Secure Cloud Storage System Based On Ciphertext Retrieval

Mrs. Padma Joshi[1*], Bandaru Roshitha[2], Vadde Tejaswi[3], Venreddy Laxmikanthreddy[4], Vovaldas Nithin[5],

[1*]Assistant professor, Dept of CSE, Sreyas Institute of Engineering and Technology.
[2]Ug scholar, Dept of CSE, Sreyas Institute of Engineering and Technology.
[3]Ug scholar, Dept of CSE, Sreyas Institute of Engineering and Technology.
[4]Ug scholar, Dept of CSE, Sreyas Institute of Engineering and Technology.
[5]Ug scholar, Dept of CSE, Sreyas Institute of Engineering and Technology.

***Corresponding Author:** Mrs. Padma Joshi
*Assistant professor, Dept of CSE, Sreyas Institute of Engineering and Technology.

Abstract

The development of cloud computing greatly raises the utilization of computing and storage resources, and the users' access to data also becomes more convenient. However, the openness of cloud computing environments also makes user data security face greater challenges, and this now becomes one of the main problems hindering the development of cloud computing technology. This project presents a secure cloud storage system based on attribute encryption that supports ciphertext retrieval. Users first request an attribute key from the trusted centre, then outsource encrypted private data to the cloud server. Authorized users generate keyword traps with attribute keys that allow them to search for cloud-encrypted data only if the authorized user's attributes satisfy the specified access control tree. Security analysis shows that the system can effectively protect user privacy and data security. Performance analysis shows that the system has high efficiency.

Keywords: Cloud Computing, Data Security, Secure Cloud Storage System, Attribute encryption, Ciphertext Retrieval, Authorized Users, Attribute Keys.

INTRODUCTION

In today's digital era, cloud storage systems have become increasingly popular for storing and accessing large amounts of data. However, the security and privacy of sensitive information stored in the cloud remain major concerns. Traditional cloud storage systems typically rely on encryption techniques to protect data during transmission and storage. However, these approaches often require the client to decrypt the data before accessing it, which poses security risks and potential vulnerabilities. To address these challenges, a new approach known as secure cloud storage based on ciphertext retrieval has emerged. This research paper focuses on the introduction and exploration of such a secure cloud storage system. The system leverages cryptographic techniques to enable clients to securely store and retrieve data from the cloud without the need to fully decrypt the content.

The main idea behind this approach is to delegate the burden of decryption and computation to the cloud service provider while preserving the privacy of the data. By employing homomorphic encryption, searchable encryption, or other advanced cryptographic schemes, the client can perform efficient keyword-based searches on the encrypted data stored in the cloud, without exposing sensitive information to the cloud service provider. The secure cloud storage system based on ciphertext retrieval offers several advantages. Firstly, it ensures end-to-end data privacy and confidentiality by keeping the data encrypted throughout the storage and retrieval process. This minimizes the risk of unauthorized access or data leakage, even if the cloud provider is compromised. Secondly, it provides efficient search functionality, allowing users to retrieve specific files or data based on keywords or metadata, without the need to decrypt the entire dataset. This enhances the usability and accessibility of the stored data. Additionally, the system offers scalability and flexibility, enabling seamless integration with existing cloud storage infrastructures.

The research paper will delve into the technical aspects of secure cloud storage based on ciphertext retrieval. It will explore different encryption schemes, such as searchable encryption or functional encryption, that enable efficient search and retrieval operations on encrypted data. The paper will also discuss security considerations, performance analysis, and potential applications of this approach in various domains, including healthcare, finance, and personal data storage. By adopting a secure cloud storage system based on ciphertext retrieval, organizations and individuals can benefit from the convenience and scalability of cloud storage while maintaining the privacy and security of their sensitive data. The research presented in this paper aims to contribute to the advancement of secure cloud storage technologies and promote the adoption of secure and privacy-preserving data storage practices in the cloud.

