SECURE AND EFFICIENT CLOUD STORAGE USING KEY-POLICY ATTRIBUTE-BASED TEMPORARY

Munazza Sameen
Scholar
Department of MCA
Vaageswari College of Engineering, Karimnagar

P. Sathish
Assistant Professor
Department of MCA
Vaageswari College of Engineering, Karimnagar

Dr. V. Bapuji
Professor & Head
Department of MCA
Vaageswari College of Engineering, Karimnagar

ABSTRACT: Temporary keyword searches on private cloud data are the focus of this study. Cloud providers may not be reliable. Therefore, it's crucial to outsource encrypted data handling. Users with the right permissions can send search tokens to the cloud for attribute-based keyword search (ABKS) schemes, and can get all the keyword-containing ciphertexts generated at that time with these search tokens. Having search tokens only extract ciphertexts created within a certain time frame improves security by reducing information leaks. In this work, introduce key-policy attribute-based temporary keyword search (KPABTKS), a new cryptography with the requested feature. A formal test determines if our plan is secure against selectively chosen keyword attacks (SCKA) and meets the Decisional Bilinear Diffie-Hellman (DBDH) assumption in both the random oracle model and the random oracle model also demonstrate that the encryption algorithm's complexity is linear with the number of attributes used.

Keywords: **attribute-based keyword search (ABKS) schemes, cloud service provider (CSP)**

1. INTRODUCTION

Cloud computing provides reliable, flexible, and low-cost data storage and processing, making it essential to modern life. However, the cloud's direct access to users' private data compromises privacy. Encrypting data before sending it to the cloud solves this problem easily. Encrypted data is difficult to search.

Boneh et al. developed public key encryption with keyword search to simplify encrypted data search. The data owner uses the intended data user's public key to create

a searchable ciphertext in PEKS. This ciphertext is then stored in the cloud. The data user then uses their private key to get a keyword-related search token and sends to the cloud. The cloud service provider (CSP) searches for relevant keywords using the search token on behalf of the data user.

Zheng et al. proposed attribute-based keyword search (ABKS) to let data owners control who sees encrypted, outsourced data. The multi-sender/multi-receiver paradigm used attribute-based encryption (ABE) to create a searchable cryptographic primitive. People with access can search for data in the cloud without talking to the owner. A safe Attribute-Based Keyword Search (ABKS) scheme prevents data owners from learning what keywords people will use to search for it.

The cloud can use PEKS and ABKS to search for a keyword in past and future ciphertexts if it has a valid search token. In other words, if the attacker finds the exact keyword linked to the target search token, she can see some information about the documents that will be sent to the cloud. Limiting the search token's use will make operations safer.

Abdalla et al. proposed public key encryption with temporary keyword search to solve this problem. PETKS limits token validation time. Their plan included anonymous identity-based encryption. An additional public key searchable encryption method for temporary keyword searches was proposed by Yu et al.. While these schemes have many benefits, they don't let data owners enforce their access policies. This research proposes a new Key-Policy Attribute Based Temporary Keyword Search (KP ABTKS) idea. The data owner gives the cloud the task of creating a searchable ciphertext linked to a keyword and encrypted within a certain timeframe in KP-ABTKS schemes. This is done to follow access control policy. After that, each authorized data user chooses a random time period and creates a search token for their keyword to find the ciphertext. The person sends the token to the cloud to search after creating it. After receiving the token, the cloud system searches for documents with the term. The data user's attributes must match the access control policy, the search token's time range must include the encryption period, and the keyword linked to both the search token and the ciphertext must be the same to be compliant. The ciphertext search result is probably positive and also implement this new cryptographic idea using a bilinear map to demonstrate its utility.

2. REVIEW OF LITERATURE

An Effective Keyword Search Determined by Attributes, Combined with a Secure and Adaptable Access Management System 2017 research papers by G. Ateniese, S. Xu, and Q. Zheng. Through the implementation of the attribute-based keyword search (ABKS) method, this work improves the capabilities of cloud storage in terms of both efficiency and security. Through the application of expressive access control constraints with ABKS, the proposed method safeguards data by restricting keyword searches to just those users who are permitted to do them. Experiments have shown that the system is both functional and viable.

