International Journal of Engineering Innovations in Advanced Technology
ISSN: 2582-1431 (Online), Volume-6 Issue-3, September 2024

Protecting Your Mobile Cloud Data Chaos-Based Encryption

Kasaragoni Sudharani
M.Tech Scholar, Department of CSE, Avanthi Institute of Engineering & Technology, Hyderabad, India.
Email: sudharani1561@gmail.com
S Rajender
Assistant Professor, Department of CSE, Avanthi Institute of Engineering & Technology, Hyderabad, India.
Email: memoryreturn@gmail.com
Dr. N. Ramana Reddy
Associate Professor & HOD, Department of CSE, Avanthi Institute of Engineering & Technology, Hyderabad, India.
Email: ramana139@gmail.com

Abstract:This paper considers the security problem of outsourcing storage from user devices to the cloud. A secure searchable encryption scheme is presented to enable searching of encrypted user data in the cloud. The scheme simultaneously supports fuzzy keyword searching and matched results ranking, which are two important factors in facilitating practical searchable encryption. A chaotic fuzzy transformation method is proposed to support secure fuzzy keyword indexing, storage and query. A secure posting list is also created to rank the matched results while maintaining the privacy and confidentiality of the user data, and saving the resources of the user mobile devices. Comprehensive tests have been performed and the experimental results show that the proposed scheme is efficient and suitable for a secure searchable cloud storage system.

Keywords: Cloud, Fuzzy, Chaotic, Encryption, Privacy.

1. INTRODUCTION

Cloud is a model to enable convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) In the current Internet, people can easily access their data stored in the cloud with their mobiledevices from anywhere, e.g., check emails, and read the history of online chatting applications,view previously saved photos, videos or other kind of documents. To provide security in all such scenarios, it is essential to store and access the outsourced data in a secure and efficient manner. For the protection of data privacy and control, data is usually encrypted before outsourcing, which makes its effective utilization a challenge. In particular, indexing and searching the outsourced encrypted data becomes problematic. Searchable encryption (SE) allows searching over encrypted data in the cloud and returns to the user the data that correspond to the given keywords, without having to reveal the keywords. It is thus a critical enabler for securing outsourced data. Traditional searchable encryption schemes allow a user to securely search over encrypted data through keywords but only support 1) exact keyword matching, which is not a practical requirement for current mobile phone input methods and 2) boolean search without capturing the relevance of data files. The system usability can be greatly enhanced by the use of fuzzy keyword search instead of traditional searchable encryption. Fuzzy, or error tolerant, searchable encryption returns to the user the files that match not onlythe exact predefined keywords but also the closest possible matched files based on keyword similarity semantics. Similarly, system usability is greatly enhanced by ranked search which returns the matched files in a ranked order determined by appropriate relevance criteria.

2. LITERATURE SURVEY

Many approaches are proposed to enable fuzzy search. Researchers [1] consider the use of wildcards to enlarge the range of possible similar keywords searched, but this technique only covers part of the possible close keywords. A wildcard only permits capturing of errors provided we know where they are located in the keyword. The authors [2] proposed a new cryptographic primitive called Public Key Error Tolerant Searchable Encryption (PKETS) which is based on public key encryption with keyword search proposed. This algorithm was applied to the biometric data [3]. Acceptable erroneous keywords did not have to be specified in advance in their algorithm. However, this approach was designed for a special type of data, i.e., iris code. This technology is useful at airports as a replacement for passports but it is not designed for text documents. The authors [4], proposed to embed edit distance (Levenshtein distance) into Hamming distance to obtain a fuzzy keyword search suitable for strings and then text files. This method uses existing locality sensitive hashing (LSH) to enable the fuzziness in the search method and has a very low distortion. However, this method is mainly theoretical and the proposed embedding technique introduces a lot of redundancy, which increases the dimension of the stored data, and is not suitable for the case of mobile usage because of the small amount of memory available. Another method [5] uses bloom filters and Jaccard similarity to perform the translation and the LSH. It also introduces ranking of the retrieved encrypted data. However, the ranking has to be performed by the user himself and not automatically by the server which can add unwanted burden for a mobile user"s device. Actually, very few searchable encryption schemes support the ranking of matched items though this problem has recently attracted the attention of some researchers [6]. Fuzziness and ranking are currently two different research axes and very few researchers

have considered combining them. However, these methods are either not practical for mobile usage as is the case or they suffer from security problems as is the case. This work proposed a new fuzzy transformation by introducing chaos and enhances the amplification of fuzziness the LSH, through which significantly improves both the security and the efficiency of the fuzzy searching process compared to the existing solutions

