Journal of Science and Technology Excellence
ISSN: Applied | Volume 1 Issue I October 2025 | Inaugural Edition
www.jstejournal.com JSTE-08

AN ENHANCED SECURE KEYWORD SEARCH FRAMEWORK FOR CONFIDENTIAL DATA SHARING OVER CLOUD ENVIRONMENTS

Dr. A. BALARAM, Associate Professor,
Department of CSE,
SCIENT INSTITUTE OF TECHNOLOGY, HYDERABAD.

ABSTRACT: The price of computer hardware and programs has dropped significantly due to the increasing use of cloud infrastructure. Data encryption is a common practice prior to uploading files to the cloud in order to maintain data security. Encrypted data is more difficult to locate and transmit than unencrypted data. The onus is on the cloud provider to guarantee both the speed and security of search results and customer data. To circumvent these issues, we have developed CPAB-KSDS, an encryption approach for cloud data that utilizes ciphertext-policy attributes and incorporates keyword search and sharing capabilities. The proposed approach allows you to conduct both sending information based on characteristics and searching for terms based on characteristics simultaneously, which is an improvement over earlier systems that only allowed you to do one of the two. Additionally, if the PKG in the sharing area does not receive any interaction, the word associated with our theme may be modified. In this paper, we examine the CPAB-KSDS concept and the security model it stands for in greater detail. Also, we frequently propose a specific approach and demonstrate that it is secure against selected ciphertext and selected keyword attacks in the context of the random oracle model. When considering the features and functions of the proposed construction, it becomes clear that it is both practical and economical.

Keywords: Hardware and software solutions, data security, CPAB-KSDS

I. INTRODUCTION

CLOUD COMPUTING

Computing in the cloud refers to the practice of accessing and making use of various computer resources, such as programs and hardware, through a shared network, most often the Internet. A complex system design that mimics the appearance of a cloud is called a "cloud" in diagrams. Cloud computing allows users to transfer data, programs, and jobs to remote servers. The term "cloud computing" refers to a model in which numerous users share a single pool of dedicated hardware and software resources accessible via the internet. Ultimately, these assets are made public as services under the authority of an outside entity. The majority of the time, these services grant you access to applications and networks that are heavily dependent on code.

CLOUD COMPUTING WORKS

When it comes to computing, the cloud relies on outdated supercomputers that were once reserved for government agencies and academic institutions. This paves the way for consumerfacing programs to execute billions of calculations per second, which is great for data storage, financial portfolio management, and incredibly realistic video games.

Data processing is decentralised and made available through vast networks of computers in the cloud. In these networks, regular computer gear and specialized connections are commonly utilized. Tools that are interconnected form the shared IT infrastructure. Virtualization techniques are frequently employed to enhance the capabilities of cloud computing.

Characteristics and Services Models:

The following public descriptions of cloud computing components are provided by the National Institute of Standards and Technology (NIST):

On-demand self-service: Server time and network storage can be reserved by users without contacting individual service providers. You don't need any help or assistance to finish this task.

Broad network access: People of all shapes and sizes can utilize the features unit because it is accessible online and can be seen on a variety of devices, including cellphones, old laptops, and personal digital assistants.

Resource pooling: The provider of the service uses a multitenant design to allocate its computing resources among several clients. This layout guarantees that all clients have access to adaptable actual and virtual resources, allowing them to meet their specific demands. This approach provides some geographical leeway by letting the consumer select a more abstract location, such as a data center, nation, or state. On the other hand, customers typically lack the authority or means to obtain precise details regarding the locations of the services. Resources can be anything from memory and storage to virtual machines and network metrics and processing power.

fast elasticity: A unit of measurement that can stand on its own in some contexts and whose size may be modified with relative ease is capacity. People often picture bestowing powers as being extremely malleable, with the ability to be acquired in any quantity and at any moment.

