Enhanced Attribute-Based Encryption with Forward Security for Cloud Assisted IOT

Ms.P.Priya[1], Dr.D.Maya[2], Mr.G.Rajamuneeswaran[3]
[1]*II –M.E Computer Science Engineering, Kangeyam Institute of Technology, Kangeyam.*
[2]*Associate Professor, Department of Computer Science Engineering, Kangeyam Institute of Technology, Kangeyam.*
[3]*Assistant Professor, Department of Computer Science Engineering, Kangeyam Institute of Technology, Kangeyam.*

Abstract: **When cloud computing first emerged, data owners were encouraged to move their intricate data management systems from local locations to commercial public clouds to save money and gain greater flexibility. However, to preserve data privacy, sensitive information must be encrypted prior to outsourcing, rendering conventional data utilization based on an outdated plaintext keyword search. Thus is crucial to enable an encrypted cloud data search service. To meet the need for effective data retrieval, the search engine must support multi-keyword queries and offer result similarity ratings, particularly given the vast number of data users and documents in the cloud. Search results are rarely differentiated in related works on searchable encryption, which concentrate on single-term or Boolean keyword searches. In this study, we define and solve the difficult problem of privacy-preserving multi-keyword ranked ontology keyword mapping and search over encrypted cloud data (EARM) for the first time. A loosely connected and expressive communication method for large-scale distributed systems is content-based publishing/subscribing.**

Through the use of Bloom filters and basic randomization techniques, this process lowers the cost of encrypted matching. Provide a thorough security analysis of the data that Bloom filters in this instance released, along with confinement obfuscation approaches. Among the many multi-keyword semantics, we select the effective "Enhanced Association Rule Mining coordinate matching" principle, which states that the goal is to capture as many matches as possible between the search query and the data documents. We then use "inner product similarity" to quantitatively formalize this principle for measuring similarity. After introducing a simple EARM system that uses safe inner product computing, we greatly enhance it to satisfy various privacy needs in two threat model tiers.

Index Terms**: Attribute-Based Encryption, Forward Security, Puncturable Encryption, Searchable Encryption.**

I. INTRODUCTION

In cloud-assisted Internet of Things (IoT) systems, attribute-based searchable encryption (ABSE) with forward security is a potent method for guaranteeing data privacy and safe access. Large volumes of sensitive data are produced by IoT devices and are frequently stored on the cloud; therefore, it is crucial to secure this data while allowing for effective search capabilities. ABSE makes it possible to encrypt and store data according to particular characteristics, including device kind, user role, or location, so that only authorized users who possess the corresponding characteristics can access and search the data. Since fresh data utilises updated keys, forward security further improves protection by guaranteeing that previously encrypted data is safe even in the event that encryption keys are compromised. This method is perfect for applications like smart cities, healthcare, and industrial IoT where data privacy and controlled access are crucial since it not only shields IoT data from unwanted access but also makes safe, effective data retrieval possible.

1.1 ATTRIBUTE-BASED ENCRYPTION

The encryption method known as attribute-based encryption (ABE) limits access to data by using qualities or traits rather than unique identities. By defining encryption policies based on particular characteristics, such a user's role, location, or department, ABE allows for a more adaptable and precise access control model. ABE can be divided into two primary categories: Ciphertext-Policy ABE (CP-ABE), in which the data is encrypted using an access policy and the users' keys are linked to attributes, and Key-Policy ABE (KP-ABE), in which the decryption keys are tied to access structures while the data is encrypted using attributes too. The data

can be securely shared among groups while strict control over who can access it is maintained since only users with matching attributes or access policies can decode the data. This makes ABE especially appropriate for cloud computing, distributed systems, and Internet of Things settings where regulated access and data protection are critical.

1.2 PUNCTURABLE ENCRYPTION

Puncturable encryption is a cryptographic technology that offers increased security and flexibility by enabling users to "puncture" or disable particular decryption capabilities in a controlled manner. The way this method operates is by changing the decryption keys so that they are still valid for everything but the designated "punctured" messages or ciphertexts, which are not decryptable. For instance, if a key is punctured for a certain message or keyword, it can still decrypt all other encrypted data but is rendered useless for that one instance. Puncturable encryption is useful in situations like revocable access control, forward security, and real-time data privacy management because of its capacity for selective limitation. It is especially helpful in settings like cloud storage, the Internet of Things, and secure messaging since it keeps data safe even in the event that certain decryption keys are stolen or when access needs to be dynamically cancelled without re-encrypting all of the data.