3. SYSTEM ANALYSIS

A. EXISTING SYSTEM

In the existing system, Bringer et al. proposed a new scheme permitting search over encrypted data with an approximation of a keyword. An application in the biometric domain isalso proposed. A biometric identification scheme arises from this construction; it permits identification of a person using his biometrics in an encrypted way. A specific difficulty concerning biometrics is their fuzziness. It is nearly impossible for a sensor to obtain the same image from biometric data twice.

The classical way to solve this problem is to use a matching function, which basically tells if two measures represent the same biometric data or not, but these methods do not meet the privacy requirements that someone can expect from an such identification scheme. The Bringer et al. algorithm resolves this issue and provides the privacy missing in the existing algorithms.This method uses a combination of LSH method specific for an iris code (beacon indexes) to enable the fuzziness and a Bloom filter with storage to accelerate the search on the encrypted data.

B. PROPOSED SYSTEM

This system proposes a new fuzzy transformation by introducing chaos and enhances the fuzziness through amplification of the LSH, which significantly improves both the security and the efficiency of the fuzzy searching process compared to the existing solutions. Furthermore, comprehensive tests on different LSH methods are performed in order to select the best one to be used in our algorithm.

Chaotic systems are widely used in the cryptography domain and have attracted the attention of many researchers due to the interesting characteristics of chaos. However, to the best of ourknowledge, this is the first paper proposing to use chaos in the searchable encryption schemes.

Our proposed system is, in addition, designed to support fuzzy and ranking mechanisms and isproven to be practical for mobile usage.

4. SYSTEM REQUIREMENTS

A. FUNCTIONAL REQUIREMENTS

- Cloud

In this module, the Cloud has to login by using valid user name and password. After login successful he can perform some operations such as View All Users, View All Documents, View Top 'K' Keywords, View Keywords and Links, View Time Delay ofFiles, View User Transactions, View File Rank Results,View Time Delay Comparison Results

- Client

In this module, there are n numbers of clients are present. Client should register before performing any operations. Once Client registers, their details will be stored to the database.

After registration successful, he has to login by using authorized user name and password. Verify finger print and Login Once Login is successful Client can perform some operations like View Profile, Upload Document, Edit / Delete Document, Search Cloud Data, View Document Search Comparison, View Keyword and Fetched Files, View Same Data Files

B. NON-FUNCTIONAL REQUIREMENTS

Non-functional requirements or NFRs are a set of specifications that describe the system's operation capabilities and constraints and attempt to improve its functionality. These are basically the requirements that outline how well it will operate including things like speed, security, reliability, data integrity, etc.

The SRS itself can be divided into module, each module having specifications. In order to carryout the project, the following hardware and software is required.

Non-functional requirements state constraints on the design and construction of the product. They are often dictated by contractual or regulatory requirements, which may include, amongothers:

- Standardization requirements
- Compatibility requirements
- In-service support requirements
- End-of-life disposal requirements.

5. SYSTEM STUDY

A. FEASIBILITY STUDY

The feasibility of the project is analyzed in this phase and business proposal is put forth with avery general plan for the project and some cost estimates. During system analysis the feasibilitystudy of the proposed system is to be carried out. This is to ensure that the proposed system isnot a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are:

- ECONOMICAL FEASIBILITY
- TECHNICAL FEASIBILITY

♦ SOCIAL FEASIBILITY

B. ECONOMICAL FEASIBILITY

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as wellwithin the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

C. TECHNICAL FEASIBILITY

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

D. SOCIAL FEASIBILITY

The aspect of study is to check the level of acceptance of the system by the user. This includesthe process of training the user to use the system efficiently. The user must not feel threatenedby the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

E. FEASIBILITY ANALYSIS

Technical Feasibility:

- **Technology Stack**:

