RESEARCHERID
THOMSON REUTERS

[Raut* *et al.*, 7(6): June, 2018]
IC™ Value: 3.00

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

KEY-AGGREGATE SEARCHABLE ENCRYPTION FOR GROUP DATA SHARING IN CLOUD STORAGE

Swapnil D. Raut*, Prof. Nitin R. Chopde
Dept. Of Computer Science and Engineering, Sant Gagde Baba Amravati University G. H. Raisoni College Of Engineering And Management Amravati.

DOI: 10.5281/zenodo.1284200

ABSTRACT

Security concerns over inadvertent data leaks in the cloud may greatly ease the capability of selectively sharing encrypted data with different users via public cloud storage. So designing such an encryption schemes is a key challenge which lies in the efficient management of encryption keys. When any group of selected documents need to share with any group of users a desired flexibility is required with demands different encryption keys, which are used for different documents. However this also indicates the need of securely sharing to users a large number of keys for encryption and search, and those users will have to safely save the received keys, and submit an equally large number of keywords trapdoors to the cloud in order to perform search over the shared data. The indicated purpose of safe communication, storage, and difficultly clearly renders the approach impractical. In this paper, we address this practical problem, which is greatly neglected in the literature, here we are proposing the new concept of key aggregate searchable encryption and instantiating the concept through a concrete KASE scheme. In this scheme, the documents are shared by just submitting a single trapdoor by the user to the cloud for querying and this single key is being received by the data owner for sharing large number of documents. Our proposed scheme can confirm prove both the safety as well as practically efficient channels by security analysis and performance evaluation. It can securely store and manage the users in their devices. In order to perform a keyword search over many files a large number of trapdoors must be generated by users and submitted to the cloud. Such a system with secure communication, storage and computational complexity may lead to inefficiency and impracticality.

KEYWORDS: Searchable encryption, data sharing, cloud storage, data privacy.

I. INTRODUCTION

Introduction is an act or process of making something known for the first time. We are introducing a new technique for secure group data sharing in cloud storage.

1.1 Objectives

Proposed system address the problem of secure group data sharing in cloud storage and proposed a new system for secure group data sharing in cloud storage,

- The novel concept of key aggregate searchable encryption(KASE) and instantiating the concept through a concrete KASE scheme.
- The proposed KASE scheme applied to cloud storage that supports the searchable group data sharing functionality, which means any user may selectively share a group of selected files with a group of selected users, while allowing the latter to perform keyword search over the former.
- It will support searchable group data sharing, The main requirements for efficient key management, the data owner only needs to distribute a single aggregate key (instead of a group of keys) to a user for sharing any number of files.
- The user only needs to submit a single aggregate trapdoor (instead of a group of trap-doors) to the cloud for performing keyword search over any number of shared files.

1.2 Introduction

Cloud storage has emerged as a promising solution for providing ubiquitous, convenient, and on-demand accesses to large amounts of data shared over the Internet. Today, millions of users are sharing personal data, such as photos and videos, with their friends through social network applications based on cloud storage on a

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

daily basis. Business users are also being attracted by cloud storage due to its numerous benefits, including lower cost, greater agility, and better resource utilization.

However, while enjoying the convenience of sharing data via cloud storage, users are also increasingly concerned about inadvertent data leaks in the cloud. Such data leaks, caused by a malicious adversary or a misbehaving cloud operator, can usually lead to serious breaches of personal privacy or business secrets (e.g., the recent high profile incident of celebrity photos being leaked in iCloud). To address users' concerns over potential data leaks in cloud storage, a common approach is for the data owner to encrypt all the data before uploading them to the cloud, such that later the encrypted data may be retrieved and decrypted by those who have the decryption keys. Such a cloud storage is often called the cryptographic cloud storage [6]. However, the encryption of data makes it challenging for users to search and then selectively retrieve only the data containing given keywords. A common solution is to employ a searchable encryption (SE) scheme in which the data owner is required to encrypt potential keywords and upload them to the cloud together with encrypted data, such that, for retrieving data matching a keyword, the user will send the corresponding keyword trapdoor to the cloud for performing search over the encrypted data.

Although combining a searchable encryption scheme with cryptographic cloud storage can achieve the basic security requirements of a cloud storage, implementing such a system for large scale applications involving millions of users and billions of files may still be hindered by practical issues involving the efficient management of encryption keys, which, to the best of our knowledge, are largely ignored in the literature. First of all, the need for selectively sharing encrypted data with different users (e.g., sharing a photo with certain friends in a social network application, or sharing a business document with certain colleagues on a cloud drive) usually demands different encryption keys to be used for different files. However, this implies the number of keys that need to be distributed to users, both for them to search over the encrypted files and to decrypt the files, will be proportional to the number of such files. Such a large number of keys must not only be distributed to users via secure channels, but also be securely stored and managed by the users in their devices. In addition, a large number of trapdoors must be generated by users and submitted to the cloud in order to perform a keyword search over many files. The implied need for secure communication, storage, and computational complexity may render such a system inefficient and impractical.