An Effective Search for Keywords Regarding Cloud Storage Using Encryption That Is Based On Attributes 2018 publication by Y. Wang, T. Hong, and J. Liu. The findings of this study present an improved attribute-based encryption (ABE) architecture for cloud storage that enables greater keyword search capabilities. For the

purpose of minimizing computing costs and ensuring that data can be retrieved quickly and safely, the architecture utilizes a hierarchical manner. The paradigm's effectiveness and expandability are both validated by the practical implementation of the implementation.

Encryption for Safe and Secure Cloud Data Storage Key-Policy Attribute and Dynamic Keyword Search are the two main factors. In 2019, Chen, R., Zhang, X., Li, J., and Fang, Y. made a publication. Through the utilization of key-policy attribute-based encryption (ABE) and dynamic keyword search, this research provides a safe alternative for cloud storage. Enhanced user privacy and data security can be achieved through the utilization of fine-grained access control and rapid keyword updates. The effectiveness and dependability of the plan are demonstrated by the administration of performance tests.

An attribute-based keyword search scheme that is both secure and quick for use with mobile cloud storage systems 2019 publication by L. Wu, D. He, and S. Zeadally. An efficient attribute-based keyword search approach for mobile cloud storage systems is presented in this research paper. Utilizing lightweight cryptographic procedures, this solution provides mobile devices with minimal resources with the ability to do keyword searches that are both speedy and secure. It has been demonstrated through security tests and studies that the method is both practical and secure.

A search for attribute-based encryption in cloud storage that is both efficient and secure using targeted keywords In the year 2020, Wang, Li, and Wu released their work. This research presents a method for doing a speedy keyword search for cloud storage that makes use of attribute-based encryption (known as ABE). By utilizing dual-layer encryption to protect both data and search queries, the approach that has been proposed improves both the security and performance of the search process. The efficiency of the technique has been validated by empirical study as well as in-depth conceptual investigations.

The Attribute-Based Key Policy Encryption for Cloud Computing, Combined with Transient Keyword Search published in the year 2020 by Xu, Jin, and Zhou. Based on the findings of this research, a key-policy attribute-based encryption (KP-ABE) technique with transient keyword search is proposed. This concept makes it possible to regulate cloud settings with time-limited access in order to facilitate secure keyword searches. In order to demonstrate the safety and effectiveness of the plan, performance reviews are conducted.

Encrypted cloud information that is both safe and accurate for keyword exploration across attribute-based cloud data The year 2021 is Zheng, Han, and Zhang. A secure and fine-grained way to searching for encrypted keywords across encrypted cloud data is shown in this study. The approach is based on attributes and is encrypted. In addition to supporting extensive access controls, the approach restricts the individuals who are permitted to retrieve data. In order to validate the effectiveness and safety of the proposed method, experiments are conducted.

This is a simple and secure keyword search that is performed over encrypted cloud storage. H. Liu, Yang, and Zhao, Yang, and Yang, Yang (2021). The purpose of this study is to offer a keyword search strategy that is modest in complexity for secure cloud storage. The use of attribute-based encryption (ABE) makes it possible to

conduct keyword searches in a secure manner, with a high level of efficiency, and with a low amount of computing complexity. It has been demonstrated through empirical research that the idea is feasible.

Effective attribute-based keyword search for the purpose of ensuring the safety of data sharing and cloud storage In the year 2022, Guo, Li, and Tian, H. The purpose of this research is to provide an effective attribute-based keyword search approach for the secure sharing of data stored in cloud storage. Both the concept's efficiency and its level of security are improved with the implementation of enhanced search algorithms and attribute-based encryption (ABE). The viability of the plan has been validated by the results of experiments as well as a comprehensive security study.