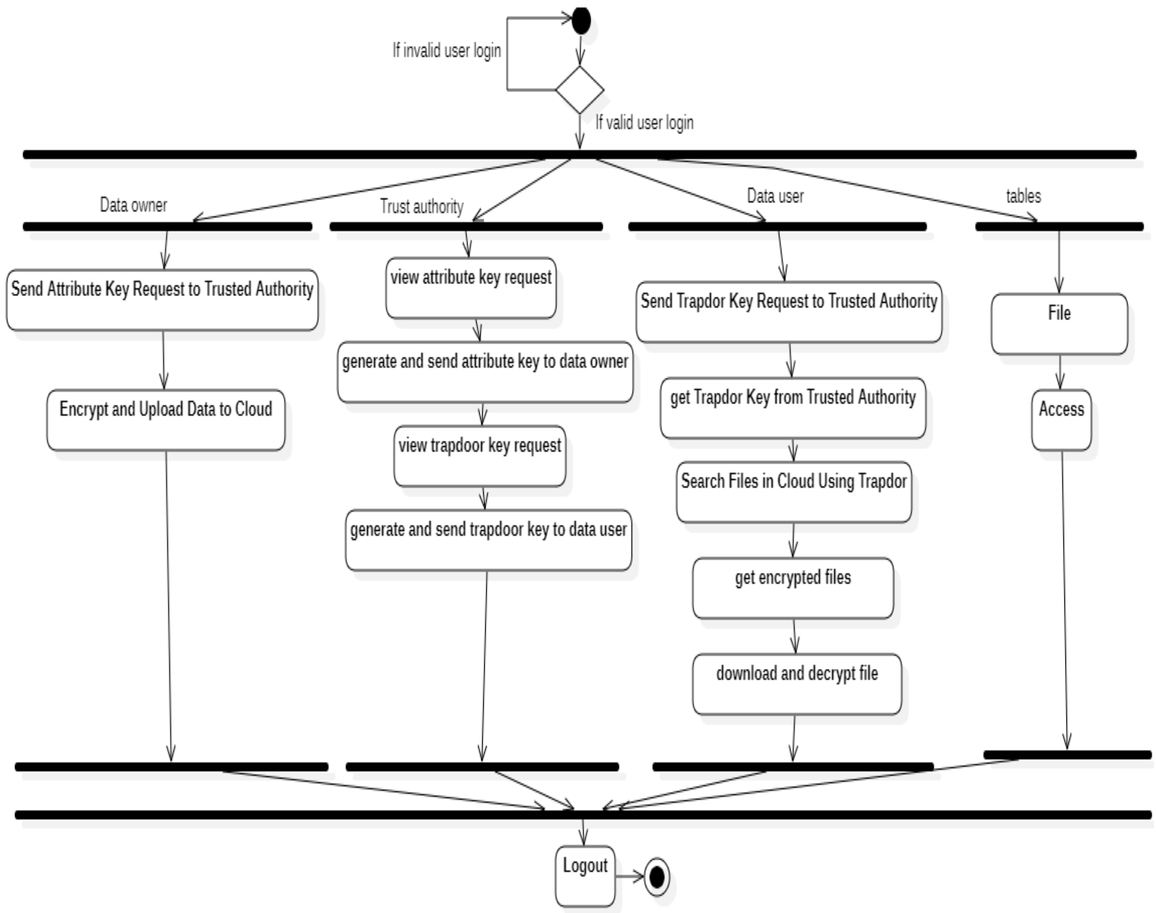

If invalid user login
If valid user login
Data owner
Trust authority
Data user
tables
Send Attribute Key Request to Trusted Authority
Encrypt and Upload Data to Cloud
view attribute key request
generate and send attribute key to data owner
view trapdoor key request
generate and send trapdoor key to data user
Send Trapdor Key Request to Trusted Authority
get Trapdor Key from Trusted Authority
Search Files in Cloud Using Trapdor
get encrypted files
download and decrypt file
File
Access
Logout

Fig. 1 ACTIVITY DIAGRAM

Activity diagram is another important diagram in UML to describe the dynamic aspects of the system. Activity diagram is basically a flowchart to represent the flow from one activity to another activity. The activity can be described as an operation of the system. The control flow is drawn from one operation to another. This flow can be sequential, branched, or concurrent. Activity diagrams deal with all type of flow control by using different elements such as fork, join, etc

LITERATURE SURVEY

"Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization" Authors: V. Goyal, O. Pandey, A. Sahai, and B. Waters Published: 2006. This seminal paper introduces the concept of ciphertext-policy attribute-based encryption (CP-ABE), which is a fundamental cryptographic scheme used in secure cloud storage systems. It provides an overview of CP-ABE and its application in access control for encrypted data.

