International Journal of Research

p-ISSN: 2348-6848

e-ISSN: 2348-795X

Volume 08 Issue 03

March 2021

Advanced Encryption Standard Encryption Scheme based Secure Data Search in Cloud Services

Shruti Bhawsar
M.Tech. Scholar
Department of Computer Science and Engineering
Lakshmi Narain College of technology,
Indore (M.P.)
shrutibhawsar95@gmail.com

Khushboo Sawant
Assistant Professor
Department of Computer Science and Engineering
Lakshmi Narain College of technology,
Indore (M.P.)
khushboosawant2019@gmail.com

ABSTRACT: Searchable symmetric encryption (SSE) has been extensively explored in cloud storage, enabling cloud services directly. Search for encrypted data. Most SSE solutions are only suitable for honest but curious cloud services and will not differ. Because storage outsourcing is not trusted, this assumption is not always true in practice. To address this issue, research has been conducted into Verifiable Searchable Symmetric Encryption (VSSE), which prevents and Realize cloud services by enabling performance confirmation. However, as far as we know, the applicability of the existing VSSE scheme is very limited. For example, it only supports static databases, requires a specific SSE structure, or works only in a single-user model. In the text propose GSSE, which is the first universal verifiable SSE scheme in the single-user multi-user model. This scheme can be anyone SSE program and additional support data update. To generally support confirmation of results, we first decouple the evidence index in the GSSE from SSE and Incremental Hash to build an evidence index with data update support. A timestamp chain has also been developed to maintain data freshness across multiple users. Careful analysis and experimental evaluation Shows that GSSE is secure and introduces a small amount of overhead for performance verification.

Key words –GSSE, SSE, cloud, encryption, decryption, cloud server

I INTRODUCTION

In recent days, Cloud storage has become good entrant for organizations that suffer from resource limitation. Cloud computing is a procedure that surveys internet founded computing. The cloud computing method is used to lessen data organisation cost or time. In addition, cloud computing is used to store data that can be retrieved in remote areas. The most challenging task in the cloud is to ensure availability, integrity, and secure file transfer. The motivation for cloud computing was needed for complex intensive application run by large

scale organization like governments. Those organizations require more computational, network and storage resources then a single computer. Using cloud computing data possessors diffuse data concluded cloud servers to individual users. The use of cloud computing procedure affects the security of the transmission of data. The encryption or decryption procedures to transmit data safely through the cloud servers Data owners encrypt data using encryption algorithms or forward the data to the cloud servers.[15][17][19] After encryption, the data is diffused to cloud attendants where data cannot be accessed directly and diffused to the individual users using precise searching technique. The National Institute of Standards or Technology (NIST) proposed most famous definition of cloud computing. NIST tells us that cloud figuring is a model for allowing an on-demand network to contact a common variable computing resource pool that can be configured highly or unconfined with minimal organisation effort or interaction between service providers Due to factors such as unreliable services and malicious attacks from hackers, recent developments in cloud computing have added value over data security. Recently, major cloud infrastructure providers have reported many cases of server damage. Data leaks from important cloud services also occur from time to time. In addition, cloud service providers actively control customer data for various motives. From the customer's perspective, the cloud is therefore neither secure nor reliable.[12][11] Without strong security, privacy and reliability guarantees, despite financial savings and service flexibility, it is difficult to expect cloud customers to deliver their data rights to cloud servers. Since last few years, cloud computing has made a speedy development. Cloud figuring provides users with a wide choice of incomes via the Internet, such as computing power, computer platforms, storage, or requests. The largest cloud providers in recent market section include Amazon, Google, IBM, Microsoft, sales teams, etc. As more and more companies take advantage of using resources in cloud, it is necessary to defend data from dissimilar users. Some of the biggest challenges facing cloud subtracting are the protection, protection or processing of data belonging to users' property. Below we describe the two main modes for storing data in cloud: when data is active (transmitted), and when data is static, people expect the data to be more protected in it. The following are two main scenarios we focus on to recognise security of data in cloud.[1][3]

II RELATED WORK

In this article, the author has used extensive research to conclude that the safety and privacy of physical, environmental and virtual security is the responsibility of the seller. This article argues that organizations can control the three major phases of physical, logical, and business processes to address central threats, cyber security and internal security. The author proposes an automated management plan that aims to address security concerns in the calculation of threat threats by establishing relationships between CSPs based on existing attacks. The author also recommends that users should be responsible for ensuring security of data center in the cloud, enforcing policy monitoring, improving users' understanding of security practices. Extending, resolving disputes,

managing legal matters, evaluating capabilities and providing solutions. we talked about purpose of this emerging cloud-based technology, which provides common sources and services for lower prices and software when using cloud services, and some security issues. In addition, while emphasizing the multi-tasking, the CSA's cloud-based data security issues were also addressed. The authors conclude that security issues with cloud computing can be mitigated by modifying or designing a proprietary architecture for many cloud applications [3][8][10]