1.3 Motivation

Today, millions of users are sharing personal data, such as photos and videos, with their friends through social network applications based on cloud storage on a daily basis. Business users are also being attracted by cloud storage due to its numerous benefits, including lower cost, greater agility, and better resource utilization while enjoying the convenience of sharing data via cloud storage, users are also increasingly concerned about inadvertent data leaks in the cloud Such data leaks, caused by a malicious adversary or a misbehaving cloud operator, can usually lead to serious breaches of personal privacy or business secrets. However, the encryption of data makes it challenging for users to search and then selectively retrieve only the data containing given keywords. A common solution is to employ a searchable encryption (SE) scheme in which the data owner is required to encrypt potential keywords and upload them to the cloud together with encrypted data, such that, for retrieving data matching a keyword, the user will send the corresponding keyword trapdoor to the cloud for performing search over the encrypted data.

II. MATERIALS AND METHODS

Communication of information over the Internet is rapidly increasing due to the progression of higher availability of the Internet and the increase in bandwidth transmission speed. However, reliability issues regarding to data transmission such as confidentiality, data security and data loss are becoming serious concerns. The Client requires that; the transmitted data should not be lost, damaged or manipulated by any unauthorized third party. Data lost can also result from network congestion due to extra overhead. Our objective of this project is to provide an integrated mechanism which can resolve security issues, provide confidentiality, and reduce information loss.

2.1 Cryptography

Since the ancient times and all the way till now people have been transferring secret messages. Ones only in the military and the state affairs, and by spreading of electronic communications in all areas of human activities; data protection, security and privacy are becoming issues of extremely important interest. By development of the electronic banking and commerce this topic also becomes more interesting in economy. Before we proceed to more specific analysis, we will define the basic concepts related to this work.

2.2 Purpose of cryptography:

1. Authentication: The process of proving one's identity. It is another part of data security that we encounter with everyday computer usage. Just think when you log into your email, or blog account. The simple sign-in

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

process is a form of authentication that allows you to log into applications, files, folders and even an entire computer system. Once logged in, you have various given privileges until logging out. Some system will cancel a session if your machine has been idle for a certain amount of time, requiring that you prove authentication once again to re-enter. The simple sign-on scheme is also implemented into strong user authentication systems. However, it requires individuals to login using multiple factors of authentication. Non-repudiation: In this, the receiver should know whether the sender is not faking. For example, if suppose when one purchases something online, one should be sure that the person whom one pays is not faking.

2. Integrity: Many a times data needs to be updated but this can only be done by authenticated people.

3. Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver. Encryption is the process of obscuring information to make it unreadable without special knowledge. Encryption has been used to protect communications for centuries, but only organizations and individuals with an extraordinary need for secrecy had made use of it. In the mid-1970s, strong encryption emerged from the sole preserve of secretive government agencies into the public domain, and is now used in protecting widely-used systems, such as Internet e-commerce, mobile telephone networks and bank automatic teller machines. Encryption can be used to ensure secrecy, but other techniques are still needed to make communications secure, particularly to verify the integrity and authenticity of a message, for example, a message authentication code (MAC) or digital signatures. Another consideration is protection against traffic analysis. Intrusion can be taken care of by sending a signal to the receiver, the one that sends the acknowledgement signal back to the transmitter, the data will be sent only to that receiver. Thus with the use of handshaking signals intrusion can be avoided.

2.3 Advanced Encryption Standards(AES)

AES, or Advanced Encryption Standards, is a cryptographic cipher that is responsible for a large amount of the information security that you enjoy on a daily basis. Applied by everyone from the NSA to Microsoft to Apple, AES is one of the most important cryptographic algorithms being used in 2018.