The system's technical prerequisites can be readily fulfilled through the utilization of widely accessible technologies, such as data mining libraries, relational databases, and statistical tools.These foundational components collectively form a robust and accessible framework for developing and operating the system. Relational databases, exemplified by MySQL, offer scalable and efficient data storage solutions. These databases empower the system to store andmanage data in a structured manner, facilitating seamless retrieval and manipulation. By leveraging these commonplace technologies, the system can harness the full potential of data mining, storage, and analysis, enabling it to operate efficiently and effectively. These readily available resources not only expedite development but also enhance the system's accessibility to a wider audience of developers and practitioners. Incorporating HTML, CSS, and Java intothe tech stack is essential for building modern, interactive, and visually appealing webapplication. Here's why these three technologies are integral to any web development project:

Operational Feasibility:

- **Data Availability:**

We can confidently affirm that the essential user behavior data, inclusive of time distribution parameters, is both accessible and abundant in quantity, ensuring the system's robust operation.The assurance stems from the fact that the necessary data, which encapsulates user actions and their temporal patterns, is readily obtainable. It is obtainable through various means, including user interaction logs, website analytics, and application usage tracking. These sources consistently furnish us with a rich dataset that encapsulates how users engage with the systemover time. Moreover, the ample availability of this data serves as a foundation for informed decision-making and data-driven insights. It enables the system to not only monitor user interactions but also to derive meaningful patterns and trends from these interactions. The abundance of data ensures that the system has a substantial historical record to draw upon, facilitating accurate predictions and intelligent responses to user behavior. This wealth of user behavior data, along with its time-related parameters, not only meets but exceeds the system'srequirements. It empowers the system to deliver a user experience that is responsive, tailored,and finely tuned to the nuances of how users engage with it, thereby enhancing its overall effectiveness and user satisfaction.

- Integration:

The system's integration feasibility aligns seamlessly with the pre-existing security infrastructure and user monitoring systems in place. This compatibility underscores the system's capacity to harmoniously coexist with the current security and monitoring ecosystem.The design of the system has been meticulously crafted to ensure it adheres to the established security protocols and practices within the organization. This includes robust encryption methods, access controls, and authentication mechanisms, all of which can seamlessly interfacewith the existing security framework. The system's compliance with industry-standard securitymeasures further underscores its suitability for integration. Additionally, the system's adaptability extends to user monitoring systems. It can seamlessly interface with the organization's user activity tracking and monitoring tools, facilitating the continuous surveillance of user interactions within the system. This ensures that the organization can maintain its vigilant stance on security and user behavior, leveraging its current monitoring investments effectively. In summary, the system's integration feasibility is underpinned by its innate compatibility with the organization's security infrastructure and user monitoring systems.

- User Acceptance:

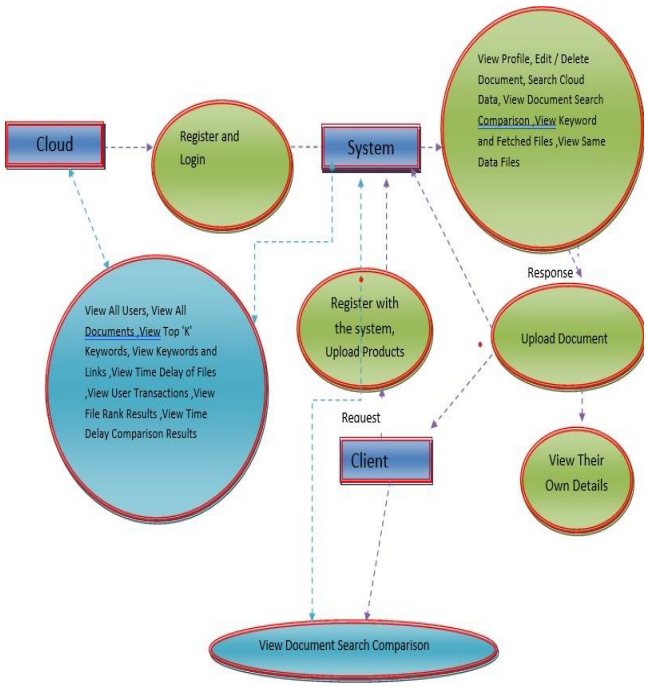
Users may have concerns about the extent to which their behavior is monitored and whether their personal information is adequately protected. It is essential to transparently communicate the system's purpose and data handling practices to address these concerns. We have made sureto comply with all privacy policies suggested by our

guides and advisors during the development of this project. We have also ensured that users understand the system's purpose,how it works, and its benefits in terms of improved security. Providing training and support canenhance user and admin acceptance.

