JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Review of Innovations in Cloud Security: Identity-Based Encryption with Secure Channel Techniques

Gaurav Pandey
Research Scholar

Mrs. Jyoti Shekhawat
Assistant Professor

Vivekananda Global University
Jaipur, India

Submitted in partial fulfillment of the requirement for the degree of
Master of Technology (M.Tech) in Cyber Security.

Enrollment Number- 21TEC3CS004

Abstract

Cloud computing offers convenient, on-demand access to a shared pool of resources, including information, applications, and hardware, enabling businesses and individuals to efficiently store and manage data in third-party data centers. As the reliance on cloud computing grows, so do concerns about data security and integrity. This review paper examines the evolution and application of fully homomorphic encryption (FHE) within cloud environments, highlighting its capability to perform computations on encrypted data without decryption, thereby maintaining security. Furthermore, the paper explores various identity-based and attribute-based encryption techniques, focusing on their role in enhancing cloud security. The review also delves into the integration of secure channels in encryption frameworks, analyzing their effectiveness in mitigating security risks. By synthesizing existing research, this paper provides a comprehensive overview of current advancements and identifies potential areas for further innovation in cloud security.

Keywords: Diffie-Hellman, Fully Homomorphic Encryption, Cloud, Identity Based Encryption

Chapter 1 Introduction

1.1 Cloud Computing Overview

Cloud computing is a model designed to ensure convenient, on-demand network access to a shared pool of configurable computing resources, which can be rapidly provisioned and released with minimal management effort. A cloud computing framework provides multiple computing resources in form of services over the web. Storage is considered to be a major amenity offered by the cloud (for example, Simple Storage Services—Amazon S3), allowing customers to save vast volume of data on a remote cloud without having to bother with perplexing handling of storage hardware. It is built on data centres and offers services through three main models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). These services range from storage solutions like Amazon S3 to complete software solutions accessible directly from a browser, all while allowing users to pay only for what they use.

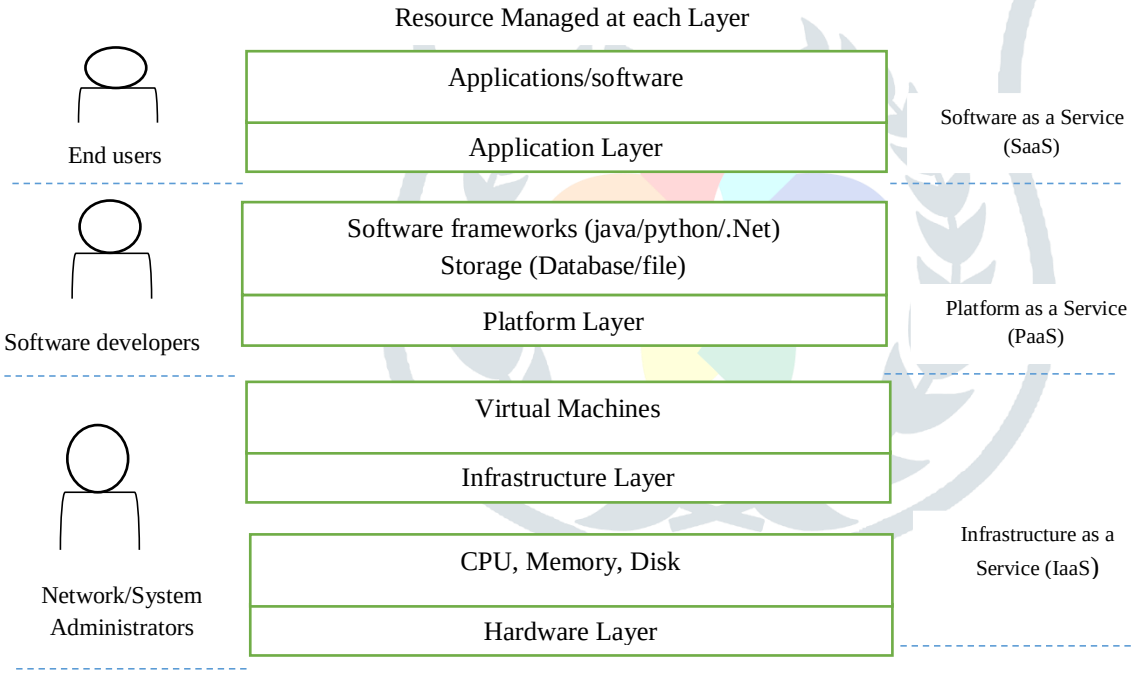

Figure 1: Hierarchical Outlook of Cloud Computing

1.1.1 Cloud Deployment Models

The NIST has outlined the four cloud deployment models of public, private, community, and hybrid clouds. These models are capable of operating on all service model types and offer information on the use and consumption of technology as illustrated in figure 2.