1.3 SEARCHABLE ENCRYPTION

Searchable encryption is a cryptographic approach that preserves data privacy while facilitating effective querying by allowing users to search over encrypted material without decrypting it. Searchable encryption systems encrypt data and store it on a distant server (like the cloud), allowing users to conduct searches using properly constructed encrypted queries. Public-key searchable encryption (PEKS), which permits searches over data encrypted with a public key, and symmetric searchable encryption (SSE), which uses the same key for both encryption and search, are the two primary varieties. In order to return encrypted results that are only decryptable by authorized users, the server immediately executes search requests on the encrypted data. In data-sensitive industries like healthcare, finance, and law enforcement, searchable encryption is particularly useful because it allows businesses to use the cloud's storage and processing capacity without disclosing private information, guaranteeing adherence to data privacy laws and preserving security even when data storage is outsourced.

1.4 FORWARD SECURITY

A security feature called forward security, sometimes referred to as complete forward secrecy, makes guarantee that encrypted data is safe even in the event that the encryption keys are later stolen. Forward-secure systems rotate or update their encryption keys on a regular basis, making it impossible to decrypt previous communications even in the event that an attacker manages to gain the current or future encryption keys. This limits the possible harm of a key breach to only recent data and not to previously encrypted information because each time data is encrypted, it depends on a distinct key that cannot be used in the past. In sensitive applications where data confidentiality over time is critical, such as cloud storage, encrypted communications, and the Internet of Things, forward security is especially important. Forward security increases overall data resilience against future risks by guaranteeing that attackers cannot access prior data, even in the case of key leakage.

II. LITERATURE REVIEW

Let us consider the following scenario: a user U wishes to save his files on a remote file server S in an encrypted format. Later on, user U wishes to quickly recover some of the encrypted files that include particular keywords while maintaining the confidentiality of the keywords and avoiding jeopardizing the security of the data that are stored remotely. For instance, a user may choose to save encrypted old emails on a server run by Yahoo or another major provider. Later, while travelling with a mobile device, the user may want to access specific emails. There are solutions to this issue under clearly stated security criteria in [2]. Due to the lack of a public-key cryptosystem, the techniques are effective. The strategy does not depend on the encryption technology used for the distant data, in fact. Additionally, they are incremental. The user U can upload new files there that are searchable against future enquiries but secure against past queries. From this, the primary idea is to store data on a different server and access it remotely using a laptop, mobile device, etc.

Even though there are obvious advantages to employing a public cloud infrastructure, there are also serious security and privacy issues. In fact, worries about data integrity and confidentiality appear to be the main barrier to the widespread use of cloud storage (and cloud computing in general). [3] gives a summary of the advantages of a cryptographic storage service, such as lowering legal risk for cloud providers and consumers and attaining regulatory compliance. In addition, a brief description of cloud services like safe backups, archival, health record systems, secure data interchange, and e-discovery that could be developed on top of a cryptographic storage service is given.

On the one hand, users who may not be familiar with the encrypted cloud data must post-process each file that is retrieved to identify the one that most closely matches their interests; on the other hand, retrieving every file that contains the requested keyword consistently results in extra network traffic, which is completely undesirable in the pay-as-you-use cloud paradigm of today. In this study, the problem of efficient yet safe ranked keyword search over encrypted cloud data has been defined and resolved [4]. By returning the matching files in a ranked order based on specific relevance criteria (such as keyword frequency), ranked ontology keyword mapping and search significantly improves system usability and moves the implementation of privacy-preserving data hosting services in cloud computing closer to reality. The work defines and resolves the difficult problem of privacy-preserving multi-keyword ranked ontology keyword mapping and search over encrypted cloud data (EARM) for the first time. It also lays out a stringent set of privacy requirements that must be met in order for such a secure cloud data utilisation system to be implemented.