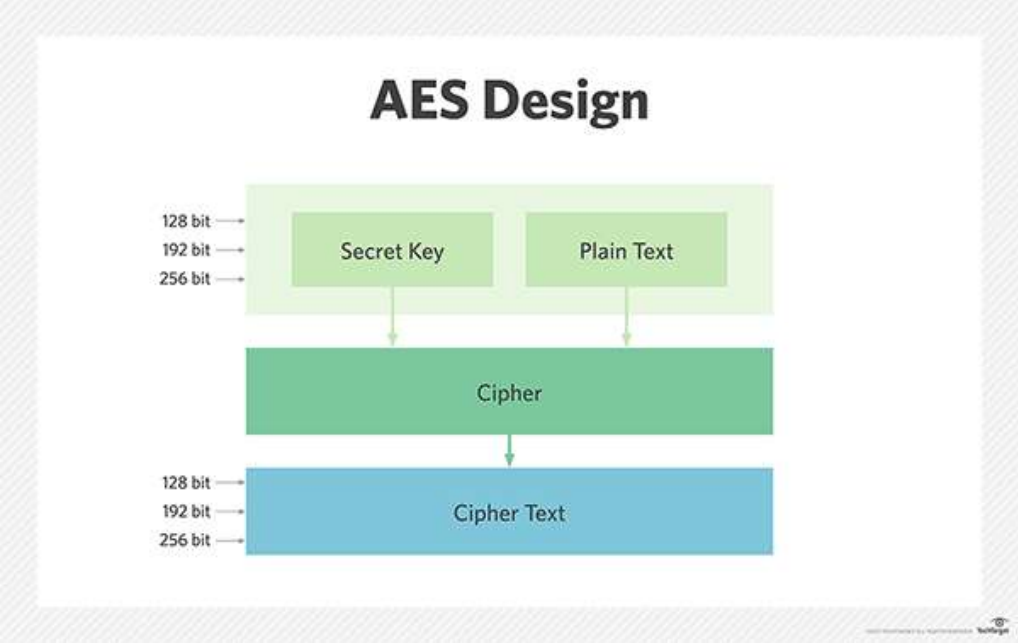

Fig.4.1 AES Design

In January, 1997 NIST began its effort to develop the AES, a symmetric key encryption algorithm, and made a worldwide public call for the algorithm to succeed DES. Initially 15 algorithms were selected, which was then reduced down to 4 algorithms, RC6, Rijndael, Serpent and Two-fish, all of which were iterated block ciphers. The four finalists were all determined to be qualified as the AES. International Journal of Emerging Technology and Advanced Engineering. The final evaluation, which also solicited worldwide public input was based on three characteristics:

i)Security:It encompassed resistance to known attacks, mathematical soundness, randomness of output and security compared to other algorithms.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

ii) Cost: Encompassed encryption speed, required memory, and no licensing agreements i.e. the algorithm had to be available worldwide royalty free.

iii) Algorithm and implementation characteristics: The algorithm had to be suitable across a wide range of hardware and software systems. The algorithm had to be relatively simple as well. After extensive review the Rijndael algorithm was chosen to be the AES algorithm.

Table 2.1. Difference Between AES And DES

Factors	**DES**	**AES**
Key Length	56 bits	128, 192, 256 bits
Block Size	64 bits	128, 192, 256 bits
Cipher Text	Symmetric block cipher	Symmetric block cipher
Developed	1977	2000
Security	Proven inadequate	Considered secure
Cryptanalysis resistance	Vulnerable to differential and linear cryptanalysis	Strong against differential and linear cryptanalysis
Possible Keys	2^{56}	2^{128}, 2^{192}, 2^{256}

AES was designed to have the following characteristics:

i) Resistance against all known attacks.
ii) Speed and code compactness on a wide range of platforms
iii) Design Simplicity