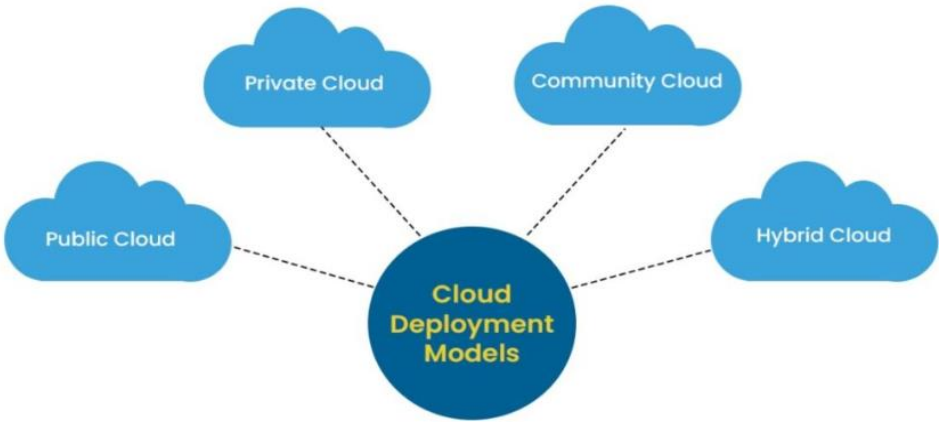

Figure 2: Cloud Computing Deployment Models

The definition of the models is:

a. Public Cloud: Any subscriber with an online connection and access to the cloud can readily access this model.
b. Private cloud: This type of cloud is set up for a single group or organisation, and it helps limit access to just that group.
c. Hybrid cloud: This model incorporates two or more clouds, each of which is maintained as a separate entity. However, standardised or proprietary technology has linked them, allowing for easier access to data and application mobility.
d. Community cloud: This concept supports a specific community capable of expressing problems and is shared by a number of organizations. It may be found on or off premises and has been managed by organizations or a third party.

1.2 Security in Cloud Computing

Cloud security is critical as data is often processed and stored by third-party cloud service providers, raising concerns about data integrity and confidentiality.

- Data Storage Security: Involves storing data across multiple locations to enhance security and ensure data availability even if one server fails.
- Secure Data Sharing: Ensures that data sharing in cloud environments is secure and only accessible to authorized users.

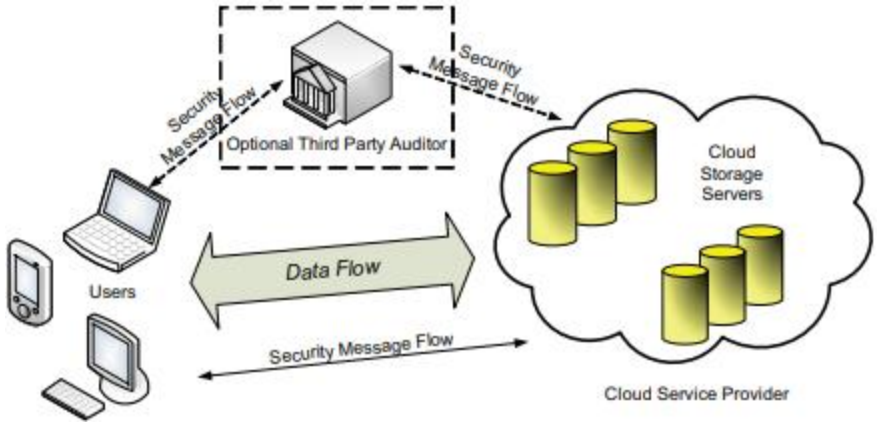

Figure 2: Cloud data storage architecture

Figure 2 represents a representative network framework for cloud data storage. Three dissimilar network entities are discussed as:

- User: These entities are present as individual consumers and organizations which aim to store the data in the cloud and depend on the cloud to compute the data.
- Cloud Service Provider (CSP): It assists in owning and operating the live CC (Cloud Computing) systems as significant resources and expertise are comprised in it to generate and manage the distributed cloud storage servers.
- Third Party Auditor (TPA): An optional TPA having proficiency and abilities which are not available for users, is reliable source for assessing and discovering the risk of cloud storage services in accordance with the users upon request.