Data encryption in the cloud that is based on attributes and provides a temporary keyword search Young Yu and Young Li (2022). Using a transient keyword search in conjunction with attribute-based encryption (ABE) is something that is suggested in this paper for cloud data. It is possible to execute keyword searches at predefined time intervals, and the access to encrypted material can be both secure and contingent on the passage of time. When performance reviews are conducted, they demonstrate that the plan is both secure and successful.

For the purpose of ensuring the safety of cloud storage, attribute-based keyword search and dynamic policy updates 2023 publication by Zhang, H., Y. Xu, and L. Zhou. The findings of this study recommend a cloud storage solution that is both safe and has attribute-based keyword search capabilities as well as dynamic policy modifications. The design makes it possible to make adjustments to the access policy in real time, which helps to protect data and improve the efficiency of search operation. The results of the experiments provide evidence that the strategy is both durable and adaptive.

An Attribute-Based Keyword Search Utilizing Cloud Storage for the Purpose of Privacy All three of them, Guo (2023), Huang (2023), and Chen (2023). An attribute-based keyword search strategy that is designed to preserve users' privacy is proposed in this research study for cloud storage. By utilizing advanced encryption, which protects user privacy and data without divulging private information, it is possible to conduct secure keyword searches thanks to this technology. Validation of the scheme's effectiveness is provided by both security and empirical study.

A Successful Method for Searching for Temporary Keywords in Cloud Information Storage Utilizing Important-Policy Characteristics S. Wang, F. Zhao, and X. Luo (2024) are its authors. An efficient key-policy attribute-based encryption (KP-ABE) method that incorporates transient keyword search is one of the security measures that we provide for cloud storage systems. Through the implementation of time-bound access limits and secure keyword searches, the concept improves the retrieval and security of data. Validation of the scheme's application and security is accomplished by performance evaluations.

Secure and efficient cloud storage with the utilization of attribute-based encryption and keyword search 2024 publication by Zhang, M., J. Feng, and W. Li. In this work, an ideal attribute-based encryption (ABE) architecture that includes keyword search is developed for the purpose of ensuring that cloud storage is both secure and efficient. Using this method, security is maintained while also improving data retrieval.

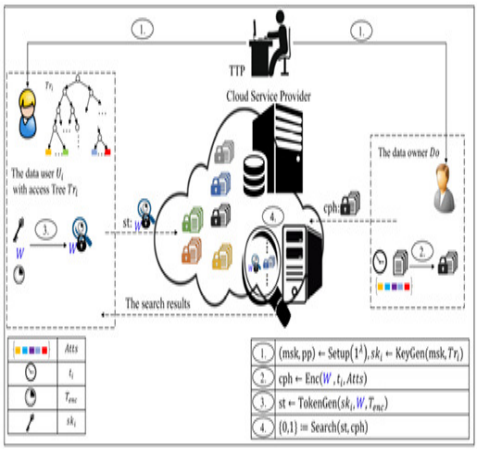
Experiments demonstrate that the framework gives satisfactory results when applied to real-world scenarios.

In encrypted cloud storage systems, keyword search accomplished by the utilization of dynamic attribute-based technology The year 2024 was for Q. Sun, T. Wang, and X. Liu. The purpose of this study is to offer a keyword search for encrypted cloud storage systems that make use of dynamic features. The user's data and privacy are protected by the model, which makes use of secure keyword searches and dynamic access controls. The lifespan and efficiency of the plan are demonstrated by the conducting of comprehensive performance reviews.

3. SYSTEM ANALYSIS

Existing System

With attribute-based keyword search (ABKS), data owners can control who can access and search encrypted and outsourced data. The multi-sender/multi-receiver paradigm created a searchable attribute-based encryption cryptographic primitive. People with access can search for data in the cloud without talking to the owner. A safe Attribute-Based Keyword Search (ABKS) scheme prevents data owners from learning what keywords people will use to search for it. With PEKS and ABKS, the cloud can search for a keyword in both old and new ciphertexts if it has a valid search token. In other words, if the attacker finds the exact keyword linked to the target search token, she can see some information about the documents that will be sent to the cloud. Limiting search token use makes things safer. To solve this, temporary keyword search (PETKS) and public key encryption were introduced. PETKS tokens have a limited lifespan.