III. SYSTEM MODEL

In our proposed there are three modules

1. Admin
2. Trapdoor
3. User

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

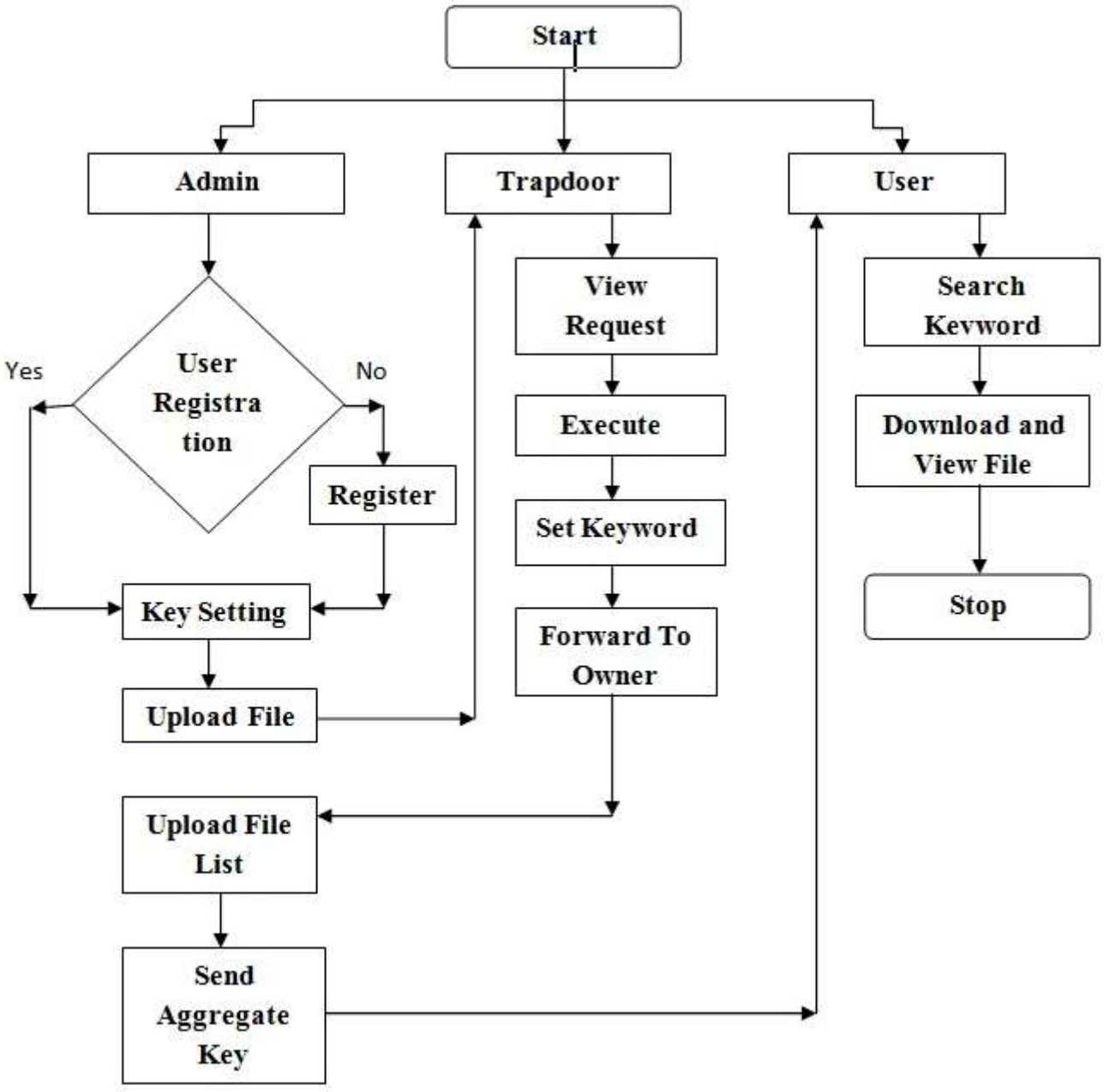

Figure 3.1:-Flow Chart diagram of proposed system

In our proposed system we have three modules the flow of our module is shows in above diagram.

Step1:

In our proposed we first login the admin module.

1.1 If already register no need to register again otherwise user have to register first.
1.2 After registration key has to be set.
1.3 Then Admin upload the file on cloud.
1.4 Logout from admin module.

Step2:

Login Trapdoor module

2.1 In trapdoor we view the request generated by Admin.
2.2 Then execute the request send by Admin.
2.3 For that request set the Keywords and forward to Admin(to be owner).
2.4 Logout from Trapdoor module.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

Step3:

Again Login Admin module

3.1 After that it will be add in Upload file List.
3.2 Then Admin will set and send Aggregate key.
3.3 Logout from Admin.

Step4:

Login User module

4.1 After that in user module user will search the file by using keywords.
4.2 Now User can successfully download the file.
4.3 User can view the file.
4.4 Logout from User

IV. RESULTS AND DISCUSSION

In this section we are discuss about result analysis. We collect the result of our proposed system on some parameters like time, keywords, Shared Documents and Cipher Text. We implement the proposed secure textual data transmission, in which we model three entities as separate programs. Data encryption which protect our data from third party, data hiding which maintain our confidential data secrecy, data compression for saving time and memory in transmission. Evaluation of the proposed system focuses secure transmission using cryptography.

In this first table we compare previous parameter with the Proposed system parameter.

Table 4.1:- Comparison of Parameter

Parameter	**Previous Parameter**	**Proposed Parameter**
Time cost of Encrypt	around 80 ms	around 76 ms
Time cost of Extract	around 50 ms	around 45ms
Time Cost of Adjust	around 50 ms	around 44ms
Time Cost of Test	around 70ms	around 60ms

The execution time of encrypt is Linear in the number of Keywords. In above table time cost of Encrypt for 5 keywords in previous system time taken is around 80ms but in our Proposed system time taken is around 76ms.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

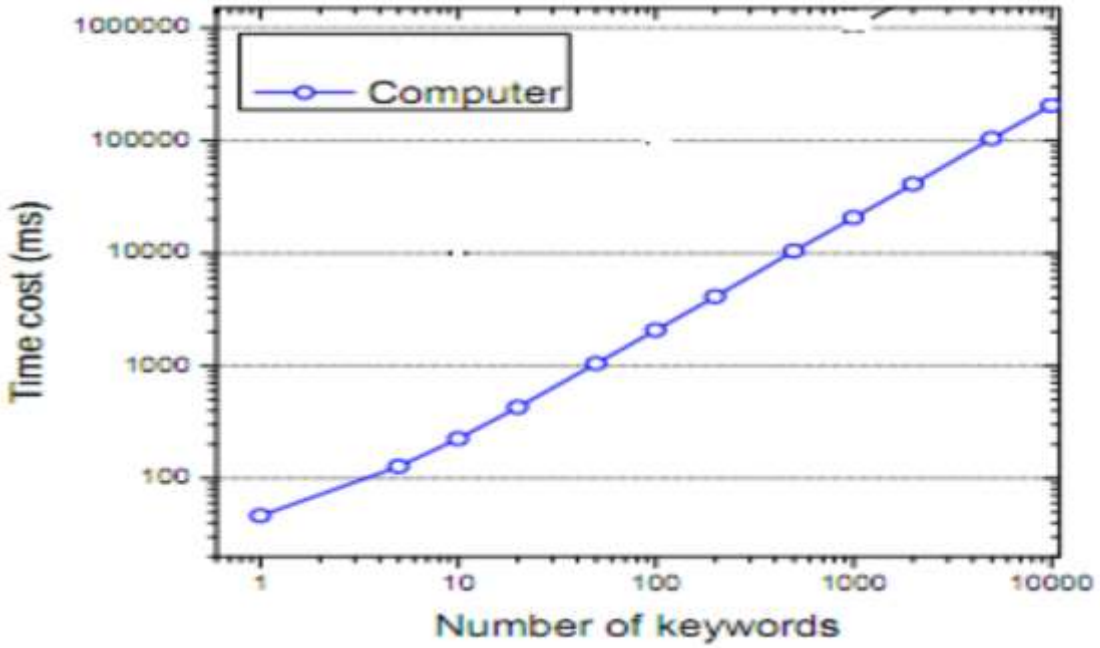

Figure 4.1:- Time cost of Encrypt(Previous System)