Formalizing and resolving the issue of efficient fuzzy keyword search over encrypted cloud data while preserving keyword privacy is the primary goal of this work [7]. Our suggested method uses this fundamental concept, but it is for multi-keyword raking search (EARM scheme). [8] suggests a secure cloud storage service design that solves the reliability problem while offering nearly ideal overall performance.

The issue of access control in cloud computing is still unsolved: how to simultaneously achieve fine grandness, scalability, and data confidentiality? The work [9] tackles this difficult open problem by allowing the data owner to assign the majority of the computation tasks required for fine-grained data access control to untrusted cloud servers without revealing the underlying data contents, while also defining and enforcing access policies based on data attributes. The authors of [10] have suggested a public auditing method that protects privacy for the security of data storage in cloud computing schemes. It makes use of random masking and the homomorphic linear authenticator to ensure that the TPA will not discover anything about the data content on the cloud server during the effective auditing process. This relieves cloud users of the burden of the time-consuming and potentially costly auditing task and also allays their concerns about the leakage of their outsourced data.

III. EXISITING SYSTEM

The fine-grained access structure and keyword retrieval ability of Cypher text-Policy Attribute-Based Searchable Encryption (CP-ABSE) make it one of the best encryption methods for cloud environments. However, ensuring the forward security of cloud data that is outsourced and safely erasing data that is no longer required without depending on the cloud are difficult issues in CP-ABSE programs. In order to address these issues, we suggest a Puncturable CP-ABSE (Pun CP-ABSE) method that uses a fine-grained access structure and a searching mechanism to provide self-controlled data deletion. To complete the data destruction, the data owner opens the trapdoor. The deletion procedure can thereby ensure forward security without requiring communication with a reliable third party. The cloud server can no longer look for the matching ciphertext after the punctuation. Additionally, we demonstrate that the Pun-CP-ABSE scheme is safe from the Chosen-Keyword Attack (CKA) and the Chosen-Plaintext Attack (CPA). To demonstrate the effectiveness and viability of the Pun-CP-ABSE plan, we have also put it into practice.

IV. PROPOSED SYSTEM

We identify and resolve the difficult privacy-preserving multi-keyword ranked ontology keyword mapping and search over encrypted cloud data (EARM) problem and develop a set of stringent privacy requirements to make such a safe cloud data utilization system a reality. Out of several multi-

keyword semantics, we opt for the effective "coordinate matching" principle. We present the Secured Multi-Keyword Search (SMS) over Encrypted Cloud Data (ECD) problem and develop a set of privacy rules for this type of safe cloud data use system. From a variety of multi-keyword semantics, we choose the most effective rule of coordinate matching—that is, as many matches as possible—to determine how similar the search query and the data are. For additional matching, we use inner data correspondence to quantitatively formalize this similarity measurement principle. In order to satisfy various privacy needs, we first provide a simple Secured multi-keyword ranking ontology keyword mapping and search strategy employing safe inner product computation. The top k retrieval results are shown in the Ranked result. Additionally, when an unauthorized person attempts to access data from the cloud, we suggest an alert system that will send out messages and emails.

V. MODULE DESCRIPTIONS

5.1 CLOUD SETUP MODULE:

Instead of giving undifferentiated results, this module improves the schemes that enable multi-keyword queries and offer result similarity rating for efficient data retrieval. Privacy-Preserving: To maintain privacy and stop the cloud server from picking up extra information from the dataset and index. Efficiency: Minimal communication overhead and processing overhead are required to meet the aforementioned privacy and functionality constraints.

5.2 EARM COORDINATE MATCHING:

"Coordinate matching" is an intermediate similarity metric that quantifies the document's relevance to the query by counting the number of query keywords that appears in the content. When users specify which subset of the dataset they want to recover, Boolean queries successfully match the user's specified search requirement. Users can more easily find a list of keywords that express their concern and retrieve the most pertinent papers in a rank order.

Data privacy: To successfully prevent the cloud server from accessing the outsourced data, the data owner can use classic symmetric key cryptography to encrypt the data prior to outsourcing.

Index privacy, in the event that the cloud server deduces any correlation between encrypted documents and keywords from the index. Thus, it is necessary to create a searchable index to stop the cloud server from executing this type of association attack.

Keyword Privacy: The most important thing is to conceal what users are searching for, i.e., the terms that the corresponding trapdoor specifies, since most users do not want their search results to be visible to others, such as the cloud server. It is possible to create the trapdoor using cryptography to safeguard the query keywords.

