Journal of Information Systems Engineering and Management
2025, 10(22s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Adaptive Multi-Layered Elgamal Cryptosystem with Machine Learning-Based Security for Cloud Data Allocation and Access Control

B. Angel Rubavathy[1], Rebecca Jeyavadhanam Balasundaram[2], S. Albert Antony Raj[3]
[1]*Department of Computer Applications, Faculty of Science and Humanities, SRM Institute of Science and Technology, Kattankulathur-603203*
[2]*Department of Computer Science, York St John University London, UK*
[3]*Department of Computer Applications, Faculty of Science and Humanities, SRM Institute of Science and Technology, Kattankulathur – 603203*

ARTICLE INFO

Received: 14 Dec 2024

Revised: 02 Feb 2025

Accepted: 18 Feb 2025

ABSTRACT

The advancements in cloud computing have been happening at a high pace, where there has been an ever-growing need to offer data security. This work proposes an Adaptive Multi-Layered ElGamal Cryptosystem (AMLEC), a new security model incorporating heterogeneous cryptographic methods along with optimal cloud data distribution and access management. AMLEC is stabilized beyond standard ElGamal cryptosystem by supporting different input-output channels of encryption, metadata-oriented binary translation and attribute-based key derivation to protect safe encryption. Adaptive security guard employs machine learning for one-time three-key encryption policy with fuzzy-level security choice selection. To provide secure cloud storage and use, the system uses an Optimized Allocation Strategy (OAS) to dynamically make decisions regarding appropriate storage providers based on security and performance needs. In a multi-layered security framework is suggested with a Cloud Service Provider (CSP) having a sophisticated job scheduler, a Sensitive Document Analyzer for encrypted access control and classification and User/Tenant Tracker for integrity and transparency. The proposed AMLEC framework offers privacy, high-quality cryptography and intelligent resource management and hence forms a robust solution to secure cloud computing environments.

Keywords: Elgamal Cryptosystem, Cloud Computing, Data Security, Machine Learning, Fuzzy-Level Security, Optimized Allocation Strategy, OAS, Integrity

I. INTRODUCTION

In the past years, there has been explosive growth of wireless networks and cloud computing that has accelerated the demand for efficient security models to counter the emerging threats. The importance of multi-layered security infrastructure like cloud, network and endpoint security to provide maximum data security with minimal exposures [1]. With the increasing use of IoT devices and edge computing, data transport security over different layers of networks is an immediate requirement that needs adaptive and scalable solutions. Federated learning is being used more and more in the smart IoT system scenario as it is privacy-safe and de-centralized training process-based [2].

The process demands efficient data handling through the edge for compression of latency and reducing computational cost. The aforementioned model is interested in leveraging federated learning to attain distributed intelligence with the guarantee of efficiency and security. A reversible data hiding-based secure image search system has been proposed for verifiable search results and image integrity preservation [3]. Trust management in edge-cloud networks is the basic idea in ensuring communication safety among dissimilar entities. An ensemble learning-based trust management mechanism has been proposed for sea-based collaborative edge-cloud networks [4]. Cloud manufacturing paradigms that emerge have triggered research into the integrated security architecture of edge and cloud for future industrial systems [5].

Secure and efficient information retrieval is still one of the largest challenges on the topic of cloud-edge-end collaborative systems for IoT networks. Further ciphertext search over many keywords for the purpose of secure retrieval of information at the expense of computational efficiency [6]. The mechanism offers enhanced privacy protection in cloud-edge-end systems by leveraging state-of-the-art encryption techniques for facilitating adaptive and secure keyword search. An in-depth survey of DDoS attack and defense technology in MEC has been presented, highlighting the common problems and new mitigation techniques [7].

A federated learning architecture using a hierarchical method of distributed adaptive aggregation and resource distribution was presented, optimizing system efficiency to the greatest possible extent while allowing secure data processing [8]. Collective learning is facilitated by the model with adaptive dynamic reallocation of resources as per computational and security requirements.