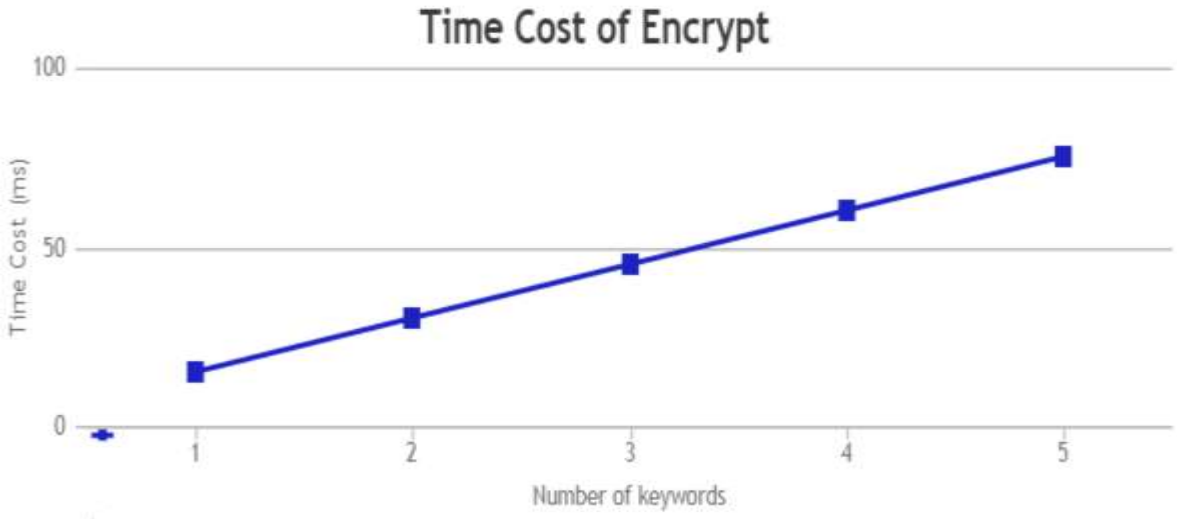

Figure 4.2:- Time cost of Encrypt (Proposed System)

The execution time of Extract is Linear in the number of shared documents . In above table time cost of Extract for 5 shared documents in previous system time taken is around 50ms but in our propose system time taken is around
45ms.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

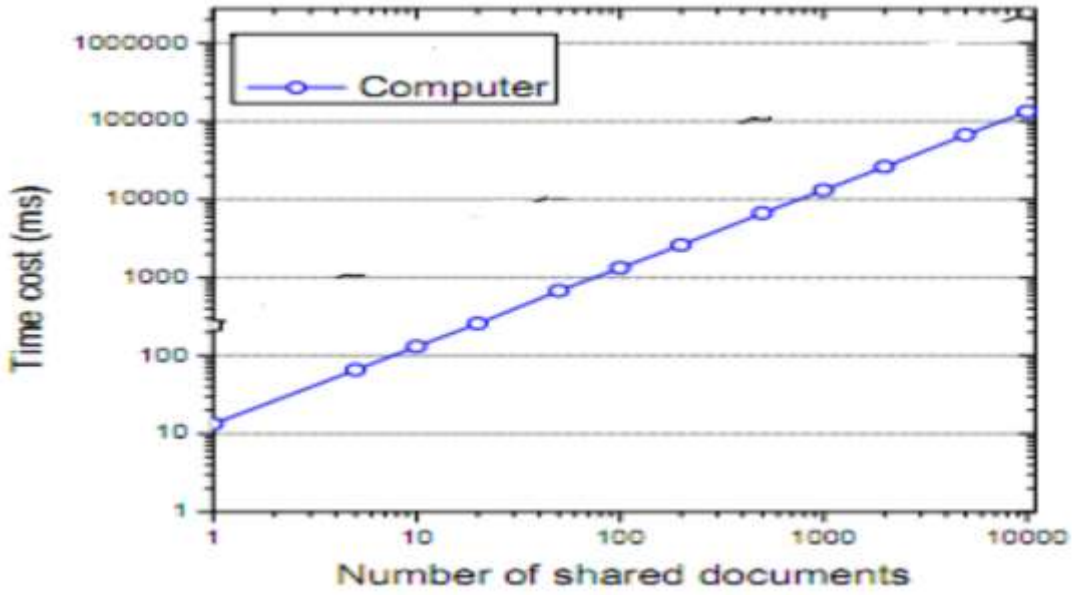

Figure 4.3:- Time cost of Extract (Previous System)