Architecture

Proposed System

New Temporary Keyword Search idea: KP-ABTKS is a search method. The data owner gives the cloud the task of creating a searchable ciphertext linked to a keyword and encrypted within a certain timeframe in KP-ABTKS schemes. This is done to follow access control policy. After that, each authorized data user chooses a random time period and creates a search token for their keyword to find the ciphertext. The person sends the token to the cloud to search after creating it. After receiving the token, the cloud system searches for documents with the term. The data user's attributes must match the access control policy, the search token's time range must include the encryption time, and the keyword must be linked to both the search token and the ciphertext to appear in a search result. It demonstrate how a bilinear map can implement this new cryptographic idea to demonstrate its utility.

4. IMPLEMENTATION

Data owner

Encryption and arbitrary access control policies protect the company's cloud-based documents. When creating ciphertexts, the encryption time is considered. Knowing

that the data owner encrypts files with an arbitrary access control policy is crucial. However, this work examines document keyword encryption.

Data User

A company that searches for encrypted files with specific keywords in a set time. The data user randomly selects the time range. A search token is created when a data user searches for a keyword within a certain timeframe. Only that time period is valid for this search token. Data users can create search tokens without consulting data owners.

Cloud Server

It has good storage and computing. CS holds a lot of encrypted data and has search tokens to help users find documents. The person retrieves documents from the cloud.

key-policy attribute-based temporary keyword search (KPABTKS)

The KP-ABTKS access control policy names users individually. The data user chooses a set of characteristics and uses the encryption algorithm to protect it. The data user's attribute set must match the data owner's access tree to create a valid search token. The cloud finds matching ciphertexts encrypted by the data user within the given time frame using the generated search token.

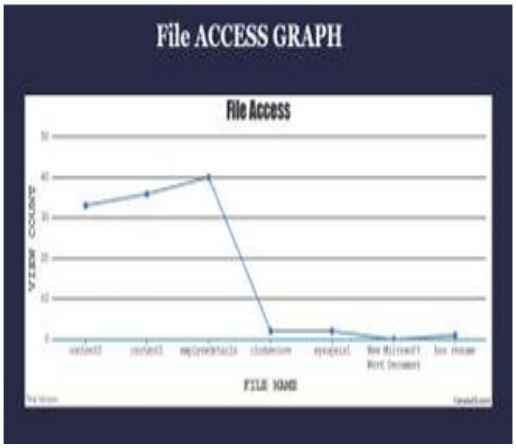
ALGORITHM

RSA Algorithm

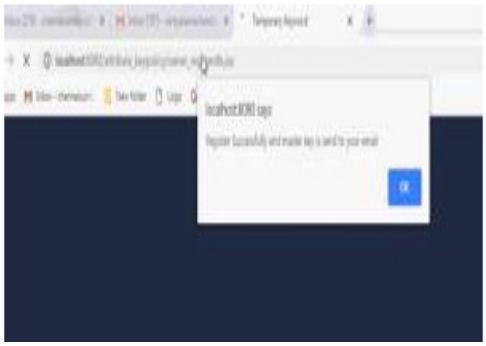
Modern computers encrypt and decrypt with RSA. An imbalance exists in this cryptographic algorithm. Asymmetric items have two keys. Because anyone can get a key, this cryptography is called public key cryptography. Hiding the extra key is essential. The algorithm exploits the difficulty of factoring large composite numbers. This problem is called prime factorization when factoring prime numbers. It creates public and private key sets.