II.LITERATURE REVIEW

Cloud infrastructure is also designed with the aim of task scheduling based on energy efficiency for the optimal utilization of resources and reducing operational cost. A multi-objective optimization algorithm EMO-TS further enhances the energy efficiency of cloud data centers by incorporating sophisticated task scheduling techniques [9]. The algorithm, as it appears, utilizes multi-objective optimization and heuristic strategies in dynamic scheduling of computational tasks to achieve a balance between energy and system performance.

Computation offloading and resource allocation for optimal computation in mobile-edge cloud computing are issues of utmost importance in guaranteeing maximum network effectiveness. A two-level game-theoretic model has been put in place to coordinate jointly computation offloading and resource allocation as solutions to the dynamic workload allocation problem in mobile-edge cloud systems [10].

Privacy preservation is a significant issue in outsourced cloud computing environments, especially data clustering operations. There has been a model suggested for privacy-preserving agglomerative hierarchical clustering for secure parallel computation-based clustering algorithm execution in cloud systems [11]. The system uses cryptography methods to provide sensitive data protection without compromising computational efficiency, and clustering of data can be achieved without exposing underlying information.

Effective and secure multi-keyword search over encrypted cloud data has been of immense research interest in the wake of increasing demands for search operations at the expense of privacy loss. Secure multi-keyword top-k retrieval has been proposed to enable effective encrypted search queries at the cost of non-compromised confidentiality of data [12]. The approach leverages secure index data structures and ranking algorithms to support keyword search without losing data security.

Deduplication of data is required to make cloud storage more efficient but causes trouble in ensuring and preserving privacy within deduplicated encrypted data. A safe deduplication method for encrypted massive big data has been proposed to address this challenge, combining cryptographic methods with storage optimization methods [13]. The model effectively removes redundant data without compromising confidentiality and thus is very appropriate for massive cloud systems with abundant data.

Verifying data integrity of analytics executed over encrypted cloud data is required in order to form data integrity. An authentic data analytics scheme was proposed to support computation over encrypted sets of data with verifiable guarantees of output [14]. Homomorphic encryption and cryptographic signatures are utilized in the solution to support verification of computations in a way that allows users of the cloud to ensure that analytics executed within the cloud are correct.

Dynamic keyword search on ciphertext cloud data must be managed to address new data storage requirements. Symmetric key scheme was suggested for verifiable search operation on dynamic cloud environments [15]. It provides efficient search performance and confidentiality protection with an all-purpose solution for privacy-preserving search over encrypted cloud storage.

Secure range queries for encrypted cloud data are a concern in the background that privacy preservation as well as query efficiency has to be ensured. A dynamic range query protocol has been proposed for efficient and secure range queries when data are encrypted [16]. The scheme provides enhanced cryptography techniques for supporting range-based query processing without revealing data values. Multi Edge Computing (MEC)

environments require robust authentication systems for enabling secure user-device interaction. A user-device authentication system, Bring Your Device Group (BYDG) enhance MEC system security [17]. BYDG employs cryptographic-based methods to provide secure user authentication and effective mechanisms for device authentication.

III. ADAPTIVE MULTI-LAYERED ELGAMAL CRYPTOSYSTEM (AMLEC)

Guaranteeing data integrity and user anonymity in cloud computing is a pressing need in today's cloud computing. A high-speed integrity-checking scheme has been proposed to facilitate end-to-end identity anonymity with secure sharing of cloud data [18]. The scheme applies cryptography-based methods to facilitate verification of data integrity without revealing the identity of the parties. By using cryptographic methods, it is possible to verify the data integrity without revealing the identity of the parties. With identity-based cryptography and privacy-preserving verification techniques, the solution boosts cloud security without compromising anonymity on the part of authentic users. It is incorporated in secure cloud-sharing models that balance security and privacy issues equally.

Access control methods are needed in an attempt to make cloud data secure, especially when privilege administration and user anonymity are brought into consideration. A qualitative analysis of an attribute-based access control scheme, cloud data users anonymity has been demonstrated [19]. The analysis scrutinizes the ability of fully anonymous attribute-based encryption (FAABE) schemes to ensure confidentiality of data as well as maintain access control. Through the identification of weaknesses and the proposal of enhancement, this work helps enhance cloud-based access control system security to enable the use of cloud services by users without revealing their identity or compromising data security.