1.3 Encryption Techniques in Cloud Security

Encryption techniques play a crucial role in ensuring information security and addressing data leakage and privacy concerns. Encryption can be applied at different levels, ranging from individual data elements to aggregated data items. However, it is essential to consider that higher granularity of encryption can also increase the risk of information leakage. Encrypting a single attribute, for example, may inadvertently expose the frequency of that attribute in the database records. On the other hand, encrypting an entire document or collection as a single unit can reduce such information leakage. There are various encryption methods and cryptosystems used for cloud-hosted databases. Some of these techniques include:

- Symmetric and Asymmetric Encryption: Utilized for securing data stored in the cloud. While symmetric key encryption uses a single key for both encryption and decryption, asymmetric encryption uses a public key for encryption and a private key for decryption.

- Advanced Encryption Standard (AES): One of the most secure encryption methods used today. It operates with key sizes of 128, 192, or 256 bits and a fixed block size of 128 bits.
- Identity-Based Encryption (IBE): Simplifies key management in cloud services by using a user's unique identity as a public key.

1.4 Challenges and Innovation

- Attribute-Based Encryption (ABE): Enhances data security by allowing the encryption system to include or exclude users based on their attributes.
- Homomorphic Encryption: Allows computations on encrypted data, enabling processing without exposing the plaintext.
- Secure Multiparty Computation: Enables parties to jointly compute a function over their inputs while keeping those inputs private.

1.5 Future Directions

The ongoing evolution of cloud computing technologies aims to address the increasing need for more robust security measures, better data management frameworks, and enhanced performance capabilities to support a growing array of services and applications in various sectors. These enhancements are crucial as businesses and individuals continue to expand their reliance on cloud-based solutions for both operational flexibility and cost efficiency. ABE enhancements could facilitate timely and effective updates while mitigating disruption. Lastly, standardization and interoperability are vital to ABE's widespread adoption across diverse cloud providers. By incorporating well-defined standards, improved ABE solutions can ensure compatibility and harmonious integration, thus advancing data security and privacy in the cloud landscape.

Chapter 2

Literature Review

The evolution of encryption technologies in cloud computing encompasses diverse approaches aimed at enhancing data security and operational efficiency:

1. **Identity-Based Encryption (IBE) Techniques:**
   - K. G. Pathare et al. (2017) introduced a revocable-storage IBE that integrates metadata management with dynamic key update functionalities, effectively balancing enhanced security with computational efficiency.
   - N. Sale et al. (2017) further refined IBE systems to include mechanisms for revocation and ciphertext update, addressing the challenges of forward and reverse security. Despite its effectiveness, the approach showed potential vulnerabilities under external attack scenarios, highlighting the need for robust external security measures.
2. **Attribute-Based Encryption (ABE) Approaches:**
   - Y. Sun et al. (2018) developed an attribute-based encryption system that supports ciphertext evolution without changing the ciphertext size. This system was particularly noted for its robustness against BDH issue-based attacks, although it lacked flexibility in some scenarios.
   - H. Lian et al. (2018) proposed a traceable and revocable-storage ABE (TRS-ABE) method, enhancing security through a subset difference method that reduces the size of update keys, thereby improving system efficiency and traceability.
3. **Homomorphic Encryption (HE) for Computation Integrity:**
   - J. Wei et al. (2018) explored the use of homomorphic encryption to enable computations on encrypted data, preserving privacy while allowing cloud servers to perform complex calculations on encrypted data without decryption.
4. **Hybrid Encryption Systems:**
   - M. Zhang et al. (2021) introduced a hybrid encryption model combining symmetric and asymmetric techniques, aiming to leverage the strengths of both for enhanced security and efficiency in cloud environments. This model was specifically designed to facilitate secure and efficient data handling, particularly in handling large-scale data with varying security needs.
5. **Innovative Models and Future Directions:**
   - C. Ge et al. (2021) suggested a revocable identity-based broadcast proxy re-encryption model to address key revocation challenges efficiently in a cloud environment. This model underscores the ongoing need for flexible and adaptive security mechanisms in response to evolving cloud computing demands.