Than MyoZaw et.al (2019) a database is a collection of organized data. Although there are various types of technologies (such as encryption and electronic signature) that can be used to protect data during cross-site transmission. Data protection refers to the common procedures used to defender safeguard data or data management software against illegal use or threats or malicious occurrences. In this article, we create 6 different ways to store and retrieve data information in a safe and efficient way in a more secure way. Discretion, integrity or accessibility (also known as three-in-one CIA) are models designed to guide information intelligence policies. There are many encryption technologies available, and ECC is one of the most powerful. Users want to store or request data, and users need to be verified. The verified user will receive the key of the main generator, and then the data must be encrypted or decrypted into database. Each key is stored in a large generator or retrieved from the key generator. Use 256-bit AES for high-level extraction, column-level theft, and component level analysis in database. The next 2 methods are to use 521-bit ECC encryption and signalling to encrypt high-level encryption or high-level encryption in the field using 256-bit AES encryption keys. The last technique is safest method in this article. This method uses AES and ECC encryption for component-level encryption to ensure confidentiality and uses ECC signatures for each component in database to ensure authenticity. In addition to translating data at interruptions, it is also significant to ensure that personal data is converted during network traffic to prevent database signatures. The advantage of the element level is difficult to attack, because attacker key will lose only one element. Loss requires thousands of keys to manage.[1]

Feng Shengwu et al. (2018), the level of information security in the cloud computing environment directly affects the data protection issues of users. Using an encryption algorithm with its unique features can compensate for the errors caused by relying on security software security strategies, further convincing them Difficulties and challenges in protecting information. By examining the basic concepts of elliptic curve encryption algorithm, the encryption algorithm curve based on cloud data protection technology creates a more efficient way to ensure the performance of available systems. safe and effective, and conducts security testing. Built with Matlab 9 software. The outcomes show that cloud-based encryption knowledge based on the ECC algorithm has high security or speed, or can effectively protect safety and security of cloud data.[2]

III PROPOSED SYSTEM

Design a generic verifiable SSE scheme that enables verifiable searches on the three-party model. In particular, the scheme should satisfy the following privacy and efficiency requirements: 1) Confidentiality: The confidentiality of data and keywords is the most important