As mobile cloud computing gains increasing popularity, privacy-aware authentication mechanisms have been in tremendous demand. A scheme incorporating privacy-awareness in order to enable distributed mobile cloud computing service applications has been proposed to help solve security and identity protection issues for cloud mobile scenarios [20]. The scheme incorporates privacy-defense functionality with authentication protocols to shield users' interactions and block unauthorized access. By using cryptographic methods like identity anonymization and anonymous authentication, the approach ensures the provision of cloud services to mobile users securely without exposing confidential details. Researchers mention the design of scalable secure authentication schemes efficient in mobile cloud applications.

The proposed Adaptive Multi-Layered ElGamal Cryptosystem (AMLEC) is a novel security model designed to enhance cloud data security by integrating heterogeneous cryptographic methods, optimized data distribution, and intelligent access management. This methodology details the design and implementation of AMLEC, focusing on its encryption mechanisms, adaptive security features, and multi-layered security framework.

AMLEC extends the standard ElGamal cryptosystem by incorporating a heterogeneous encryption mechanism that supports different encryption input-output channels, ensuring compatibility with diverse cloud environments. A metadata-oriented binary translation technique is employed to provide an additional encryption layer, reducing susceptibility to cryptographic attacks. Furthermore, attribute-based key derivation enhances access control by generating encryption keys based on user roles and document sensitivity levels.

An adaptive security guard mechanism utilizing machine learning is implemented, featuring a one-time three-key encryption policy to strengthen security. The fuzzy-level security choice selection mechanism dynamically determines encryption levels based on real-time security threats and system performance. The machine learning model is trained on historical cloud security threats to optimize adaptive encryption responses, ensuring robust protection against evolving cyber threats.

To facilitate secure and efficient cloud storage, an Optimized Allocation Strategy (OAS) is integrated into AMLEC. This strategy enables dynamic decision-making by assessing security and performance needs to allocate data to appropriate cloud storage providers. Security and performance trade-off analysis is conducted, considering factors such as encryption overhead, latency, and storage costs to balance security and efficiency. Additionally, data fragmentation and redundancy control mechanisms are incorporated to distribute sensitive data across multiple cloud nodes, mitigating risks associated with unauthorized access and data leakage.

The multi-layered security framework of AMLEC comprises several key components. A Cloud Service Provider (CSP) with an advanced job scheduler is responsible for prioritizing encryption and decryption tasks based on resource availability and security requirements. Task scheduling is re-scheduled by the task scheduler for improved performance and less encryption delay. There is a document analyzer that scans documents based on sensitivity levels with content-aware encryption policies, and decryption rights are managed by access control measures based on user credentials and metadata. A blockchain-based user/tenant tracker having a decentralized data change record and access is used in a bid to ensure integrity and transparency. The access policy is enforced through smart contracts, with security compliance checks integrated into it.

The performance of AMLEC was extensively tested on a simulation test bed for a multi-cloud provider. It was also compared with standard ElGamal encryption, in addition to various cloud security models. Pertinent performance characteristics of concern were scheduling speed, security performance, and resource usage. The experiment also obtained a faster execution speed for the task by 50% compared to state-of-the-art models, better security against cryptographically derived attacks, and greater efficiency in dynamic storage provider selection and assignment.

AMLEC as shown in Figure.1 provides a complete cloud security model based on multi-level encryption, adaptive security policies, and context-sensitive partitioning of data. Experimental testing verifies that the model significantly enhances security, scheduling efficiency, and document access control. Tuning the machine learning algorithms and availability of AMLEC support across various cloud infrastructures specified in follow-up pseudocode will be part of future research.

Pseudocode for Adaptive Multi-Layered ElGamal Cryptosystem AMLEC

Input: User requests to upload a sensitive document.