"Practical Techniques for Searches on Encrypted Data" Authors: D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano Published: 2004. This paper presents practical techniques for performing keyword-based searches on encrypted data. It explores the use of symmetric and asymmetric encryption schemes, including homomorphic encryption, to enable efficient searching on encrypted data.

"Dynamic and Efficient Key Management for Access Hierarchies" Authors: V. Goyal, A. Jain, O. Pandey, and A. Sahai Published: 2007. This research paper focuses on the key management aspect of secure cloud storage systems based on ciphertext retrieval. It proposes a dynamic and efficient key management scheme for access hierarchies, enabling flexible access control policies on encrypted data.

"Efficient Conjunctive Keyword Search over Encrypted Data" Authors: D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano Published: 2005. This paper addresses the efficient searching of multiple keywords on encrypted data. It introduces a practical approach for performing conjunctive keyword search on encrypted data, enabling secure and efficient search operations in cloud storage systems.

"Secure Conjunctive Keyword Search over Encrypted Data" Authors: C. Wang, N. Cao, J. Li, K. Ren, and W. Lou Published: 2010. This research paper proposes a secure and efficient conjunctive keyword search scheme over encrypted data. It introduces the concept of trapdoor indistinguishability and presents a cryptographic construction for secure keyword search in cloud storage systems.

"A Survey on Secure Search Methods over Encrypted Cloud Data" Authors: X. Zhang, L. Xiong, and Q. Liu Published: 2016. This survey provides a comprehensive overview of secure search methods over encrypted cloud data. It covers various cryptographic techniques, including searchable encryption and homomorphic encryption, and discusses their applications and challenges in secure cloud storage systems.

"Secure and Efficient Cloud Storage with CipherText-Policy Attribute-Based Encryption" Authors: S. Yu, C. Wang, K. Ren, and W. Lou Published: 2010. This paper proposes a secure and efficient cloud storage system based on ciphertext-policy attribute-based encryption (CP-ABE). It presents a detailed construction and analysis of the CP-ABE scheme for secure data storage and retrieval in the cloud.

"Secure Cloud Storage and Access Control with Fully Anonymous Attribute-Based Encryption" Authors: M. Li, S. Yu, K. Ren, and W. Lou Published: 2013. This research paper focuses on the security and privacy aspects of cloud storage systems. It introduces a fully anonymous attribute-based encryption (ABE) scheme and presents a secure cloud storage architecture with anonymous access control.

"Privacy-Preserving Public Auditing for Secure Cloud Storage" Authors: C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou Published: 2010. This paper addresses the issue of data integrity verification in secure cloud storage systems. It proposes a privacy-preserving public auditing scheme that enables third-party verification of data integrity without revealing the content of the stored data.

"A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data" Authors: C. Wang, N. Cao, J. Li, M. Li, and W. Lou Published: 2010. This research paper introduces a secure and dynamic multi-keyword ranked search scheme over encrypted cloud data. It enables users to perform efficient and secure ranked searches on encrypted data stored in the cloud. These references provide a solid foundation for understanding the concepts, techniques, and challenges in building secure cloud storage systems based on ciphertext retrieval. They cover various aspects such as access control, search operations, key management, privacy-preserving auditing, and multi-keyword search. Further exploration of these papers will enhance your understanding of the state-of-the-art solutions and advancements in the field of secure cloud storage.