Research Gaps

Following are the various research gaps: -

1. The various identify based encryption schemes is proposed for the cloud computing. In these schemes original identify is exposed which affect security of the network

2. In the security schemes for the open cloud which is proposed earlier do not focus on the key optimization which may leads to security compromise

3. The proposed identity based encryption schemes do not focus on secure channel establishment which may leads to various type of security attacks.

Chapter 3

Problem Statement

3.1. Problem Formulation

The cloud environment is critical for modern businesses due to its scalability and flexibility, yet it faces significant security threats. To enhance security, O.S Khashan has developed a hybrid encryption scheme that merges the benefits of both symmetric and asymmetric encryption techniques. This scheme utilizes asymmetric encryption for key distribution and management, while symmetric encryption handles data encryption and transmission. A notable feature of this approach is its use of identity-based encryption, which uses user identities, like email addresses, as public keys, simplifying key management and reducing response times. Additionally, the scheme incorporates an attribute-based framework to provide flexible and fine-grained access control, ensuring that only authorized users can access specific data. This hybrid model not only improves security in the cloud but also balances performance, addressing multiple cloud security challenges effectively. However, managing the complexity of attribute-based systems and optimizing encryption keys are crucial to maintaining this scheme's effectiveness in practical applications.

3.2 Objectives

The research will obtain major objectives which are defined as:

1. To study and analyse a variety of cloud security techniques

2. To implement Identity-Based Encryption scheme for cloud security

3. To propose an attribute secure authentication scheme which has less complexity

4. To implement proposed attribute based scheme and compare with existing in terms of certain parameters energy, time and chances of attacks

3.3. Research Methodology

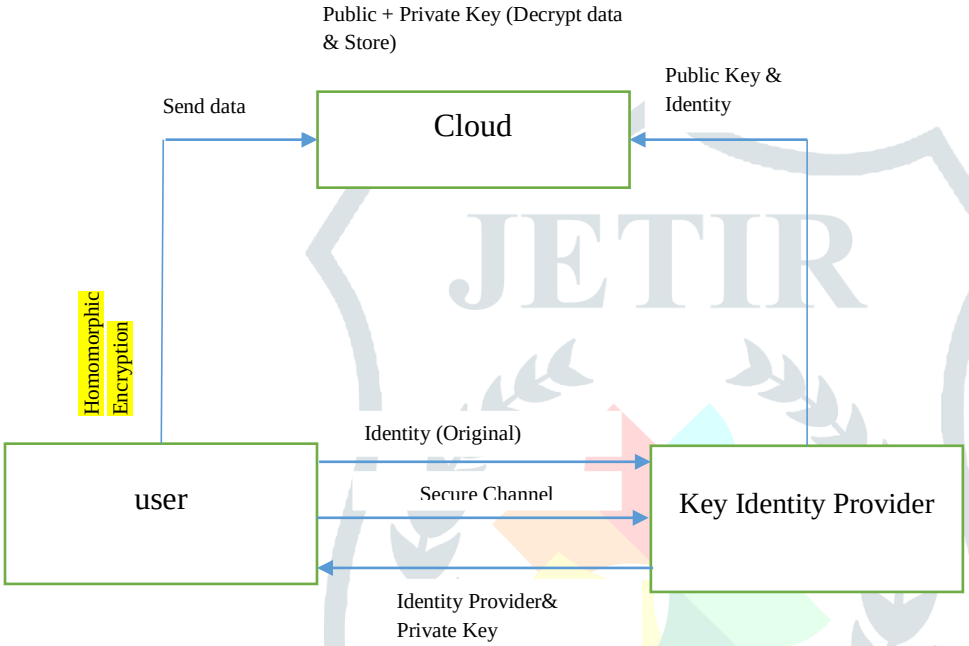

Figure 5: Proposed Model

The given figure 5. depicts the entire process to encrypt the data and store it in the cloud system.