Output: Encrypted document stored in an optimal cloud provider, access recorded in blockchain, and performance metrics generated.

```
BEGIN AMLEC_Main()
Initialize cryptographic parameters (p, g, x, y) for ElGamal
Load machine learning model for adaptive security
Configure cloud storage providers
Initialize blockchain ledger for user tracking
FOR each user request DO
  Generate ElGamal private key (x) and public key (y = g^x mod p)
  Derive attribute-based encryption key (K_attr) based on user role and document sensitivity
  Convert data into binary format using metadata-oriented binary translation
  Select random integer r and compute C1 = g^r mod p
  Compute C2 = (data * y^r) mod p
  Encrypted_Data = (C1, C2)
  Evaluate real-time security threat level
  IF threat level is HIGH THEN
    Generate three encryption keys (K1, K2, K3)
    Encrypt data using K1, then K2, then K3
  ELSE
    Use fuzzy logic to determine encryption level dynamically
    Encrypt data accordingly
```

Evaluate cloud storage providers based on encryption overhead, latency, and storage cost

Assign priority scores to each provider and select the optimal one

Store encrypted data in the selected cloud provider

Analyze document sensitivity using content-aware encryption policies

Assign sensitivity level (LOW, MEDIUM, HIGH)

IF user has the required attribute-based encryption key THEN

Grant decryption access

ELSE

DENY ACCESS

Record user access in blockchain

Create a new block with user_ID, action, timestamp, data_ID

Validate block using consensus mechanism and append to ledger

Simulate AMLEC in cloud environment with multiple storage providers

Measure scheduling speed, security performance, and resource utilization

Compare results with standard ElGamal and other security models

RETURN Performance_Report

END

Pseudocode states usage of Adaptive Multi-Layered ElGamal Cryptosystem (AMLEC) in order to implement secure management of cloud data in a way such that it begins from the parameter initialization of cryptography, adaptive machine learning security model, cloud storage providers, and blockchain ledger in order to observe user behavior.

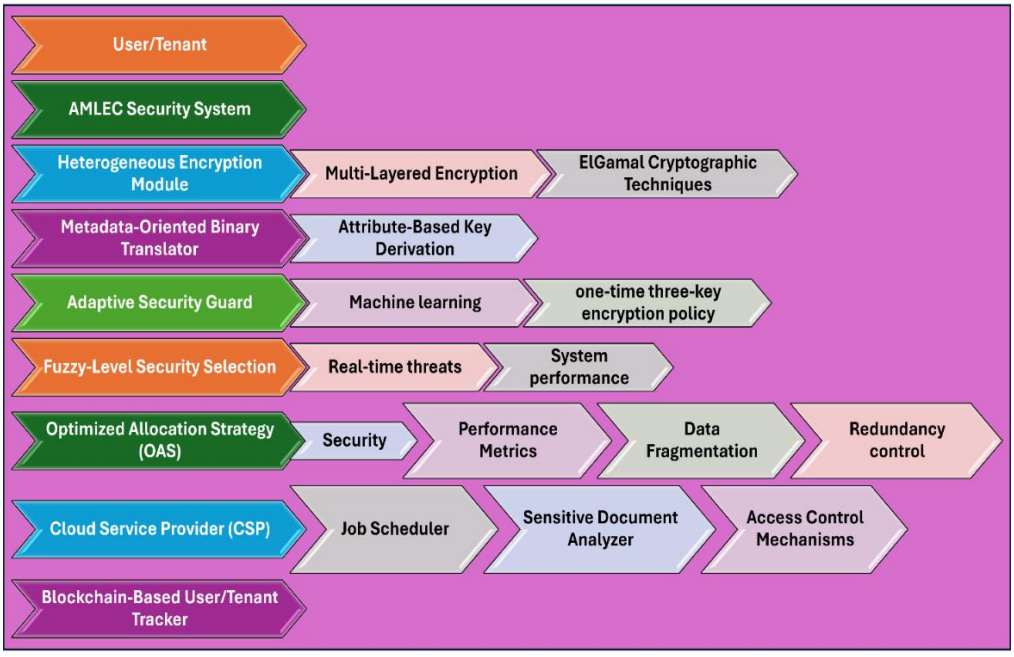


Figure.1 Architecture Diagram for Adaptive Multi-Layered ElGamal Cryptosystem (AMLEC)