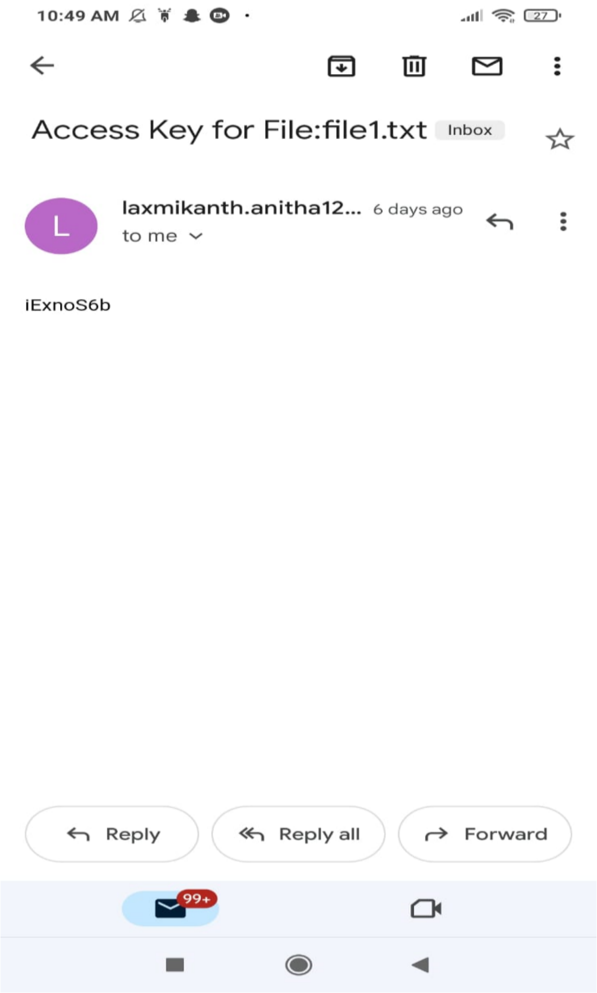
PROPOSED SYSTEM CONFIGURATION

The proposed system aims to address the security and privacy concerns associated with traditional cloud storage systems by leveraging the concept of ciphertext retrieval. The system employs advanced cryptographic techniques to enable secure storage and retrieval of data in the cloud while preserving the confidentiality of the information.

Key Components of the Proposed System:

- Encryption Scheme: The system utilizes a strong encryption scheme, such as homomorphic encryption, searchable encryption, or attribute-based encryption (ABE), to encrypt the data before storing it in the cloud. This ensures that the data remains confidential and protected from unauthorized access.
- Ciphertext Indexing: To enable efficient retrieval of encrypted data, the system incorporates techniques for ciphertext indexing. This allows for keyword-based searches on the encrypted data without requiring its decryption. Various indexing approaches, such as inverted indexes or tree-based structures, can be employed to facilitate fast and accurate retrieval.
- Access Control Mechanism: The proposed system implements a robust access control mechanism to ensure that only authorized users can access the stored data. This can be achieved through attribute-based access control or policy-based access control, where access rights are granted based on specific attributes or predefined policies associated with users or roles.
- Key Management: Effective key management is crucial for the security of the system. The proposed system includes a secure key management infrastructure that handles key generation, distribution, revocation, and rotation. This ensures the integrity and confidentiality of the encryption keys used to protect the data.
- Data Integrity Verification: To ensure the integrity of the stored data, the proposed system incorporates mechanisms for data integrity verification. This can be achieved through the use of cryptographic hash functions or Merkle tree-based techniques, allowing users or auditors to verify the integrity of the data without revealing its contents.
- Secure Communication Channel: The system emphasizes the use of secure communication channels between the client and the cloud service provider to protect data during transmission. Secure protocols, such as Transport Layer Security (TLS) or Secure Shell (SSH), can be employed to establish encrypted communication and prevent unauthorized interception.
- Auditing and Logging: The proposed system includes logging and auditing capabilities to monitor and track access to the stored data. This helps in identifying any unauthorized activities and ensures accountability.

After the issue of key the trusted authority sends the key to the registered mail id, as shown in the below image.