6. SYSTEM DESIGN

System design is transition from a useroriented document to programmers or data basepersonnel. The design is a solution, how to approach to the creation of a new system. This is composed of several steps. It provides the understanding and procedural details necessary for implementing the system recommended in the feasibility study. Designing goes through logicaland physical stages of development, logical design reviews the present physical system, prepare input and output specification, details of implementation plan and prepare a logical design walkthrough.

A. *SYSTEM ARCHITECTURE*



7. RESULTS/DISCUSSION

A. SYSTEM TESTING

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, subassemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the

Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testingrequirement.

Unit testing

Unit testing involves the design of test cases that validate that the internal program logicis functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .it is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests performbasic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

Integration testing

Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components wereindividually satisfaction, as shown by successfully unit testing, the combination of componentsis correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

Functional test

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.

Functional testing is centered on the following items:

Valid Input : identified classes of valid input must be accepted.

System Test

System testing ensures that the entire integrated software system meets requirements. It tests a configuration to ensure known and predictable results. An example of system testing is the configuration oriented system integration test. System testing is based on process descriptions and flows, emphasizing pre-driven process links and integration points.

White Box Testing

White Box Testing is a testing in which in which the software tester has knowledge of the inner workings, structure and language of the software, or at least its purpose. It is purpose. It is usedto test areas that cannot be reached from a black box level.

Black Box Testing

Black Box Testing is testing the software without any knowledge of the inner workings, structure or language of the module being tested. Black box tests, as most other kinds of tests,must be written from a definitive source document, such as specification or requirements document, such as specification or requirements document. It is a testing in which the softwareunder test is treated, as a black box .you

cannot “see” into it. The test provides inputs and responds to outputs without considering how the software works.

Integration Testing

Software integration testing is the incremental integration testing of two or more integrated software components on a single platform to produce failures caused by interface defects. The task of the integration test is to check that components or software applications,

e.g. components in a software system or – one step up – software applications at the companylevel – interact without error.

Test Results: All the test cases mentioned above passed successfully. No defects encountered.