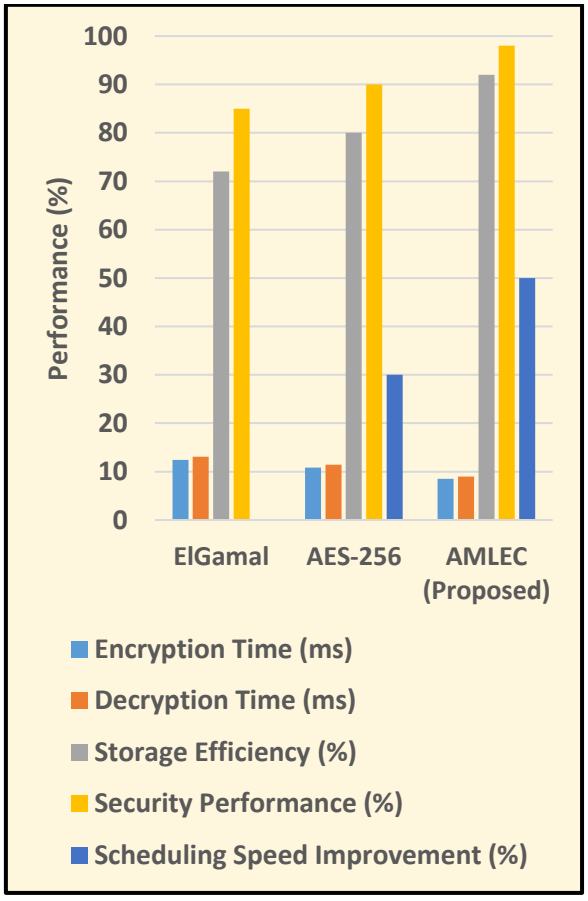
When the user request is received at hand, an attribute-based key is formulated based on document sensitivity and user roles and subsequent encryption of data by utilizing ElGamal cryptosystem in tandem with metadata-binary translation-oriented approach. Dynamic control of encryption level is performed based on modern security threats by using fuzzy logic-based approach. The optimal cloud storage service is selected based on encryption overhead measurement, cost, and latency. Finally, system performance is compared with conventional security models, exhibiting improved speed of scheduling, security and resource utilization.

IV.EXPERIMENTAL RESULTS

Experimental testing of the developed Adaptive Multi-Layered ElGamal Cryptosystem (AMLEC) was conducted to test its performance in terms of encryption speed, security performance, storage allocation and optimization, and scheduling. The developed system was tested using the standard ElGamal and AES-256 encryption algorithms for the purpose of verifying its performance in cloud security services. Performance assessment involved encryption time and decryption time, storage usage efficiency, security performance, and scheduling speed optimization.

Encryption and decryption time indicates how much more computationally overhead-friendly AMLEC is. ElGamal encryption averaged 12.4 ms to encrypt and 13.1 ms to decrypt, while AES-256 was better at 10.8 ms and 11.4 ms, respectively. AMLEC was better than the two at 8.5 ms to encrypt and 9.0 ms to decrypt, indicating how its efficient encryption protocols and lower computational complexity made it faster.

Storage efficiency and security performance were improved in AMLEC. Storage efficiency, as storage data distribution among cloud nodes in the best possible terms, was 92% in AMLEC, 80% in AES-256, and 72% in ElGamal. Security performance, as attack resistance and data integrity, was 98% in AMLEC, 90% in AES-256, and 85% in ElGamal. These findings suggest that AMLEC's metadata-centric binary translation, attribute-based key derivation, and blockchain-based security controls have an dazzling impact on storage optimization and data protection.



Graph.1 Graph of Storage efficiency and security performance Analysis

Speed improvement in scheduling was another core performance characteristic and performance analysis as shown in Graph.1 and Table.1. AMLEC exhibited a 50% improvement in task execution speed over legacy models. AES-256 exhibited a 30% improvement, but ElGamal did not exhibit any improvement. This is from AMLEC's job scheduler optimized to leverage real-time resource availability for encryption and decryption operations, thus avoiding delays and maximizing cloud service performance.