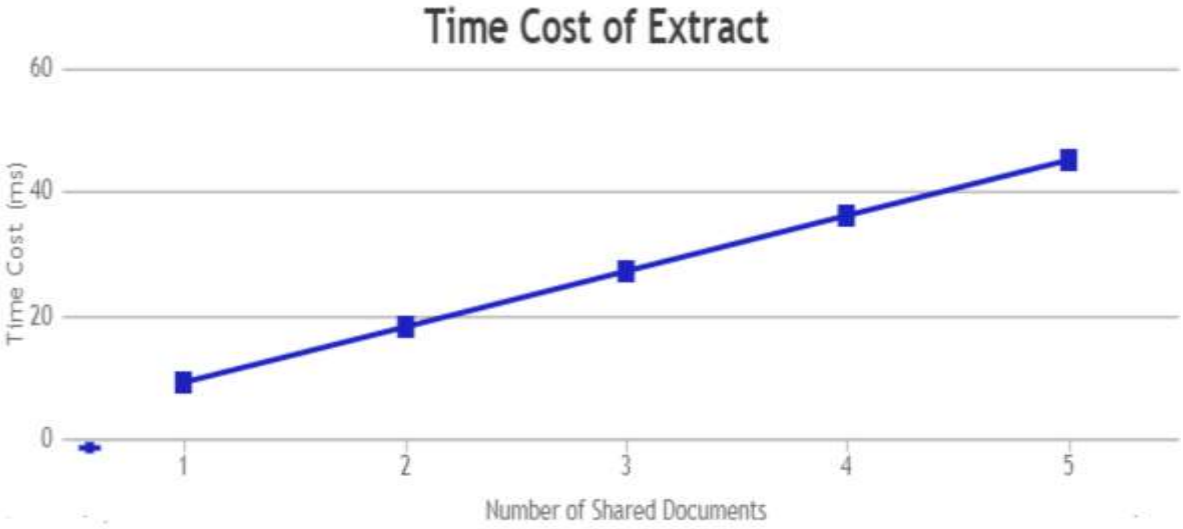

Figure 4.4:- Time cost of Extract (Proposed System)

The execution time of Adjust is Linear in the number of documents . In above table time cost of Adjust for 5 documents in previous system time taken is around 50ms but in our propose system time taken is around 44ms.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

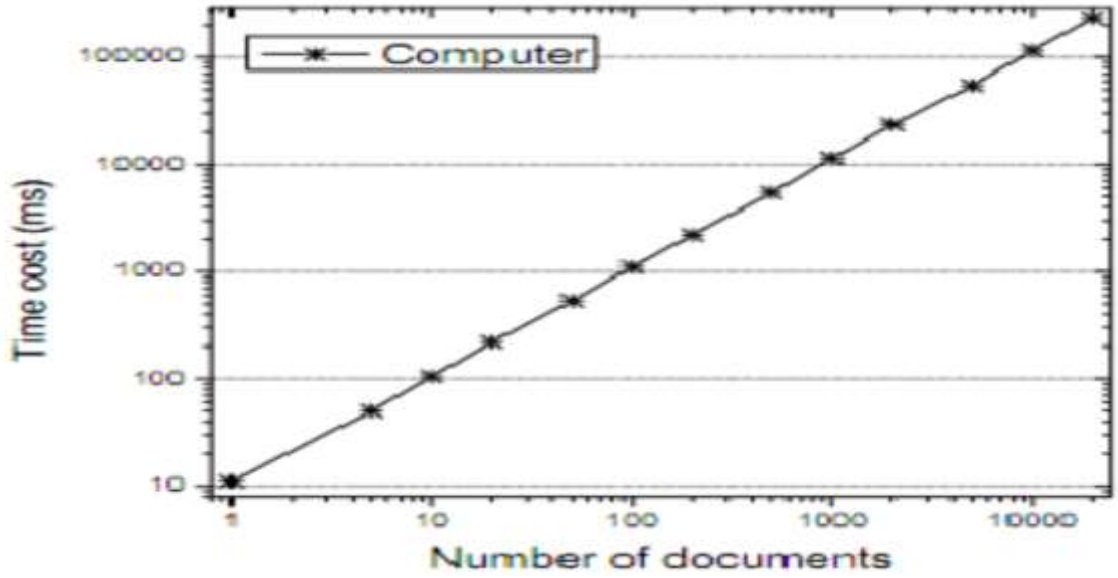

Figure 4.5:- Time Cost of Adjust (Previous System)