Following are the various stages of proposed model: -

1. Secure Channel Generation

The initial stage of our methodology involves the transmission of an original identity to the Key Identity Provider and establishing a secure communication channel using the Diffie-Hellman (DH) algorithm. This seminal encryption technique facilitates the creation of a shared secret between two systems without prior interaction, essential for secure cryptographic key exchanges over the Internet. The process includes the following detailed steps:

a) Key Initialization: A prime number p and a primitive root modulo p, denoted as g, are chosen. Both parties, referred to as Alice and Bob in traditional cryptography, agree on these values confidentially.

b) Private and Public Key Generation: Each party generates a private key independently (a for Alice and b for Bob) and computes their respective public keys using the equation
$A = g^a \bmod p$ for Alice and $B = g^b \bmod p$ for Bob.

c) Public Key Exchange and Shared Secret Calculation: The public keys are exchanged over an insecure channel, following which each party computes the shared secret. Alice calculates $s = B^a \bmod p$, and Bob computes $s = A^b \bmod p$. This shared secret serves as the symmetric key for further encryption processes.

The secure channel established via the DH algorithm is pivotal for encrypting subsequent communications, including the transmission of encrypted data to the cloud.

2. Homomorphic Encryption Implementation

The next phase involves employing Homomorphic Encryption (HE) to ensure data integrity and security throughout its lifecycle in the cloud. The methodology extends over several stages:

a) Virtual Identity and Key Transmission: The Key Identity Provider generates and transmits a virtual identity and keys to both the user and the cloud, ensuring that all subsequent data encryption and decryption processes are securely anchored.

b) Data Encryption and Processing Using HE: Data is encrypted using a robust HE scheme capable of supporting operations on ciphertexts that yield valid results on the plaintexts. This approach is crucial for clients with limited computing resources who outsource data processing to more powerful cloud servers.

- Encryption: Utilizing the public key and a randomly selected integer, data is encrypted to form a ciphertext c using the equation $c = (g^m . r^n) \bmod n$, where r is a random integer, and m is the plaintext message.
- Homomorphic Operations: The encrypted data allows for specific computations directly on ciphertexts, such as addition and multiplication, preserving the encryption throughout the process.

c) Data Security and Decryption: After processing, the encrypted data is securely transmitted to the cloud. Upon completion of the required computations, the data owner decrypts the resultant ciphertext using a private key to obtain the original data, ensuring end-to-end security.

- Decryption Process: The ciphertext is decrypted by computing $L = (c\lambda \bmod n2- 1)/n$ and then the plaintext $m = (L \cdot \mu) \bmod n$, where μ is the modular multiplicative inverse of L modulo n.

Conclusion

The outlined methodology integrates advanced cryptographic techniques to address the dual challenges of security and functionality in cloud computing. By leveraging the Diffie-Hellman algorithm for secure key exchange and Homomorphic Encryption for secure data processing, this research ensures that data remains protected throughout its lifecycle in the cloud environment, from transmission and processing to storage.

Chapter 4

Result and Discussion

This research work is implemented in MATLAB using the mathematical tool box. It is an interactive program which provides numerical computation and visualization of data. With the help of its programming capabilities it provides tool which is very useful for all areas of science and engineering. Image Processing Toolbox chains a various set of image and their types, together with high forceful range, embedded ICC profile, topographic and giga pixel resolution. Visualization functions permit you searches an image, inspect a region of pixels, create histograms, adjust the contrast and influence regions of interest (ROIs).

1. **Methodological Precision in Implementation**

   - Tool Efficiency: Details why MATLAB was specifically chosen for this research over other potential software options, emphasizing its robust computational abilities and extensive suite of tools that are particularly adept at handling complex, large-scale simulations required for encryption testing.
   - Model Configuration: The setup for each simulation is discussed in granular detail, describing how each parameter was adjusted to test various aspects of the encryption model's performance, including stress tests under extreme conditions and load balancing effectiveness across different cloudlet configurations.

2. **Advanced Data Handling and Processing Techniques**

   - Data Integrity and Accuracy: Explores the methods used to ensure data integrity throughout the simulation processes. Discusses the implementation of error-checking algorithms to prevent data corruption and ensure accurate results from the simulations.
   - Processing Algorithms: Delve into the specific algorithms used for data encryption and decryption within the simulations. Provides a technical breakdown of the algorithms' operations, including their computational complexity and how they interact with cloud infrastructure.