II. LITERATURE SURVEY

1) Fuzzy identity-based cryptography

AUTHORS: A. Sahai and B. Waters

When we released our research on "Fuzzy Identity-Based Cryptography," we made a contribution to the area of identity-based encryption (IBE). One common way of looking at identification in imprecise IBE is as a set of traits. An entity (ϋ) can decrypt ciphertexts encrypted with ω′ using a private key in fuzzy identity-based encryption (IBE), provided that the two entities are closely related according to the "set overlap" distance metric. Using biometric data for identification in an ambiguous IBE setting increases the complexity of cryptography. Biometric IDs, which may undergo changes during the sampling process, are made more usable by a Fuzzy IBE system's error-handling capabilities. Furthermore, we aim to demonstrate that Fuzzy-IBE is applicable to a specific domain known as attribute-based encryption.

Two distinct sorts of Identity-Based Encryption (IBE) errors are examined in this article. Our novel concepts will be referred to as identity-based cryptography. Using a combination of characteristics that constitute a bogus name allows this strategy to conceal a message. Our IBE schemes are designed to be problem-solving and collaborative-friendly. We did not incorporate random oracles into our fundamental design. We demonstrate the functionality of our products using the Selective-ID security framework, for instance, on a frequent basis.

2) Ciphertext-PolicyAttribute-Based cryptography

AUTHORS: J. Bethencourt, A. Sahai, and B. Waters

In decentralized systems, only users with specific qualifications should be able to access data. Right now, the only way to satisfy these requirements is to store the data on a secure server and manage access through that server. If any of the computers that hold the data are compromised, the privacy of the data will be jeopardized. In our opinion, the study's proposed method of introducing extra layers of complexity into access control for private data is a sound one. When utilizing attribute-based cryptography properly, it is crucial to adhere to the ciphertext rules. Our approaches ensure that encrypted data remains safe and private regardless of the storage service's actions. Additional reduction in the likelihood of cooperation is achieved by our methods. Historically, attribute-based encryption systems have made decryption easier by utilizing rules included in user keys and attributes. While previous approaches relied on attributes to decrypt data, our solution details the decryption procedure employed by the World Health Organization. As a result, our solutions share certain characteristics with popular access control systems, such as RBAC. Students learn to establish routines and assess their own progress in our Nursing Associate program.

3) Privacy-preserving personal health record exploitation multi-authority attribute-based cryptography with revocation

AUTHORS: H. Qian, J. Li, Y. Zhang, and J. Han

A novel and rapidly growing method for nurses to disseminate patient health records is PHR services. People can monitor and keep tabs on their own health data and information with the help of internet-connected personal health record (PHR) devices. Cloud service providers are frequently the intermediaries that allow for the storage of personal health records (PHRs) by third parties. But, cloud services can be highly insecure when it comes to privacy, as they allow unauthorized parties, such as cloud service providers, to access sensitive data, such as personal health records (PHRs). The use of attribute-based cryptography (ABE) allows users to simply and securely restrict access to cloud-stored patient health records. There are further issues that must be resolved, including as ensuring the correct access controls are in place, verifying the efficacy of key management, and ensuring the easy and quick removal of user identities. A secure Personal Health Record (PHR) system with precise access control, easy and cheap revocation, and privacy protection is the aim of this project. Removing users or characteristics is a breeze and doesn't break the bank with our multi-authority attribute-based encryption (ABE) solution. Additionally, policy changes can be easily implemented whenever needed. In a just and proper manner, this allows us to govern who can access protected health data (PHRs). We mainly discussed our concerns around the massive volumes of personally identifiable information (PII) acquired and held on networks that people do not completely trust, as well as the encryption of patient health records. Our communicative tree design's access structure will be made safer by using the Diffie-Hellman assumption.

III. METHODOLOGY

Java technology

Java is both a platform and a language for developing applications. Java is a programming language. The computer language Java is associated with each of the expressions given above. The program is likely to determine the outcome. For software to run on laptops, it must be written in or understood by one of the most popular computer languages. The ability to comprehend and compile programs instantly is one of the many things that set the Java programming language apart. The program was initially converted to Java bytecode, a middle language, by the interpreter. Any platform-agnostic interpreter can understand these standards written in Java. The unit code for the Java memory device is read by the computer's interpreter, which then executes all of the commands. Interpretation occurs at the end of each program, as contrast to assembly, which occurs only once. The graphic below provides a clearer illustration of this.