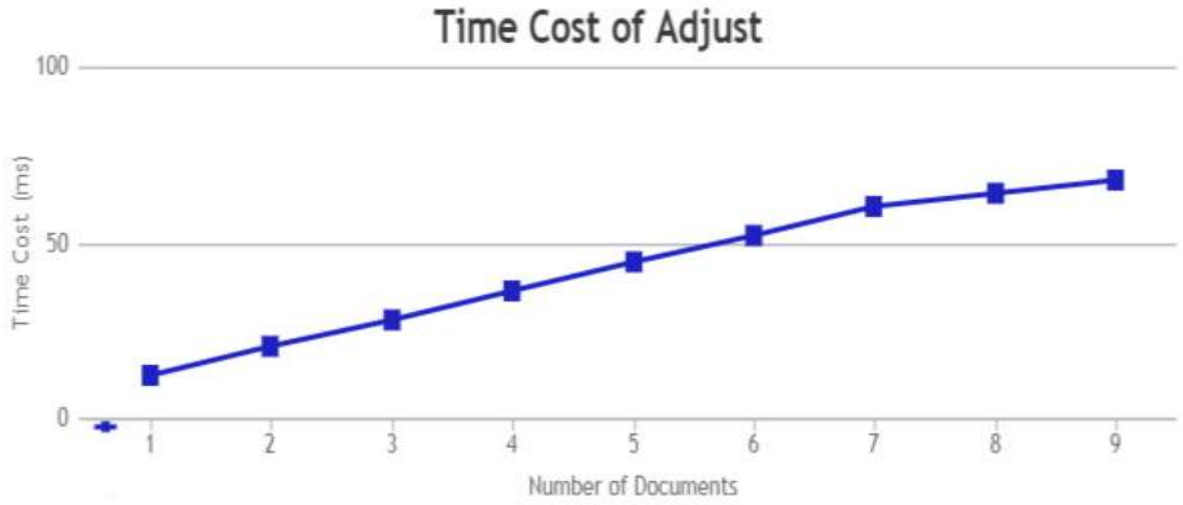

Figure 4.6:- Time Cost of Adjust (Proposed System)

The execution time of Test is Linear in the number of Keyword Ciphertext. In above table time cost of Test for 5 keyword Ciphertext in previous system time taken is around 70ms but in our propose system time taken is around 60ms.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

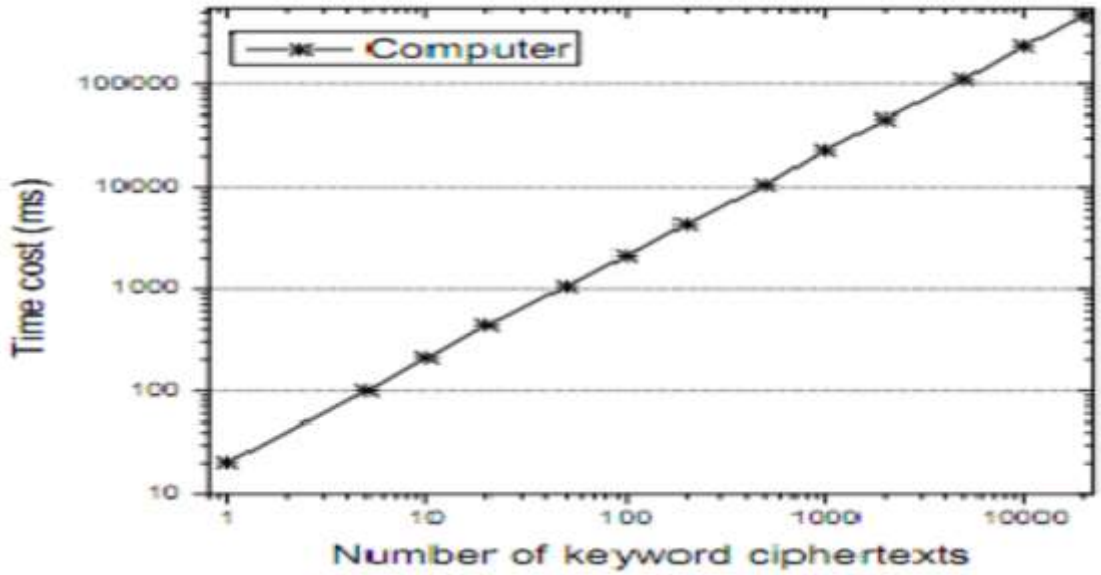

Figure 4.7:- Time Cost of Test(Previous System)

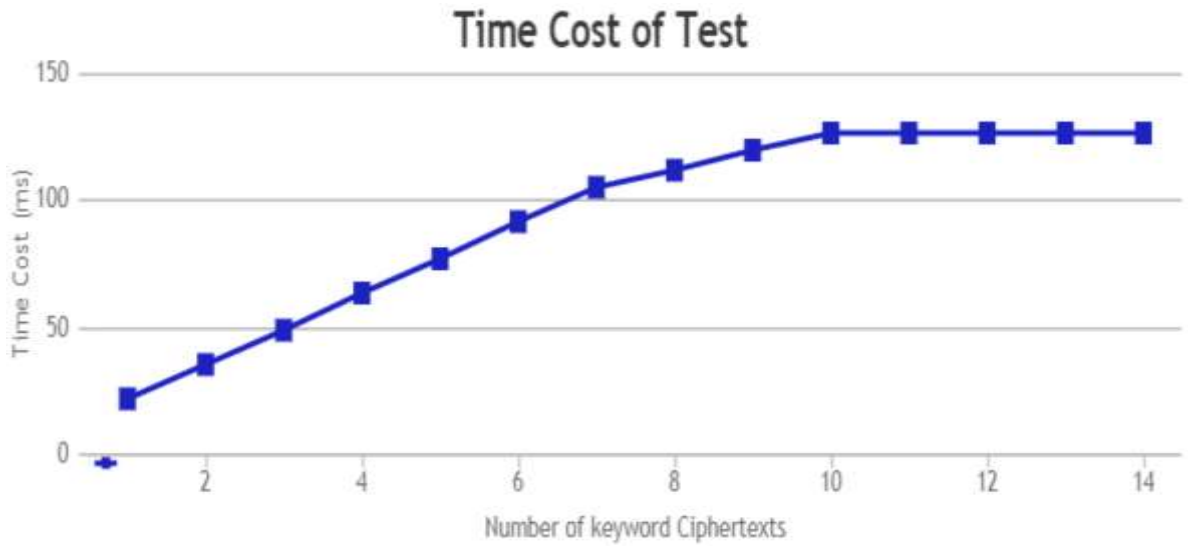

Figure 4.8:- Time Cost of Test(Proposed System)