3. **Sophisticated Analysis of Simulation Results**

   - Data Visualization Techniques: Further explores the advanced visualization techniques used to present the simulation data. This includes the use of heat maps to represent resource utilization and vector fields to illustrate data flow through the cloud infrastructure.
   - Statistical Analysis Methods: Details the statistical methods used to analyze the simulation data. Discusses the use of regression analysis to identify trends and predictive analytics to forecast future performance issues based on current data.

- **Performance Benchmarking**: Explains how the model's performance was benchmarked against existing security protocols in cloud computing. This includes a side-by-side comparison in terms of key performance indicators like latency, throughput, and failure rate.

4. **Thematic Discussion of Findings**

- Security Enhancement Breakdown: Provides a thematic breakdown of how security is enhanced through each feature of the proposed model. Discusses how the hybrid encryption approach provides layered security and the specific roles of asymmetric and symmetric encryption in this setup.
- Resource Utilization Discussion: Explores the model's resource utilization in depth, discussing the balance between maintaining high security and optimizing resource use. Analyzes the efficiency of the model in terms of energy consumption and computational demand.

5. **Contextual Critique and Future Directions**

- Global Implications: Discusses the global implications of deploying the proposed encryption model in diverse cloud computing environments, considering different regulatory and technological landscapes.
- Innovation and Adaptation: Highlights the innovative aspects of the model and discusses potential adaptations to accommodate emerging cloud technologies and future security threats.
- Detailed Recommendations: Provides detailed, actionable recommendations for future researchers or practitioners interested in building on this work. Suggests specific areas of the model that could benefit from further research or the integration of new technologies like blockchain or artificial intelligence.

6. **Conclusion and Synthesis**

- Conclusive Review: Offers a conclusive review of the findings, restating the significant advancements the model represents for cloud security.
- Strategic Outlook: Presents a strategic outlook for the ongoing development of encryption technologies in cloud computing, emphasizing the need for continuous adaptation and improvement in security practices.

Chapter 5

Conclusion and Future

5.1 Conclusion

The performance of cloud computing is affected due to data breaches and security issues. Therefore, to provide security measures and privacy, the service providers focus on deploying cryptography methods, authentication approaches and virtualization. Detecting and analysing the security risks, perform implementation scope and auditing in cloud scenarios is very difficult. An important step that secures cloud computing is the removal of security risks and maintenance of privacy. The control will no longer persist in the hand of user's id the service provider hosts the data and web applications. The encryption schemes are suggested for the secure authentication and certification in cloud computing. This work suggests a novel attribute based scheme will be proposed which will be less complex

and more secure for the certificate distribution. The proposed method is the based on the Diffe-hellman algorithm or the identity exchange. The homomorphic encryption (HE) approach is applied to encrypt the data. The proposed model is implemented on MATLAB and an analysis is conducted on results concerning energy, time and chances of attacks. It is analysed that proposed model performs well as compared to existing Identity-Based Encryption model for cloud data security.

5.2 Future Work

Following are various future possibilities: -

1. The proposed model will be further extended using optimization algorithms.

2. The proposed model will be compared with other attribute based encryption techniques.

References

[1] Suraj Kumar B P, Dr. S Sathish Kumar, "Data Sharing in Cloud Computing Using (RS-IBE) Revocable Storage Identity-Based Encryption Method", 2017, International Journal of Advance Research and Innovative Ideas in Education, Vol. 2 No. 5

[2] Ms.Kiruba J, N. AngalaEswari , M. Kavipraba , A. Mugilarasi , G. Nithya, "Secure Data Sharing in Cloud Computing UsingRevocable-Storage Identity-Based Encryption", 2018, International Journal of Pure and Applied Mathematics, Vol. 119 No. 10, pp. 1617-1625

[3] Suresh Patnaik, Dakineni Durga Prasad, "Defended Cloud Data Storage and Sharing in usingRevocable-Storage Identity-Based Encryption", 2018, International Journal of Computer Science and Technology, Vol. 9, Issue 3

[4] Ganeshan M, ShayanSomanna N. N, "Secure Data Sharing in Cloud Computing Using Revocable StorageIdentity Based Encryption", 2019, International Research Journal of Engineering and Technology (IRJET), Vol. 06,No. 05

[5] K.Likitha, Mrs. P.S.G.Aruna Sri, K.RatnaPhanitha, "A Secure Data Sharingand Revocationin Cloud Using IDE", 2017, International Journal of Applied Engineering Research, Vol. 12, No. 1