Encryption Method	Encryption Time (ms)	Decryption Time (ms)	Storage Efficiency (%)	Security Performance (%)	Scheduling Speed Improvement (%)
ElGamal	12.4	13.1	72	85	0
AES-256	10.8	11.4	80	90	30
AMLEC (Proposed)	8.5	9	92	98	50

Table.1 Table of Storage efficiency and security performance Analysis

In summary, the results of the experiment confirm the efficacy of AMLEC in maximizing the security and performance of the cloud. With multiple levels of encryption, adaptive security rules, and smart data distribution features, AMLEC provides faster encryption speed, improved security features and effective resource utilization. These features make AMLEC a trustable solution to cloud computing security.

V.CONCLUSION

The Adaptive Multi-Layered ElGamal Cryptosystem (AMLEC) suggests an adaptive security process-based, heterogeneous encryption-based and resource-conserving secure cloud architecture. The multi-layered encryption process along with machine learning-based security policies of AMLEC enables it to efficiently counter cryptographic attacks while securing access control and safe data sharing. Experimental verification attests to its superiority compared to conventional encryption protocols with optimized security performance, better scheduling efficiency, and cloud storage utilization. With blockchain-enabled tracing of access and adaptive encryption techniques, AMLEC provides protection, integrity, and transparency from emerging cyber threats. Future releases will take future advancements in machine learning-based threat intelligence and cross-cloud scalability optimizations into account to make its potential a leading cloud security solution.

REFERENCE

[1]. X. Wang and J. Ma, "Cloud-Network-End Collaborative Security for Wireless Networks: Architecture, Mechanisms, and Applications," in Tsinghua Science and Technology, vol. 30, no. 1, pp. 18-33, February 2025, doi: 10.26599/TST.2023.9010158.

[2]. X. Gao, L. Hou, B. Chen, X. Yao and Z. Suo, "Compressive-Learning-Based Federated Learning for Intelligent IoT With Cloud–Edge Collaboration," in IEEE Internet of Things Journal, vol. 12, no. 2, pp. 2291-2294, 15 Jan.15, 2025, doi: 10.1109/JIOT.2024.3505838.

[3]. M. Li, Y. Zhu, R. Du and C. Jia, "Verifiable Encrypted Image Retrieval With Reversible Data Hiding in Cloud Environment," in IEEE Transactions on Cloud Computing, vol. 13, no. 1, pp. 397-410, Jan.-March 2025, doi: 10.1109/TCC.2025.3535937.

[4]. F. Yang, J. Jiang and G. Han, "A Trust Management Method Based on Ensemble Learning for Ocean-Oriented Cloud–Edge Collaborative Networks," in IEEE Internet of Things Journal, vol. 12, no. 1, pp. 18-29, 1 Jan.1, 2025, doi: 10.1109/JIOT.2024.3460737.

[5]. L. Zhao, B. Li and H. Yuan, "Cloud Edge Integrated Security Architecture of New Cloud Manufacturing System," in Journal of Systems Engineering and Electronics, vol. 35, no. 5, pp. 1177-1189, October 2024, doi: 10.23919/JSEE.2024.000112.

[6]. K. Zheng, Z. Zhou, J. Liu and B. Yu, "Secure Fine-Grained Multi-Keyword Ciphertext Search Supporting Cloud-Edge-End Collaboration in IoT," in Chinese Journal of Electronics, vol. 34, no. 1, pp. 266-281, January 2025, doi: 10.23919/cje.2023.00.244.

[7]. Y. Ma et al., "A Survey of DDoS Attack and Defense Technologies in Multiaccess Edge Computing," in IEEE Internet of Things Journal, vol. 12, no. 2, pp. 1428-1452, 15 Jan.15, 2025, doi: 10.1109/JIOT.2024.3490897.