5.3 PREFILTERING AND SECURITY MANAGEMENT MODULE:

With the use of this module, the user can obtain precise results based on a variety of keyword concepts. After searching that word file in our database, the server will break the user's multiple-word query into a single word. Lastly, the user retrieves the file from the database's matched word list after prefiltering it. Another way to represent the search query is as a binary vector association rule, where each bit indicates whether or not the relevant keyword appears in the request. An accurate way to measure similarity would be to take the inner product of the query vector and the data vector.

Encrypt Module: This module aids the server with encrypting the document using the TRIPLE DES Algorithm, converting it to a Zip file containing an activation code, and sending the user the code to download.

Client Module: Based on the user query, this module assists the client in searching the file utilising the idea of multiple key phrases and obtains an accurate result list. Before entering the activation code, the user must choose the necessary file, register their information, and get an activation code via email from the "customerservice404" email. The user can then download and extract the Zip file.

Module with several keywords:

With the use of this module, the user can obtain precise results based on a variety of keyword concepts. After searching that word file in our database, the server will break the user's multiple-word query into a single word. Lastly, show the database's matched word list, and the user can select the file from it. Another way to define the search query is as a binary vector, where each bit indicates whether a related keyword appears in the request.

This allows the inner product of the query vector and the data vector to precisely assess the similarity. However, it will be against index or search privacy to directly outsource data or query vectors. Based on a secure k-nearest neighbour (kNN) technique, we propose a basic SMS scheme that uses secure inner product computation to address the challenge of supporting such multi-keyword semantic without compromising privacy. We then gradually enhance it to meet different privacy requirements in two levels of threat models.

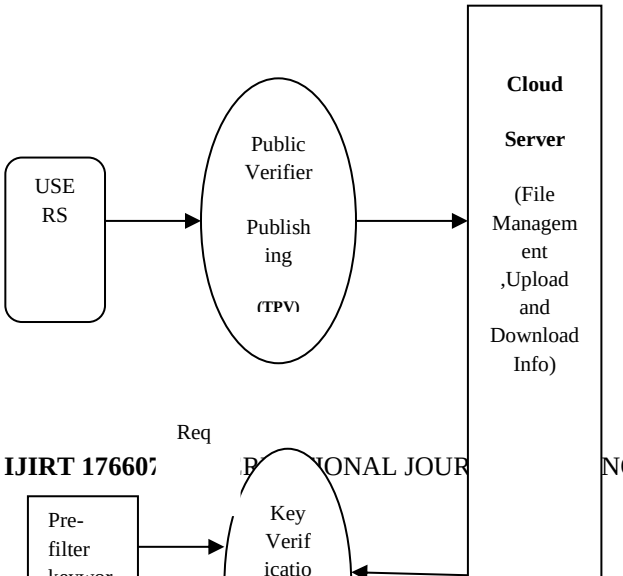
1) Illustrating the Secure Multi-Keyword Search issue with encrypted cloud data

2) Provide two systems that adhere to the inner product similarity and coordinate matching principles.

Admin Module: This module aids the server in viewing information and securely uploading files. The admin logs in using the log key. Change the log key prior to the admin logout. After logging in, the administrator can check the user's downloading information and the number of file request details on the flowchart, as well as change the password. Following the Zip file format conversion, the administrator can upload the file.File upload Module: This module aids the server in viewing information and securely uploading files. The admin logs in using the log key. Change the log key prior to the admin logout. After logging in, the administrator can check the user's downloading information and the number of file request details on the flowchart, as well as change the password. Following the Zip file format conversion, the administrator can upload the file.

Ranking Outcome: The k-nearest neighbour technique is used to rank the data according to user requests. The "coordinate matching" technique is applied for ranking. The user receives the anticipated query results after ranking.

VI. RESULT ANALYSIS



The suggested method successfully integrates coordinate matching for similarity ranking and safe inner product computation to meet the difficulties of privacy-preserving multi-keyword search over encrypted cloud data. Symmetric key cryptography safeguards data privacy, while custom-built indexes defend against inference attacks, protecting the private of both keywords and indexes. Users can obtain the most pertinent results while protecting their privacy because to the system's efficient multi-keyword query processing and low computational overhead. The use of ZIP file encryption provides an additional layer of data protection, and the incorporation of an alarm mechanism for unauthorized access reinforces security. All things considered, the system offers a safe, scalable, and effective way to search for encrypted cloud data with strong privacy protections and precise result ranking.