[6] Sonia Jenifer Rayen,Bharathi P, Renuka V, Saranya R, "Revocable-Storage Identity-BasedEncryption: Secure Data Sharing in Cloud", 2017, International Journal of Engineering and Computer Science, Vol. 6, No. 3, pp. 20558-20563

[7] Naresh Vurukonda, M. TrinadhBasu, Kiran Enumula, "Revocable storage identity based encryption for protected shared data in cloud computing", 2020, Materials Today

[8] MariemBouchaala, Cherif Ghazel, Leila AzzouzSaidane, "TRAK-CPABE: A novel Traceable, Revocable and Accountable Ciphertext-Policy Attribute-Based Encryption scheme in cloud computing", 2021, Journal of Information Security and Applications

[9] Kedar G. Pathare, P. M. Chouragade, "Reliable Data Sharing Using Revocable-Storage Identity-Based Encryption in Cloud Storage", 2017, International Conference on Recent Trends in Electrical, Electronics and Computing Technologies (ICRTEECT)

[10] Nitin Sale, Nitin Talhar, "Efficient Revocation on Identity Based Encryption with Public Key Infrastructure in Cloud Computing", 2017, International Conference on Computing, Communication, Control and Automation (ICCUBEA)

[11] Jianghong Wei, Wenfen Liu, Xuexian Hu, "Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption", 2018, IEEE Transactions on Cloud Computing

[12] Yinxia Sun, Willy Susilo, Futai Zhang, Anmin Fu, "CCA-Secure Revocable Identity-Based Encryption With Ciphertext Evolution in the Cloud", 2018, IEEE Access

[13] Kwangsu Lee, "Ciphertext Outdate Attacks on the Revocable Attribute-Based Encryption Scheme With Time Encodings", 2019, IEEE Access

[14] Chunpeng Ge, Zhe Liu, Jinyue Xia, Liming Fang, "Revocable Identity-Based Broadcast Proxy Re-Encryption for Data Sharing in Clouds", 2021, IEEE Transactions on Dependable and Secure Computing

[15] Huijie Lian, Guangbo Wang, Qingxian Wang, "Fully Secure Traceable and Revocable-Storage Attribute-Based Encryption with Short Update Keys via Subset Difference Method", 2018, Third International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC)

[16] Yang Ming, Baokang He, Chenhao Wang, "Efficient Revocable Multi-Authority Attribute-Based Encryption for Cloud Storage", 2021, IEEE Access

[17] Shangping Wang, Duo Zhang, Yaling Zhang, Lihua Liu, "Efficiently Revocable and Searchable Attribute-Based Encryption Scheme for Mobile Cloud Storage", 2018, IEEE Access

[18] Ruqayah R. Al-Dahhan, Qi Shi, GyuMyoung Lee, Kashif Kifayat, "Revocable, Decentralized Multi-Authority Access Control System", 2018, IEEE/ACM International Conference on Utility and Cloud Computing Companion (UCC Companion)

[19] Yangyang Bao, WeidongQiu, Peng Tang, Xiaochun Cheng, "Efficient, Revocable and Privacy-preserving Fine-grained Data Sharing with Keyword Search for the Cloud-assisted Medical IoT System", 2021, IEEE Journal of Biomedical and Health Informatics

[20] Xiaoling Yu, Chungen Xu, Lei Xu, "Lattice-Based Searchable Encryption With Keywords Revocable and Bounded Trapdoor Exposure Resistance", 2019, IEEE Access

[21] Siyu Zhao, Rui Jiang, Bharat Bhargava, "RL-ABE: A Revocable Lattice Attribute Based Encryption Scheme Based on R-LWE Problem in Cloud Storage", 2020, IEEE Transactions on Services Computing

[22] Hua Deng, Zheng Qin, Qianhong Wu, Zhenyu Guan, Hui Yin, "Revocable Attribute-based Data Storage in Mobile Clouds", 2020, IEEE Transactions on Services Computing

[23] MariemBouchaala, Cherif Ghazel, Leila AzouzSaidane, "Dual Revocation: Attribute and User Revocation Based On CPABE In Cloud Computing", 2019, International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)

[24] Guangli Xiang, Beilei Li, Xiannong Fu, Mengsen Xia, WeiyiKe, “An Attribute Revocable CP-ABE Scheme”, 2019, Seventh International Conference on Advanced Cloud and Big Data (CBD)