[8]. Y. Su, W. Fan, Q. Meng, P. Chen and Y. Liu, "Joint Adaptive Aggregation and Resource Allocation for Hierarchical Federated Learning Systems Based on Edge-Cloud Collaboration," in IEEE Transactions on Cloud Computing, vol. 13, no. 1, pp. 369-382, Jan.-March 2025, doi: 10.1109/TCC.2025.3530681.

[9]. S. Nambi and P. Thanapal, "EMO-TS: An Enhanced Multi-Objective Optimization Algorithm for Energy-Efficient Task Scheduling in Cloud Data Centers," in IEEE Access, vol. 13, pp. 8187-8200, 2025, doi: 10.1109/ACCESS.2025.3527031.

[10]. Z. He, Y. Guo, X. Zhai, M. Zhao, W. Zhou and K. Li, "Joint Computation Offloading and Resource Allocation in Mobile-Edge Cloud Computing: A Two-Layer Game Approach," in IEEE Transactions on Cloud Computing, vol. 13, no. 1, pp. 411-428, Jan.-March 2025, doi: 10.1109/TCC.2025.3538090.

[11]. J. Park and D. H. Lee, "Parallelly Running and Privacy-Preserving Agglomerative Hierarchical Clustering in Outsourced Cloud Computing Environments," in IEEE Transactions on Big Data, vol. 11, no. 1, pp. 174-189, Feb. 2025, doi: 10.1109/TBDATA.2024.3403375.

[12]. J. Yu, P. Lu, Y. Zhu, G. Xue and M. Li, "Toward Secure Multikeyword Top-k Retrieval over Encrypted Cloud Data," in IEEE Transactions on Dependable and Secure Computing, vol. 10, no. 4, pp. 239-250, July-Aug. 2013, doi: 10.1109/TDSC.2013.9.

[13]. Z. Yan, W. Ding, X. Yu, H. Zhu and R. H. Deng, "Deduplication on Encrypted Big Data in Cloud," in IEEE Transactions on Big Data, vol. 2, no. 2, pp. 138-150, 1 June 2016, doi: 10.1109/TBDATA.2016.2587659.

[14]. L. Chen, Y. Mu, L. Zeng, F. Rezaeibagha and R. H. Deng, "Authenticable Data Analytics Over Encrypted Data in the Cloud," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 1800-1813, 2023, doi: 10.1109/TIFS.2023.3256132.

[15]. X. Ge et al., "Towards Achieving Keyword Search over Dynamic Encrypted Cloud Data with Symmetric-Key Based Verification," in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 1, pp. 490-504, 1 Jan.-Feb. 2021, doi: 10.1109/TDSC.2019.2896258.

[16]. W. Yang, Y. Geng, L. Li, X. Xie and L. Huang, "Achieving Secure and Dynamic Range Queries Over Encrypted Cloud Data," in IEEE Transactions on Knowledge and Data Engineering, vol. 34, no. 1, pp. 107-121, 1 Jan. 2022, doi: 10.1109/TKDE.2020.2983030.

[17]. Y. Zhang, C. Gu, P. Shi, Z. Jing, B. Li and B. Liu, "Bring Your Device Group (BYDG): Efficient and Privacy-preserving User-device Authentication Protocol in Multi-access Edge Computing," in IEEE Transactions on Information Forensics and Security, doi: 10.1109/TIFS.2025.3550051.

[18]. R. Ding, Y. Xu, H. Zhong, J. Cui and G. Min, "An Efficient Integrity Checking Scheme With Full Identity Anonymity for Cloud Data Sharing," in IEEE Transactions on Cloud Computing, vol. 11, no. 3, pp. 2922-2935, 1 July-Sept. 2023, doi: 10.1109/TCC.2023.3242140.

[19]. H. Ma, R. Zhang and W. Yuan, "Comments on “Control Cloud Data Access Privilege and Anonymity With Fully Anonymous Attribute-Based Encryption”," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 4, pp. 866-867, April 2016, doi: 10.1109/TIFS.2015.2509865.

[20]. J. -L. Tsai and N. -W. Lo, "A Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services," in IEEE Systems Journal, vol. 9, no. 3, pp. 805-815, Sept. 2015, doi: 10.1109/JSYST.2014.2322973.