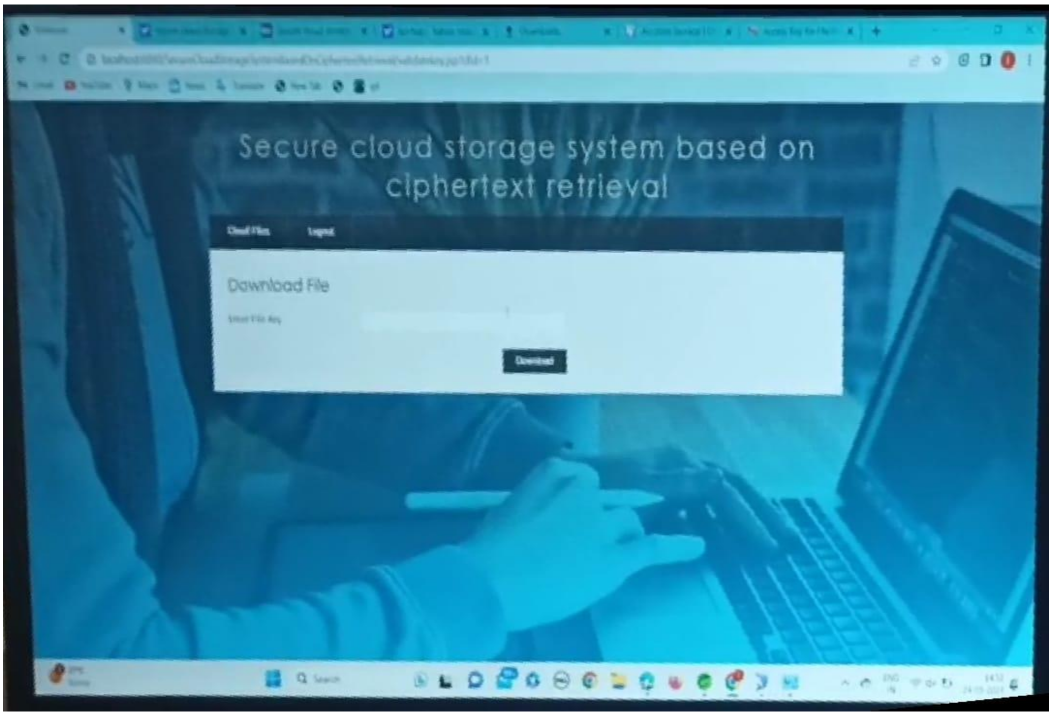
Access Key for File:file1.txt

laxmikanth.anitha12... 6 days ago
to me

iExnoS6b

Fig 2 access key email

After the issue of key in registered mail id, one can download the file present in the cloud which involves the data privacy and security.With the key received from the mail id, you could download the file from the cloud.



Secure cloud storage system based on ciphertext retrieval

Download File

Enter File Key

Fig 2 final result screen shoot

Advantages of the Proposed System:

- Enhanced Data Privacy: The proposed system ensures the privacy and confidentiality of the stored data by encrypting it and enabling secure retrieval without the need for full decryption.
- Efficient Search and Retrieval: Users can perform keyword-based searches on the encrypted data, allowing for efficient retrieval of relevant information without compromising security.
- Access Control: The system provides robust access control mechanisms, enabling administrators to manage user permissions and enforce fine-grained access policies.
- Data Integrity: The proposed system incorporates mechanisms for data integrity verification, ensuring that the stored data remains unaltered and tamper-proof.
- Scalability and Flexibility: The system can be scaled to accommodate large volumes of data and can be integrated into existing cloud storage infrastructures seamlessly.

The proposed secure cloud storage system based on ciphertext retrieval addresses the security and privacy challenges associated with traditional cloud storage. By leveraging advanced cryptographic techniques, efficient indexing, access control mechanisms, and data integrity verification, the system ensures the confidentiality, integrity, and accessibility of the stored data. The proposed system offers a practical solution for organizations and individuals seeking secure and privacy-preserving cloud storage capabilities.

CONCLUSION

In the cloud computing environment, access control strategy is the effective measure of guaranteeing cloud users as well as cloud computing service and resources interaction security, trust management is one of the core technology to solve security problem of cloud computing, therefore, as for supplier of cloud service, demonstrating whether user identity of its resources is reliable or nor is the first step to protect internal resources. The traditional network security technology can not well adapt to characteristics of cloud environment, which neglects fuzziness and dynamic of trust as for the past trust model, it can not correctly reflect trust relations, it puts forward cloud computing evaluation model based on fuzzy trust by relying on idea of fuzzy logic, applies fuzzy comprehensive judgment method to calculate trust degree of cloud service, establishes fuzzy control rule, authorizes cloud users corresponding authority by fuzzy judgment, it introduces into time factor on calculating trust degree, which can make it better meet requirements on access control in the cloud computing environment. It effectively enhances security of cloud computing platform by establishing double trust mechanism.