Algorithm	Accuracy
Existing	65
Proposed	80

Table 1. Comparison table

Figure 1. Comparison graph

One of the most widely used metrics for assessing classification performance is accuracy, which is calculated as the ratio of correctly segmented samples to all samples.

Accuracy = TP/ (TP+ FN)

Precision: The number of positive class predictions that truly belong to the positive class is quantified by precision, which is estimated in the manner described below.

Precision = TP / (TP + FP)

The ratio of true positives to total (real) positives in the data is known as recall or sensitivity. Sensitivity and recall are synonymous.

Recall = TP / (TP + FN)

The ratio of genuine negatives to total negatives in the data is known as specificity. Specificity is the program's accurate designation for everyone who is actually healthy.

Specificity = TN / (TN + FP)

VII. CONCLUSION

In this work, we design and solve the multi-keyword ranked ontology keyword mapping and search over encrypted cloud data problem for the first time, and we set certain privacy constraints. We select the efficient principle of "coordinate matching," which means as many matches as possible, from a variety of multi-keyword semantics to capture similarity between query keywords and outsourced documents. We then use "inner product similarity" to quantitatively formalize this principle for measuring similarity.

In order to address the problem of enabling multi-keyword semantics without compromising privacy, we first suggest a simple EARM approach that makes use of safe inner product computation. We then greatly enhance it to meet privacy requirements in two threat model levels. A detailed examination of the privacy and efficiency guarantees of the suggested schemes is provided, and tests on the real-world dataset demonstrate that our suggested schemes have little computational and communication overhead. Future research will include ensuring privacy in a more robust threat model, integrity checking of rank order in search results, and providing additional multi-keyword semantics (such as weighted queries) over encrypted data.

VIII. FUTURE WORK

Future improvements to the system could include the addition of more sophisticated encryption methods, including blockchain-based access control or homomorphic encryption, to further improve data security and integrity. Data retrieval can become more flexible and intelligent by expanding the search process to include natural language queries and fuzzy keyword search. Incorporating machine learning models can also enhance the relevance and accuracy of ranked search results by taking into account user behavior and query history. Automated reaction mechanisms and real-time danger identification are potential additions to the alert system. Enhancing accessibility and scalability may also involve cross-cloud interoperability and support for mobile platforms. These improvements will increase the system's resilience, intelligence, and flexibility in response to changing user requirements and new security threats in cloud computing settings.

IX. REFERENCES

[1] "A break in the clouds: towards a cloud definition," ACM SIGCOMM Comput. Commun. Rev., vol. 39, no. 1, pp. 50–55, 2020 L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner.

[2] S. Kamara and K. Lauter discuss "Cryptographic cloud storage." Springer, Heidelberg.In RLCPS, January 2021 LNCS.

[3] A. Singhal, "A quick introduction of modern information retrieval," IEEE Data Engineering Bulletin, issue 4, pages 35–43, 2021.

[4] A. Moffat, T. C. Bell, and I. H. Witten, "Managing gigabytes: Compressing and indexing documents and images," May 2020, Morgan Kaufmann Publishing, San Francisco.

[5] D. Song, D. Wagner, and A. Perrig, "Practical approaches for searches on encrypted data"Proc. of S&P, 2021;
[6] Goh, E.-J., "Trustworthy indexes," Cryptology ePrint Archive, 2021, http://eprint.iacr.org/2003/216.
[7] "Privacy preserving keyword searches on remote encrypted data," in Proceedings of the American Computer Network, 2021, by Y.-C. Chang and M. Mitzenmacher.
[8] R.Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky published "Searchable symmetric encryption: better definitions and efficient constructions."In the Proc. of ACM CCS, 2020.
[9] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Keyword search for public key encryption," in Proceedings of EUROCRYPT, 2021.
[10] "Deterministic and efficiently searchable encryption" by M. Bellare, A. Boldyreva, and ONeill, in Proceedings of Cryptography, 2021.