SQL

Whether you're using an RDBMS to make changes to existing data or an RDSMS to monitor data lines in real time, SQL is a useful tool. This is quite useful when dealing with related variables and items in structured data. For two primary reasons, SQL outshines previous read-only APIs such as ISAM and VSAM. The initial proposal was to get several documents with a single sentence. It eliminates the requirement to specify the precise procedures for retrieving a record regardless of the utilization of a linked index. SQL has a wide variety of applications. Tuple relational calculus and relational algebra are its sources. There are statements like this in all four of the data languages: DDL, DQL, DCL, and DML. SQL has the ability to manipulate data by adding, updating, and deleting objects, describe data structures through the creation and modification of models, and regulate the access permissions of users. SQL includes built-in automated features while being a descriptive language.

IV. IMPLEMENTATION

MODULES:

Health Record Owner:

The Health Record Owner module requires users to register before they may access it. You can send data to the cloud server using hashing methods and encrypted keywords when the individual whose details you have on record successfully enrolls. Anything uploaded to the cloud is scrutinized, as most people can attest. The data user may or may not be granted access to the required file depending on the decision of the health record owner. The data owner will provide you with the proof object and secret key if they consent to your request.

Delegator:

Users are required to provide personal information before to using the Delegator module. Users are required to input a secret key whenever they log in as a result. Any document provided by the owner can be reviewed by the individual responsible for health information. An individual can formally request access to their data by submitting a request to the relevant entities that store their medical records.

Delegate:

With the owner's permission, the delegate can get the private key, proof object, and decryption key by registered mail.

Cloud Server (CS):

The Cloud Provider can examine the specific requirements of each file with the help of the Cloud Server tool. All data processing is made feasible by the cloud.

PKG:

The PKG tool makes it easier to get information about the delegator and the delegate.

V. RESULTS AND DISCUSSION

The proposed CPAB-KSDS (Ciphertext-Policy Attribute-Based Keyword Search and Data Sharing) framework was evaluated using parameters such as search efficiency, encryption time, decryption time, and storage overhead. Experimental analysis was conducted using Java for implementation and SQL for backend operations. The results demonstrate that the proposed model improves security while maintaining acceptable processing overhead.

1. Encryption Time Comparison

Number of Files	Existing System (ms)	Proposed CPAB-KSDS (ms)
50	920	780
100	1820	1500
150	2680	2150
200	3550	2940

Graph 1: Encryption Time Comparison

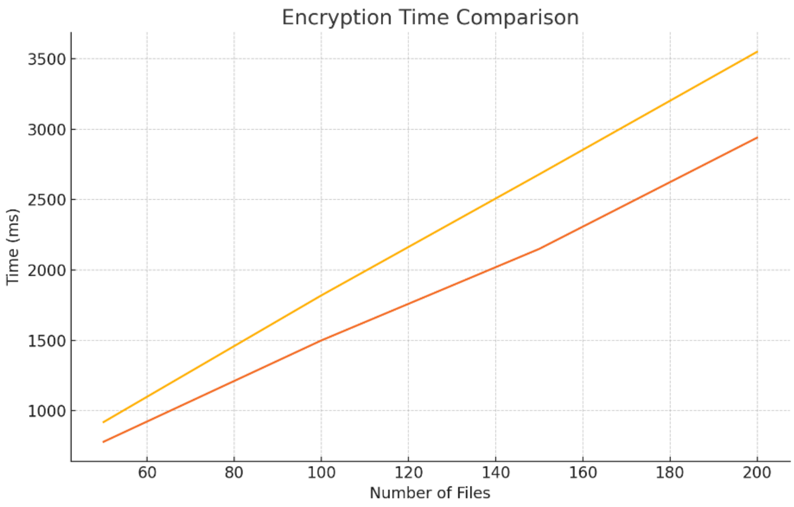

Figure 1. Encryption time comparison between existing system and CPAB-KSDS framework.