V. APPLICATIONS

1. **Confidential Communication**
   The two companies or organizations are Suppose to deal with another companies or organization then between those companies much more confidential data is transfer through mail or communication is happen related to company and if that confidential data goes in third hand then it is harmful for companies or organization And to maintained the confidential communication secure we use proposed system.
2. **Hiding Secret Data**
   To keep the confidentiality of data or information and to secure that data there is need to hide that data from everyone. So we can use the proposed technique to hide the data behind useless data.
3. **Maintaining Confidentiality**
   The database or information used in school, colleges, companies and organizations is the detail information about students, employees and workers such as account number, pan card number, which is the confidential data. And to maintain this confidential data we can use the proposed system.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

4. Protection

In social networking sites we are transfer much more data sometimes that data is confidential like pan card number, account number. And if that confidential data goes in third hand then it is harmful so for protect our confidential data from third party we can used our proposed system.

V. CONCLUSION

Considering the practical problem of privacy preserving data sharing system based on public cloud storage which requires a data owner to distribute a large number of keys to users to enable them to access his/her documents, we for the first time propose the concept of key-aggregate searchable encryption (KASE) and construct a concrete KASE scheme. Both analysis and evaluation results confirm that our work can provide an effective solution to building practical data sharing system based on public cloud storage.

VI. REFERENCES

[1] S. Kamara, C. Papamanthou, T. Roeder. "Dynamic searchable symmetric encryption", Proceedings of the 2012 ACM conference on Computer and communications security (CCS), ACM, pp. 965- 976, 2012.
[2] D. Boneh, C. G, R. Ostrovsky, G. Persiano. "Public Key Encryption with Keyword Search", EUROCRYPT 2004, pp. 506C522, 2004.
[3] X. Song, D.Wagner, A. Perrig. "Practical techniques for searches on encrypted data", IEEE Symposium on Security and Privacy,IEEE Press, pp. 44C55, 2000.
[4] R. A. Popa ,N. Zeldovich. "Multi-key searchable encryption".Cryptology ePrint Archive, Report 2013/508, 2013.
[5] C. Chu, S. Chow,W. Tzeng, et al. "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage", IEEE Transactions on Parallel and Distributed Systems, 2014, 25(2): 468-477.
[6] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing", Proc. IEEE INFOCOM, pp. 534-542, 2010
[7] D. Boneh, C. Gentry and B. Waters. "Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys",CRYPTO'05, pp. 258C275, 2005.
[8] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing", Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.
[9] R. Curtmola, J. Garay, S. Kamara, R. Ostrovsky. "Searchable symmetric encryption: improved definitions and efficient constructions", In: Proceedings of the 13th ACM conference on Computer and Communications Security, ACM Press, pp. 79-88, 2006.
[10] P. Van,S. Sedghi, JM. Doumen. "Computationally efficient searchable symmetric encryption", Secure Data Management, pp. 87-100, 2010.
[11] S. Kamara, C. Papamanthou, T. Roeder. "Dynamic searchable symmetric encryption", Proceedings of the 2012 ACM conference on Computer and communications security (CCS), ACM, pp. 965- 976, 2012.
[12] Y. Hwang, P. Lee. "Public Key Encryption with Conjunctive Keyword Search and Its Extension to a Multi-user System", In:Pairing-Based Cryptography C Pairing 2007, LNCS, pp. 2-22, 2007.
[13] J. Li, Q. Wang, C. Wang. "Fuzzy keyword search over encrypted data in cloud computing", Proc. IEEE INFOCOM, pp. 1-5, 2010.
[14] C. Bosch, R. Brinkma, P. Hartel. "Conjunctive wildcard search over encrypted data", Secure Data Management. LNCS, pp. 114- 127, 2011.
[15] C. Dong, G. Russello, N. Dulay. "Shared and searchable encrypted data for untrusted servers", Journal of Computer Security, pp. 367-397, 2011.
[16] F. Zhao, T. Nishide, K. Sakurai. Multi-User Keyword Search Scheme for Secure Data Sharing with Fine-Grained Access Control. Information Security and Cryptology, LNCS, pp. 406-418, 2012.
[17] J. W. Li, J. Li, X. F. Chen, et al. "Efficient Keyword Search over Encrypted Data with Fine-Grained Access Control in Hybrid Cloud", In: Network and System Security 2012, LNCS, pp. 490- 502, 2012.
[18] J. Li, K. Kim. "Hidden attribute-based signatures without anonymity revocation", Information Sciences, 180(9): 1681-1689,Elsevier, 2010.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

CITE AN ARTICLE

Raut, S. D., & Chopde, N. R., Prof. (2018). KEY-AGGREGATE SEARCHABLE ENCRYPTION FOR GROUP DATA SHARING IN CLOUD STORAGE. *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY, 7*(6), 264-274.