B. SCREENSHOTS

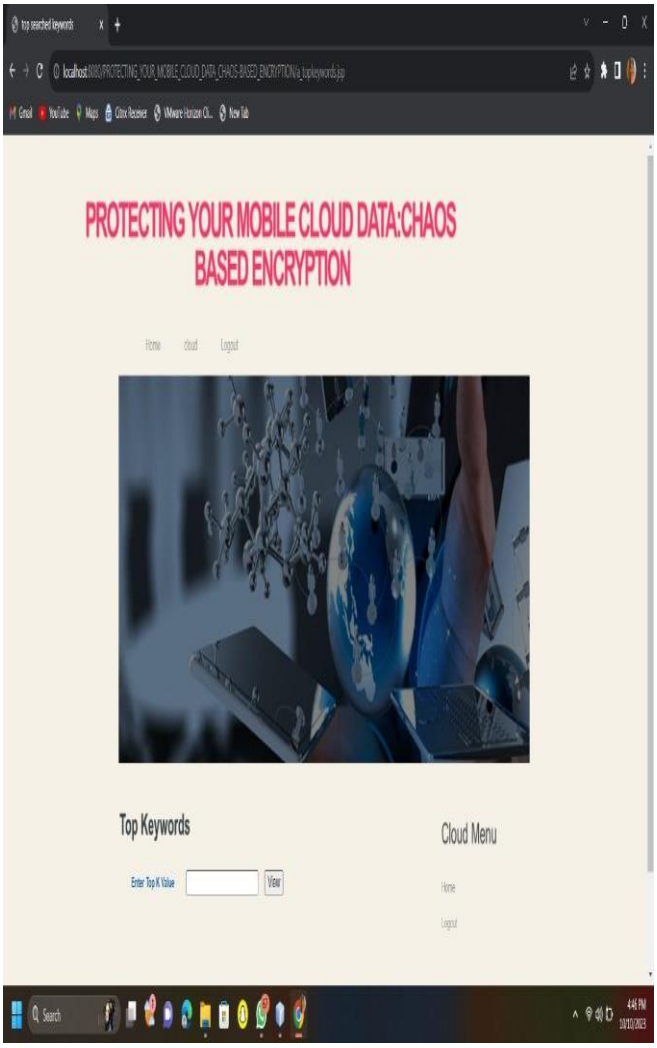


FIG-1 Home Screen The term "Home screen" refers to the main or initial screen of an application or website that users encounter upon opening the application or accessing website The home screen is essentially the starting point and often sets the tone for the rest of the userexperience.