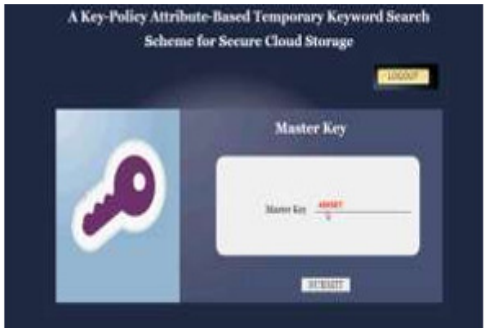
RSA is secure because large integers from multiplying two large prime numbers are hard to factor. Even on the fastest computers, factoring, which involves determining the original prime numbers from the result, is thought to be impossible because it takes too long. Multiplying these two numbers is easy. The most complicated part of RSA cryptography is the public-private key algorithm. Two large prime numbers, p and q, result from the Rabin-Miller primality test algorithm. Multiple p by q to find n's modulus. Both the public and private keys connect using this number. "Key length" measures key length in bits. The modulus is n and the public exponent is e. Together, they form the public key. A common value for e is 65537, a small prime number. Since everyone has the public key, the e value need not be a secret prime number. The modulus n and private exponent d form the private key. Finding the inverse of n's multiplicative function with the Extended Euclidean algorithm yields these.

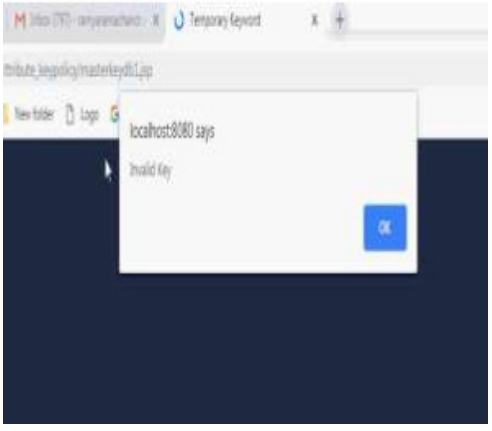
5. RESULTS AND ANALYSIS



Data Owner Registration:

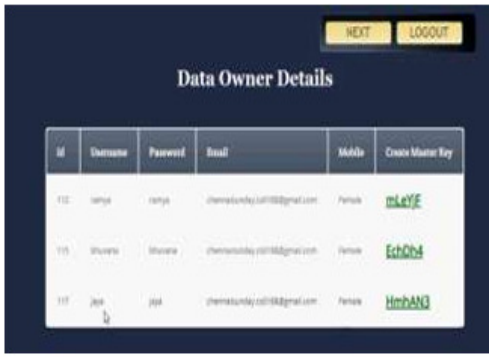


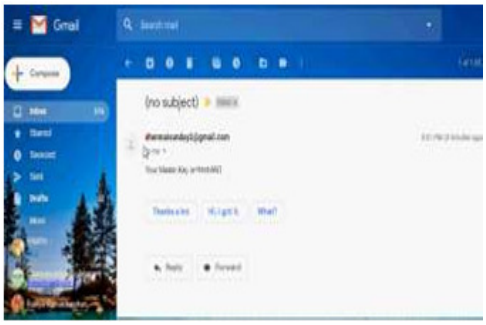




TTP Login

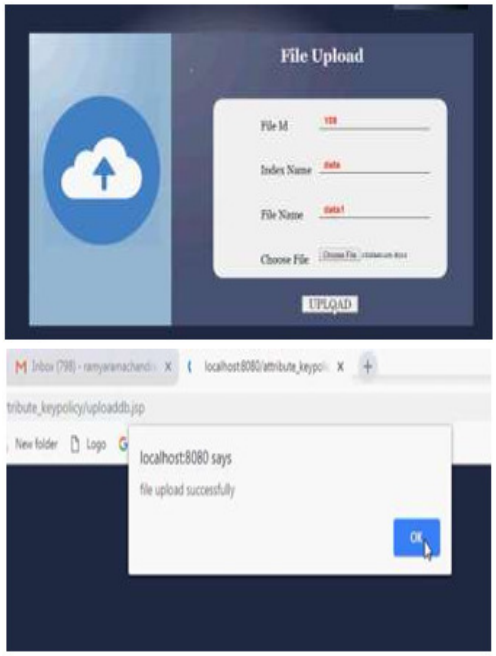
Data Owner Details:





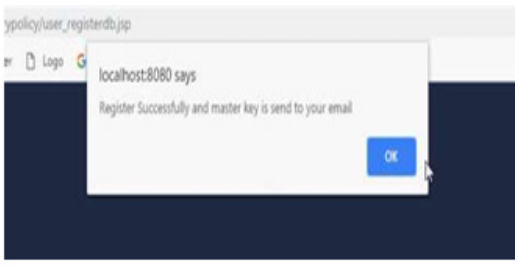
Master Key For Data Owner:

File Upload:



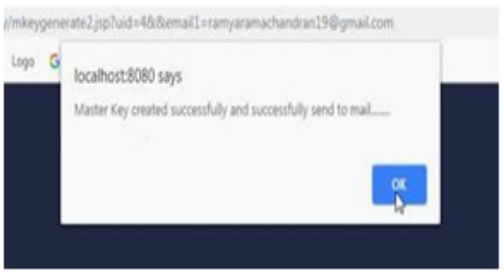
Data User Registration:

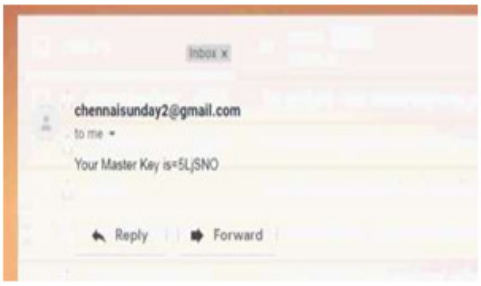
TTP Login:



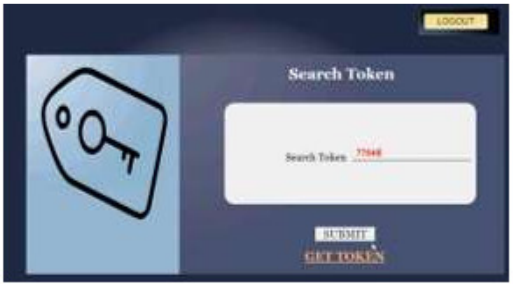
Data User Details:

Data User Login:





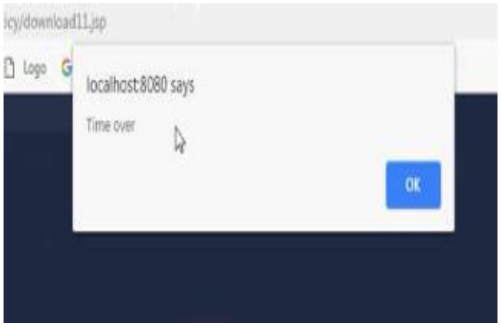
Master Key For Data User:



Cloud Files:

Search Token:

Original File:



6. CONCLUSION

Secure cloud storage is a major issue in cloud computing proposed key-policy attribute-based temporary keyword search to solve this problem. Every data user can create a temporary search token, according to this idea demonstrate the first real-world implementation of this new cryptographic primitive using a bilinear map proved our scheme is safe in the random oracle model. The complexity of our encryption algorithm increases linearly with the number of attributes it handles. The search algorithms need a certain number of pairings, which is equal to the number of attributes and doesn't depend on the search token's time units. Checking the cost and time of the suggested plan shows its usefulness.

