

[15] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proc. IEEE Symp. Security and Privacy, 2007, pp. 321–334.

[16] Q. Jiang, J. Ni, J. Ma, L. Yang, and X. Shen, "Integrated authentication and key agreement framework for vehicular cloud computing," IEEE Netw., vol. 32, no. 3, pp. 28–35, 2018.

[17] M. Sabt, M. Achemlal, and A. Bouabdallah, "Trusted Execution Environment: What it is, and what it is not," in Proc. IEEE Trustcom/BigDataSE/ISPA, 2015, pp. 57–64.

[18] D. He, N. Kumar, M. Khan, and J. H. Lee, "Anonymous two-factor authentication for consumer roaming service in global mobility networks," IEEE Trans. Consumer Electron., vol. 59, no. 4, pp. 811–817, 2013.

[19] S. Kamara, C. Papamanthou, and T. Roeder, "Dynamic searchable symmetric encryption," in Proc. ACM Conf. Computer and Communications Security, 2012, pp. 965–976.

[20] C. Gentry, "Fully homomorphic encryption using ideal lattices," in Proc. 41st Annual ACM Symp. Theory of Computing, 2009, pp. 169–178.

https://doi.org/10.63665/IJMEC.1104s.41
ISSN: 2456-4265
IJMEC 2026