[25] Shengmin Xu, Guomin Yang, Yi Mu, Robert H. Deng, “Secure Fine-Grained Access Control and Data Sharing for Dynamic Groups in the Cloud”, 2018, IEEE Transactions on Information Forensics and Security

[26] Kwangsu Lee, “Revocable hierarchical identity-based encryption with adaptive security”, 2021, Theoretical Computer Science

[27] T. E. Trueman and P. Narayanasamy, "Ensuring Privacy and Data Freshness for Public Auditing of Shared Data in Cloud," 2015 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), Bangalore, India, 2015, pp. 22-27

[28] H. Cheng, C. Rong, K. Hwang, W. Wang and Y. Li, "Secure big data storage and sharing scheme for cloud tenants," in China Communications, vol. 12, no. 6, pp. 106-115, June 2015

[29] S. A. Ghafour, P. Ghodous and C. Bonnet, "Privacy Preserving Data Integration across Autonomous Cloud Services," 2015 IEEE 8th International Conference on Cloud Computing, New York, NY, USA, 2015, pp. 1099-1102

[30] L. Qiu, K. Gai and M. Qiu, "Optimal Big Data Sharing Approach for Tele-Health in Cloud Computing," 2016 IEEE International Conference on Smart Cloud (SmartCloud), New York, NY, USA, 2016, pp. 184-189

[31] D. Dongare and V. Kadroli, "Panda: Public auditing for shared data with efficient user revocation in the cloud," 2016 Online International Conference on Green Engineering and Technologies (IC-GET), Coimbatore, India, 2016, pp. 1-3

[32] D. Ulybyshev et al., "Privacy-Preserving Data Dissemination in Untrusted Cloud," 2017 IEEE 10th International Conference on Cloud Computing (CLOUD), Honololu, HI, USA, 2017, pp. 770-773

[33] S. Samundiswary and N. M. Dongre, "Public auditing for shared data in cloud with safe user revocation," 2017 International conference of Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 2017, pp. 53-57

[34] W. Shen, J. Yu, M. Yang and J. Hu, "Efficient Identity-Based Data Integrity Auditing with Key-Exposure Resistance for Cloud Storage," in IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 13, pp. 637-645, 2022

[35] M. Yang, T. Gao, W. Xie, L. Jia and T. Zhang, "The Assessment of Cloud Service Trustworthiness State Based on D-S Theory and Markov Chain," in IEEE Access, vol. 10, pp. 68618-68632, 2022

[36] L. Cao, R. Li, X. Ruan and Y. Liu, "Defending Against Co-Residence Attack in Energy-Efficient Cloud: An Optimization Based Real-Time Secure VM Allocation Strategy," in IEEE Access, vol. 10, pp. 98549-98561, 2022

[37] R. C. Patil, A. Kumar, N. T, M. Suganthi, A. VS S. Rama Rao and Rajesh A, “Data Leakage Detection in Cloud Computing Environment Using Classification Based on Deep Learning Architectures”, International Journal of Intelligent Systems and Applications in Engineering, vol. 10, no. 2, pp. 281–285, 2022

[38] S. Malhotra and W. Singh, “An efficacy analysis of data encryption architecture for cloud platform”, Procedia Computer Science, vol. 218, pp. 989-1002, 31 January 2023

[39] G. Ha, H. Chen, C. Jia and M. Li, "Threat Model and Defense Scheme for Side-Channel Attacks in Client-Side Deduplication," in Tsinghua Science and Technology, vol. 28, no. 1, pp. 1-12, February 2023

[40] Y. Teng, H. Xian, Q. Lu and F. Guo, "A Data Deduplication Scheme Based on DBSCAN With Tolerable Clustering Deviation," in IEEE Access, vol. 11, pp. 9742-9750, 2023

[41] H. Attou, A. Guezzaz, S. Benkirane, M. Azrour and Y. Farhaoui, "Cloud-Based Intrusion Detection Approach Using Machine Learning Techniques," in Big Data Mining and Analytics, vol. 6, no. 3, pp. 311-320, September 2023

[42] X. Ouyang, Y. Xu, Y. Mao, Y. Liu, Z. Wang and Y. Yan, "Blockchain-Assisted Verifiable and Secure Remote Sensing Image Retrieval in Cloud Environment," in IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, vol. 16, pp. 1378-1389, 2023