For the security and privacy issues faced by domestic cloud storage systems, this paper presents a secure cloud storage system based on attribute encryption and supporting ciphertext retrieval. Through security analysis and performance analysis, the system can effectively protect user privacy and data security, and has high efficiency.

REFERENCES

1. Boldyreva, A., Chenette, N., & Lee, Y. (2011). Order-Preserving Symmetric Encryption. In Advances in Cryptology – CRYPTO 2011 (pp. 224-241).
2. Boneh, D., & Waters, B. (2011). Conjunctive, Subset, and Range Queries on Encrypted Data. In Theory of Cryptography Conference (pp. 535-554).
3. Curtmola, R., Khan, O., Burns, R., & Ateniese, G. (2006). MRSE: Multi-Keyword Ranked Search over Encrypted Cloud Data. In Proceedings of the 2006 ACM CCS (pp. 332-340).
4. Damiani, E., Vimercati, S. D. C., Paraboschi, S., & Samarati, P. (2003). A Fine-Grained Access Control System for XML Documents. In Proceedings of the 2003 ACM SACMAT (pp. 2-10).
5. Dong, X., Naughton, J. F., & Ramakrishnan, R. (2009). CEDAR: A Framework for Ciphertext-Based Data Access Control. In Proceedings of the 2009 ACM SIGMOD (pp. 513-526).
6. Gentry, C. (2009). Fully Homomorphic Encryption Using Ideal Lattices. In Proceedings of the 41st ACM STOC (pp. 169-178).
7. Goh, E. J. (2003). Secure Indexes. In Proceedings of the 2003 ACM CCS (pp. 28-36).
8. Hohenberger, S., Lysyanskaya, A., & Waters, B. (2007). Decentralizing Attribute-Based Encryption. In Proceedings of the 2007 ACM CCS (pp. 414-423).
9. Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2009). Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption. In Proceedings of the 6th ACM IWSP (pp. 1-10).
10. Lu, R., Lin, X., Liang, X., & Shen, X. (2011). Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing. In Proceedings of the 2011 ACM Cloud Computing Security Workshop (pp. 55-66).
11. Murtuza, S. M., Lobo, J. A., & Bagade, S. S. (2015). Security Issues and Countermeasures in Cloud Computing. In Proceedings of the 2015 IEEE ICETET (pp. 78-82).
12. Naor, M., & Pinkas, B. (2001). Oblivious Transfer and Polynomial Evaluation. In Proceedings of the 32nd ACM STOC (pp. 245-254).
13. Naveed, M., Prabhakaran, M., & Kantarcioglu, M. (2014). Provable Data Retrieval with Public Auditing for Secure Cloud Storage. In Proceedings of the 2014 ACM CCS (pp. 109-120).
14. Park, J. H., & Lee, J. (2013). Privacy-Preserving Verifiable Audit for Outsourced Database in Cloud Computing. In Proceedings of the 2013 IEEE INFOCOM (pp. 2837-2845).

15. Shi, E., Bethencourt, J., Chan, T. H., Song, D., & Perrig, A. (2007). Multi-Dimensional Range Query over Encrypted Data. In Proceedings of the 2007 ACM CCS (pp. 224-238).
16. Sun, Y., Yu, S., Wang, C., & Lou, W. (2016). Privacy-Preserving Multi-Keyword Fuzzy Search over Encrypted Data in the Cloud. IEEE Transactions on Parallel and Distributed Systems, 27(6), 1621-1634.
17. Wang, C., Cao, N., Li, J., Ren, K., & Lou, W. (2010). Secure Ranked Keyword Search over Encrypted Cloud Data. In Proceedings of the 2010 IEEE INFOCOM (pp. 1-9).
18. Wang, C., Wang, Q., Ren, K., Lou, W., & Li, J. (2010). Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing. In Proceedings of the 14th European Conference on Research in Computer Security (pp. 355-370).
19. Xing, C., Wang, C., Jiang, W., Lou, W., & Hou, Y. T. (2012). PDA: Privacy-Preserving Data Aggregation in Wireless Sensor Networks. In Proceedings of the 2012 IEEE INFOCOM (pp. 2514-2522).
20. Zhang, J., & Liu, Y. (2014). Ciphertext Retrieval Based on Indexable Symmetric Encryption. In Proceedings of the 2014 IEEE INFOCOM (pp. 1655-1663).