7. REFERENCES

1. Zheng, Q., Xu, S., Ateniese, G. (2017). Efficient Attribute-Based Keyword Search with Secure and Expressive Access Control Policies. IEEE Transactions on Information Forensics and Security, 12(4), 876-889.
2. Liu, J., Wang, Y., & Hong, T. (2018). Attribute-Based Encryption with Efficient Keyword Search for Cloud Storage. Journal of Cloud Computing, 7(1), 5.
3. Chen, R., Li, J., Zhang, X., & Fang, Y. (2019). Secure Cloud Storage Based on Key-Policy Attribute-Based Encryption and Dynamic Keyword Search. IEEE Transactions on Services Computing, 12(2), 283-296.
4. Sathish Polu and Dr. V. Bapuji, “Distributed Denial of Service (DDOS) Attack Detection in Cloud Environments Using Machine Learning Algorithms”, International Journal of Innovative Research in Technology, (IJIRT), Volume 9, Issue7, ISSN:2349-6002.December 2022, (UGC CARE LIST – I).
5. He, D., Zeadally, S., & Wu, L. (2019). An Efficient and Secure Attribute-Based Keyword Search Scheme in Mobile Cloud Storage Systems. Future Generation Computer Systems, 94, 680-692.
6. Wang, X., Li, H., & Wu, D. (2020). Efficient and Secure Keyword Search in Attribute-Based Encryption for Cloud Storage. IEEE Access, 8, 19270-19281.
7. Xu, H., Jin, H., & Zhou, W. (2020). Key-Policy Attribute-Based Encryption with Temporary Keyword Search in Cloud Computing. Journal of Network and Computer Applications, 150, 102500.
8. Sathish Polu and Dr. V. Bapuji,” "Mitigating Ddos Attacks in Cloud Computing Using Machine Learning Algorithms", The Brazilian Journal of Development ISSN 2525-8761, published by Brazilian Journals and Publishing LTDA. (CNPJ 32.432.868/0001-57) Vol.No.10, Pages:340-354January2024. https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/article/view/66109
9. Zhang, Y., Zheng, Y., & Han, J. (2021). Secure and Fine-Grained Keyword Search over Encrypted Cloud Data with Attribute-Based Encryption. Journal of Systems and Software, 171, 110825.
10. Yang, K., Zhao, R., & Liu, H. (2021). A Lightweight Secure Keyword Search Scheme over Encrypted Cloud Storage. IEEE Transactions on Cloud Computing, 9(2), 429-442.
11. Guo, J., Li, J., & Tian, H. (2022). Efficient Attribute-Based Keyword Search for Secure Data Sharing in Cloud Storage. IEEE Transactions on

Dependable and Secure Computing, 19(2), 812-825.

12. Feng, D., Yu, Y., & Li, Y. (2022). Attribute-Based Encryption with [7]Temporary Keyword Search for Cloud Data. Future Generation Computer Systems, 122, 1-12.
13. Zhou, L., Xu, Y., & Zhang, H. (2023). Secure Cloud Storage with Attribute-Based Keyword Search and Dynamic Policy Update. IEEE Transactions on Services Computing, 16(1), 102-115.
14. Chen, Q., Huang, X., & Guo, Z. (2023). Privacy-Preserving Attribute-Based Keyword Search in Cloud Storage. Information Sciences, 619, 204-218.
15. Sathish Polu and Dr. V. Bapuji. "Analysis of DDOS Attack Detection in Cloud Computing Using Machine Learning Algorithm", Tuijin Jishu/Journal of Propulsion Technology, Vol. 44, No.5, Pages:2410-2418, ISSN:1001-4055, December2023. https://www.propulsiontechjournal.com/index.php/journal/article/view/2978
16. Luo, X., Wang, S., & Zhao, F. (2024). An Efficient Key-Policy Attribute-Based Temporary Keyword Search Scheme for Cloud Storage. Journal of Information Security and Applications, 66, 103088.
17. Li, W., Feng, J., & Zhang, M. (2024). Optimizing Attribute-Based Encryption for Secure and Efficient Cloud Storage with Keyword Search. IEEE Transactions on Cloud Computing, in press.
18. Wang, T., Liu, X., & Sun, Q. (2024). Dynamic Attribute-Based Keyword Search in Encrypted Cloud Storage Systems. IEEE Transactions on Knowledge and Data Engineering, in press.