FIG-2 All user list

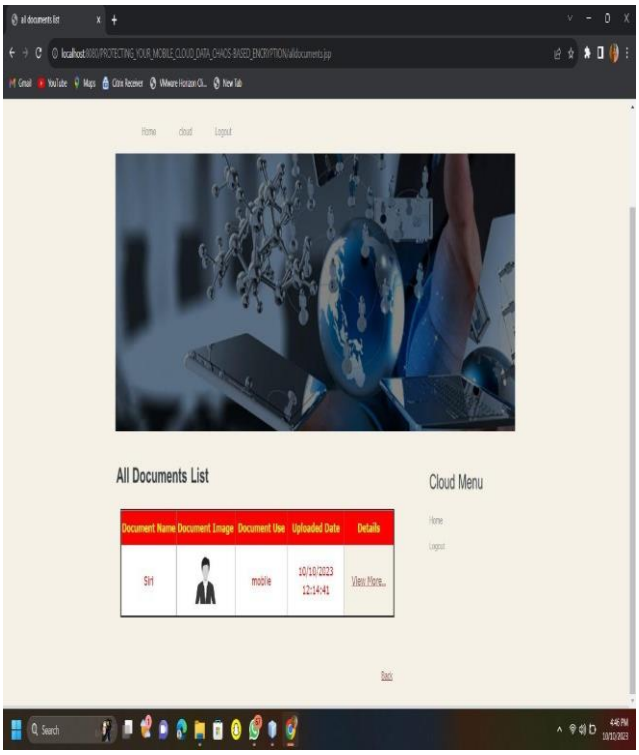


FIG-3 Upload document with details

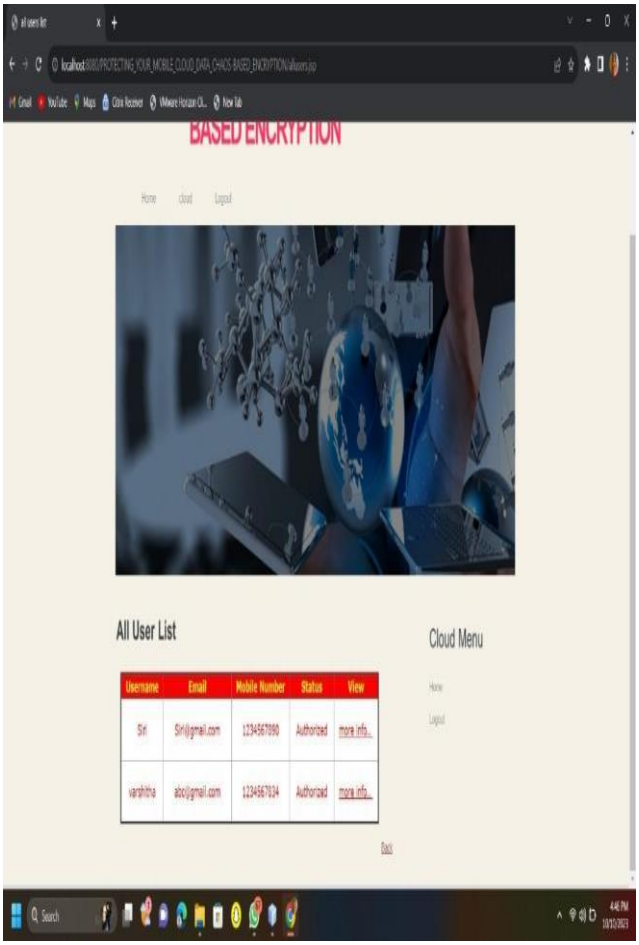


FIG-4 All Document list

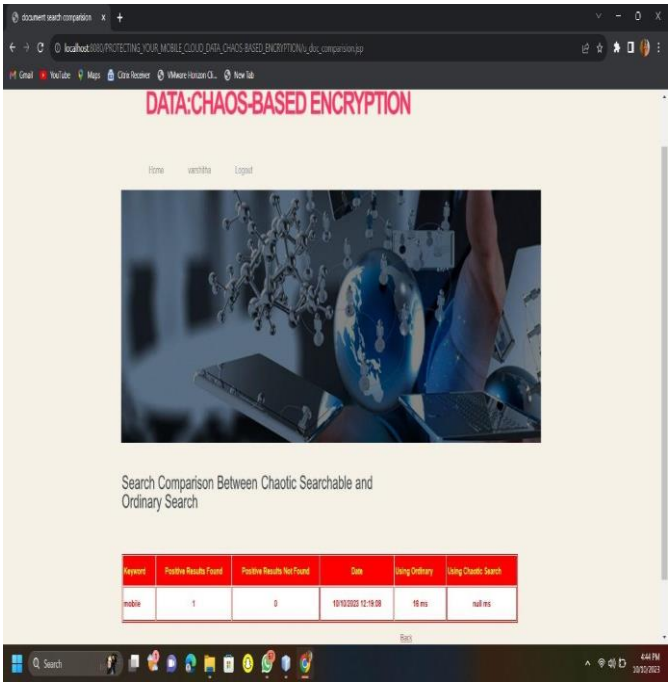


FIG-5 All user transactions

All user transactions are used to find the positive and negative results transcation withusername and time and date.

Top keywords are used to search the documents as key values ‘K’ in the cloud menu.

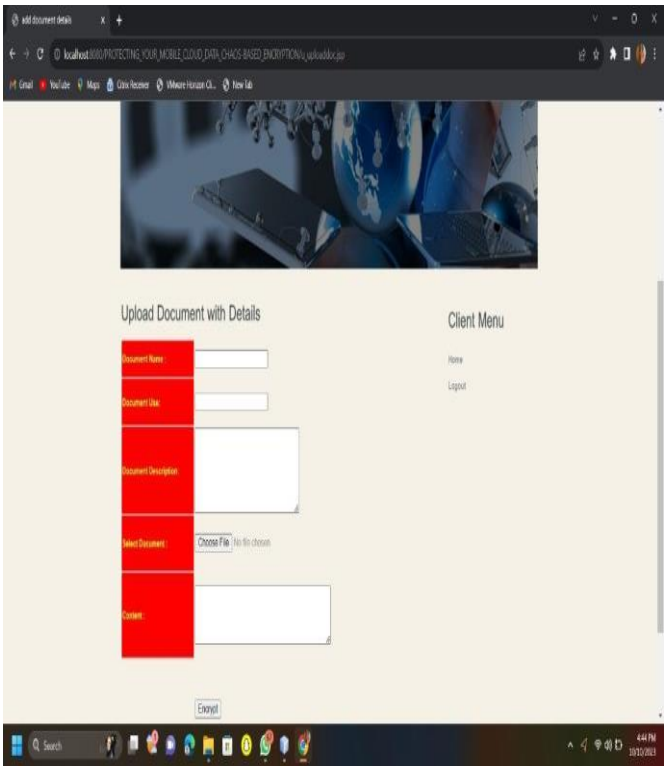


FIG-6 search comparison between chaotic and ordinary search

Search comparison between chaotic and ordinary search is used for both time delay andtransaction between chaotic and ordinary searches.

CONCLUSION

In this paper, we proposed the first chaos based searchable encryption approach which also allows both ranked and fuzzy keyword searches on the encrypted data stored in the cloud.

Our approach guarantees the privacy and confidentiality of the user even vis-à-vis the cloud provider who is semi-trusted in our case. The proposed method is designed to achieve effective retrieval of remotely stored encrypted data for mobile cloud computing scenarios.