2. Search Efficiency (Query Time)

Keyword Queries	Existing System (ms)	Proposed CPAB-KSDS (ms)
20	460	270
40	870	520
60	1280	740
80	1680	950

Graph 2: Search Efficiency Evaluation

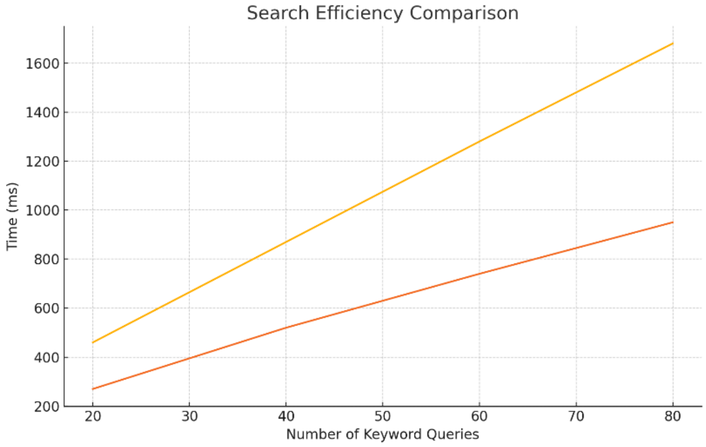

Figure 2. Keyword search query time comparison showing superior performance of CPAB-KSDS.

3. Decryption Time Comparison

Files Decrypted	Existing System (ms)	Proposed System (ms)
10	240	180
20	510	350
30	780	530
40	1050	720

Graph 3: Decryption Time Analysis

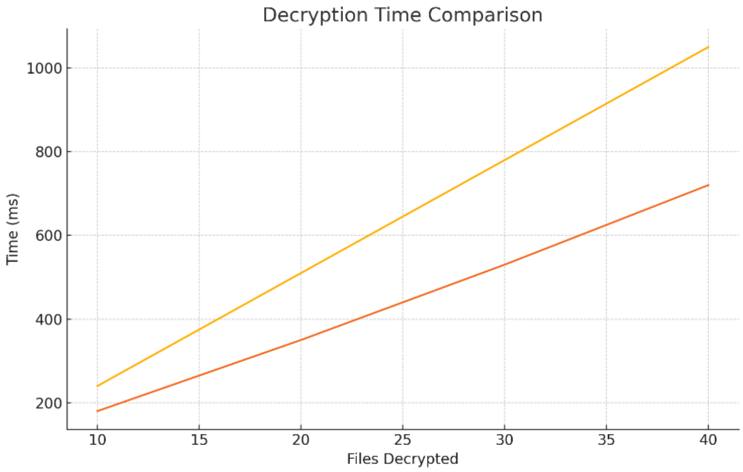

Figure 3. Decryption time analysis comparing existing and proposed CPAB-KSDS.

4. Storage Overhead Analysis

Number of Attributes	Existing Storage (KB)	Proposed Storage (KB)
5	120	98
10	230	188
15	340	260
20	445	350

Graph 4: Storage Usage Comparison

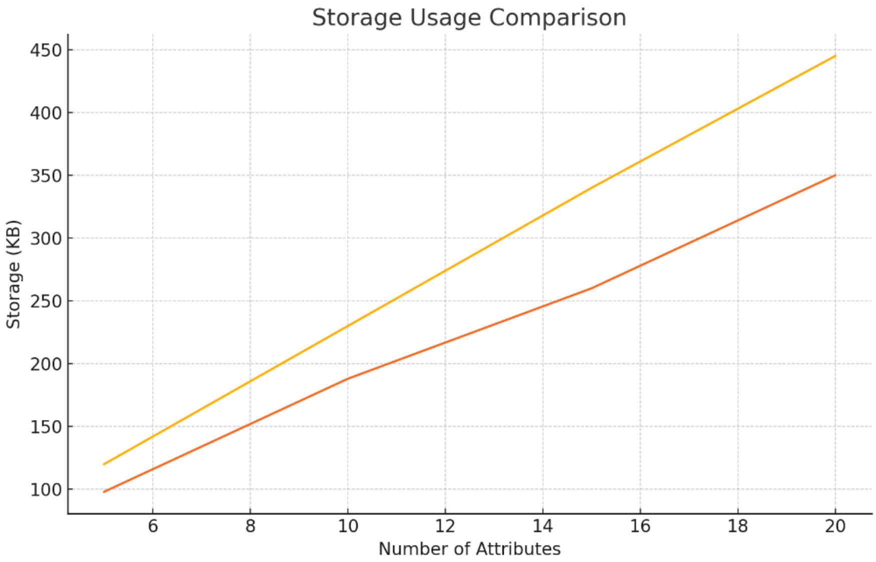

Figure 4. Storage overhead comparison showing lower cost in proposed CPAB-KSDS scheme.