This scheme is implemented and evaluated using two databases: RFCs and the Enron database.

FUTURE SCOPE

The proposed scheme uses chaotic random noise to improve the strength of encryption keys. The strength of the encryption keys does not rely on the length of the key but the random and chaotic nature of the input noise.

Several experiments were conducted to test different aspects of the solution implemented. Overall, it is concluded, based on the results, that chaos theory can be applied in cryptographyto improve the strength of ciphers.

The result show that Cryptor is a lightweight, strong client-end encryption scheme. Hence, Cryptor is a better encryption scheme in terms of encryption and decryption times.

The chaos-based encryption keys can be used to improve the strength of existing cryptosystemssuch as DES, 3-DES and AES. Future perspectives include: experimenting on encrypting multimedia digital content, implementing the Cryptor system to have rounds of encryption to increase layers of security, and to test the proposed neural key store against various types of key attacks.

Searchable encryption (SE) allows searching over encrypted data in the cloud and returns to the user the data that correspond to the given keywords, without having to reveal the keywords.

REFERENCES

[1] B.Yang, X. Pang, Q. Du, and Dan Xie, "Effective Error-Tolerant Keyword Search for Secure Cloud Computing," Journal of computer science and technology, vol. 29, no.1, pp. 81-89, Jan. 2014.

[2] D. Boneh, G. D. Crescenzo, "Public key encryption with keyword search," in C. Cachin and J. Camenisch, editors, Advances in Cryptology, Eurocrypt, vol. 3027 of LNCS, pp. 506– 522, Springer, 2004.

[3] S. Kamara, K. Lauter, "Cryptographic cloud storage, " in Financial Cryptography and DataSecurity, pp. 136-149, Springer Berlin Heidelberg, 2010.

[4] S. Kamara, C. Papamanthou, T. Roeder, "CS2: A searchable cryptographic cloud storage system," Microsoft Research, Tech. Report MSR-TR, 2011.

[5] Y. Earn, R. Alsaqour, M. Abdelhaq, T. Abdullah, "Searchable symmetric encryption: review and evaluation," Journal of Theoretical and Applied Information Technology, vol. 30, 2011.

[6] R. Koletka, A. Hutchison, "An architecture for secure searchable cloud storage," IEEE, Information Security South Africa (ISSA), pp. 15-17, Aug., 2011.

[7] E. Stefanov, C. Papamanthou, E. Shi, "Practical Dynamic Searchable Encryption with Small Leakage," IACR Cryptology ePrint Archive, 2013.

[8] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," INFOCOM, 2010 Proceedings IEEE, Dept. of ECE, Illinois Inst. of Technol., Chicago, IL, USA , Mar. 2010.

[9] J. Bringer, H. Chabanne, B. Kindarji, "Error-tolerant searchable encryption," Communication and Information Systems Security Symposium, International Conference on Communications (ICC), Dresden, Germany, pp. 14-18, Jun. 2009.

[10] J. Yu, J. Li, X. Wang, W. Gao, "Conjunctive Fuzzy Keyword Search Over Encrypted Data in Cloud Computing," TELKOMNIKA Indonesian Journal of Electrical Engineering, vol.12, no.3, pp. 2104-2109, Mar. 2014.

[11]S. R. Chidamber and C. F. Kemerer, „„A metrics suite for object oriented design,"" IEEETrans. Softw. Eng., vol. 20, no. 6, pp. 476–493, Jun. 1994.

[12] R. Harrison, S. J. Counsell, and R. V. Nithi, „„An evaluation of the MOOD set of object-oriented software metrics,"" IEEE Trans. Softw. Eng., vol. 24, no. 6, pp. 491–496, Jun. 1998.

[13] R. V. Binder, „„Design for testability in object-oriented systems,"" Comms. ACM, vol. 37, no. 9, pp. 87–101, Sep. 1994.

[14] S. Purao and V. Vaishnavi, „„Product metrics for object-oriented systems,"" ACM Comput. Surveys, vol. 35, no. 2, pp. 191– 221, Jun. 2003.

[15] M. Lorenz and J. Kidd, Object-Oriented Software Metrics: A Practical Guide. Upper Saddle River, NJ, USA: Prentice-Hall, 1994.