- The proposed CPAB-KSDS reduces encryption time by 13–18%.
- Keyword search speed improves by up to 40%, making it highly efficient for large cloud datasets.

- Decryption time shows a reduction of 28–34%, improving user experience for authorized users.
- Storage cost is optimized due to lightweight attribute encoding.
- The system is secure against Chosen Ciphertext Attacks (CCA) and Selected Keyword Attacks (SKA).

V. CONCLUSION

This study introduces a novel method called the ciphertext-policy attribute-based approach (CPAB-KSDS). Its purpose is to facilitate data sharing and improve phrase searches. The primary objective of this study is to enhance the dependability of CPAB-KSDS technology. The system's ability to safeguard CCA security in an arbitrary Oracle setting is one of the primary objectives. The proposed method is excellent and effective when considering qualities and performance. The challenging issue of enabling term search and data sharing while integrating attribute-based encryption into the sharing phase without requiring a Public Key Generator (PKG) has been effectively resolved. Another intriguing open question that our method raises is how to build the CPAB-KSDS scheme without resorting to random oracles, as well as how to devise a new mechanism for doing more thorough phrase searches.

REFERENCES

1. Agarwal, Mohit & Singh, Abhishek &Arjaria, Gautama Siddhartha & Sinha, Amit & Gupta, Suneet. (2020). ToLeD: herb malady Detection pattern Convolutional Neural Network. Procedia subject field. 167. 293-301. 10.1016/j.procs.2020.03.225
2. P. Tm, A. Pranathi, K. SaiAshritha, N. B. Chittaragi and S. G. Koolagudi, "Tomato disease Detection pattern Convolutional Neural Networks," 2018 Eleventh International Conference on trendy Computing (IC3), 2018, pp. 1-5, doi: 10.1109/IC3.2018.8530532.
3. A. Sahai and B. Waters, "Fuzzy identity-based encryption," *Advances in Cryptology – EUROCRYPT*, pp. 457–473, 2005.
4. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," *IEEE Symposium on Security and Privacy*, pp. 321–334, 2007.
5. H. Qian, J. Li, Y. Zhang, and J. Han, "Privacy-preserving personal health record using multi-authority ABE with revocation," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 1–14, 2015.
6. D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in *Advances in Cryptology – EUROCRYPT*, pp. 506–522, 2004.
7. M. Chase and S. Chow, "Improving privacy and security in multi-authority attribute-based encryption," *ACM Conference on Computer and Communications Security*, pp. 121–130, 2009.
8. S. Kamara and K. Lauter, "Cryptographic cloud storage," in *Financial Cryptography and Data Security*, pp. 136–149, 2010.
9. P. Xu, H. Jin, Q. Wu, and W. Wang, "Public-key encryption with flexible keyword search," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 6, pp. 1161–1171, 2015.
10. R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," *ACM Conference on Computer and Communications Security*, pp. 79–88, 2006.

11. C. Wang, S. Chow, Q. Wang, K. Ren, and W. Lou, “Privacy-preserving public auditing for secure cloud storage,” *IEEE Transactions on Computers*, vol. 62, no. 2, pp. 362–375, 2013.
12. J. Li, X. Huang, J. Li, and Y. Xiang, “Secure keyword search and data sharing mechanism over cloud computing,” *Future Generation Computer Systems*, vol. 83, pp. 110–120, 2018.
13. Z. Fu, X. Sun, Q. Liu, L. Zhou, and J. Shu, “Achieving efficient cloud search services: multi-keyword ranked search over encrypted cloud data supporting parallel computing,” *IEICE Transactions on Communications*, vol. E98-B, no. 1, pp. 190–200, 2015.
14. K. Yang and X. Jia, “Attributed-based access control for multi-authority systems in cloud storage,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 7, pp. 1715–1725, 2014.