International Journal of Research

p-ISSN: 2348-6848

e-ISSN: 2348-795X

Volume 08 Issue 03

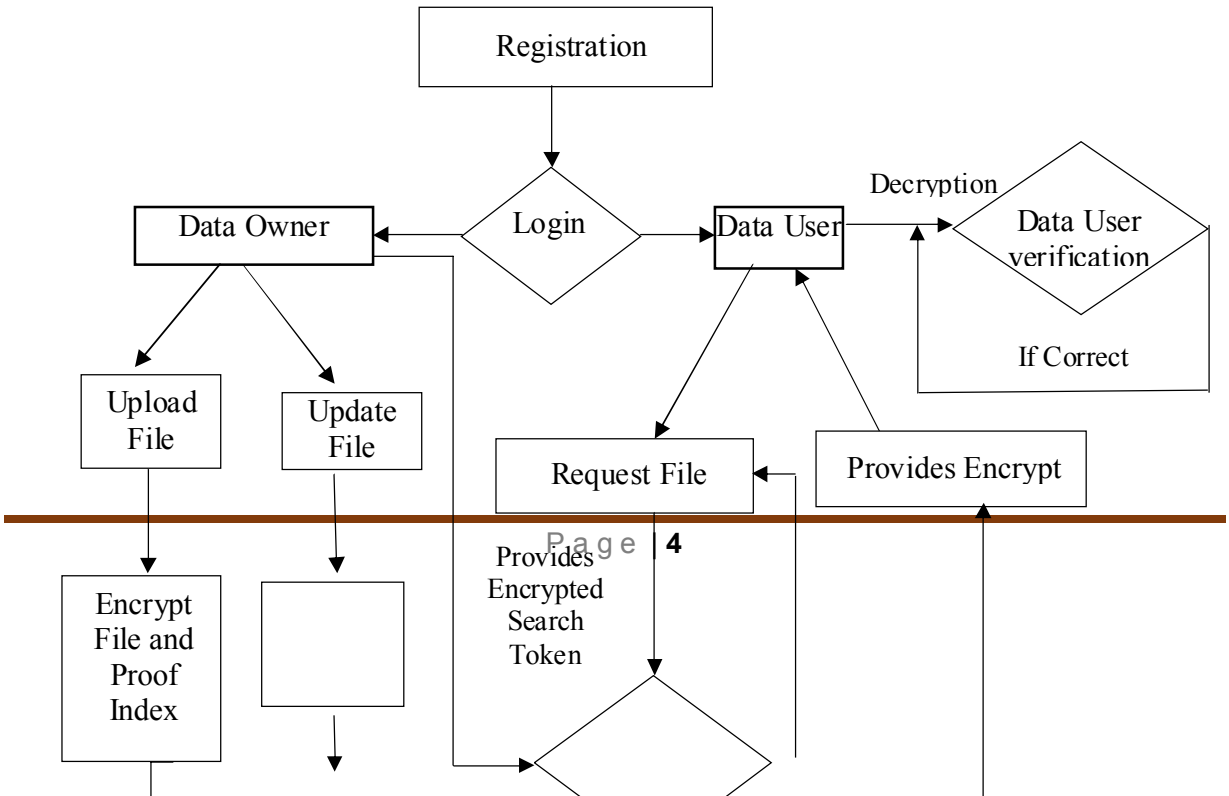
March 2021

privacy requirements in SSE. It ensures that users' plaintext data and keywords cannot be revealed by any unauthorized parties, and an adversary cannot learn any useful information about files and keywords through the proof index and update tokens used in GSSE. 2) Verifiability: A verifiable SSE scheme should be able to verify the freshness and integrity of the search results for users. 3) Efficiency: A verifiable SSE scheme should achieve sub linear computational complexity

The data owner first citations keywords of each article or build a keyword directory. He/she encrypts papers as well as keyword index. The data owner blocks the file and password folders locked in the cloud. Data users can obtain individual results, evidence or key credentials in public, and they or others can verify the accuracy, reliability and validity of the search results without decryption. The advantage of a cloud computing equity service is that it provides reliable returns on investment, but the losses are even greater. Compared to traditional computer technology, cloud computing has various advantages. Cloud computing provides customers with supercomputing and high-end devices at affordable prices

We aim to develop a verifiable SSE scheme, i.e., GSSE, that allows the index used for search result verification to be separated from the one used for the SSE operations. Therefore, GSSE is decoupled from the existing SSE schemes. In particular, data owner will builds an encrypted index based on the Merkle Patricia Tree (MPT) and upload it to cloud services, which enables data users to verify the integrity of search results. Meanwhile, data owner will also upload a timestamp-chain based on the root of MPT to ensure data freshness across multiple users. GSSE is defined as follows. Definition 3 (GSSE Scheme). In a GSSE scheme, there are three parties, i.e., data owners, authenticated users and an untrusted server. A data owner provides a proof index and an authenticator to the untrusted server such that it allows the server to provide a proof of the search result and authenticators for the authenticated users to ensure the integrity and freshness of the SSE search results.

.



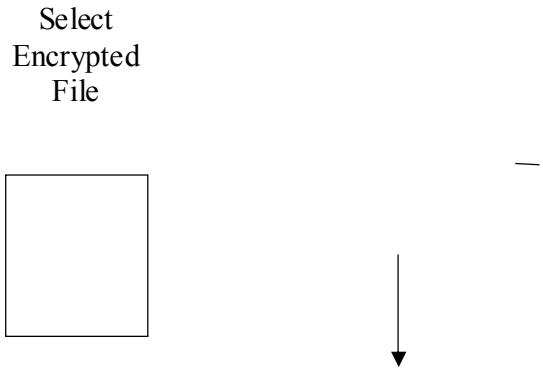


Fig.1 Proposed architecture diagram

IV MODULES DESCRIPTION

Registration: This is the process of registering or registering to cloud. To take benefit of cloud documents, all data owners and data users must register. During this process, your basic information (such as email, contacts, etc.) will be collected and stored in the cloud. During the registration process, a particular user's cloud ID is generated automatically.

Cloud ID: Each user must produce a Cloud ID or use it to classify an identifier with near security. The identifier does not repeat the identifiers that have been or will be twisted to identify other identifiers. Therefore, the information marked with Cloud ID by liberated parties can later be collective into a single folder or transmitted on same channel without the need to tenacity struggles among identifiers

Data Owner: Data Owner extracts keywords of each article or also figures a keyword Index. Data Owner encrypts documents r keyword Index using a key and outsources in Cloud.Data Owner provides the Public Verification Key and Proof Index to the Data User via Cloud for document verification. Data Owner is the only authorized person to add, modify, or delete the document(s) from the cloud.

Cloud Service Provider: The cloud service provider can see all uploaded or transferred documents in cloud. CSP obtains document request from the data user, verifies identity before granting permission, and then CSP executes query or revenues encrypted document based on search token, or also returns document with other evidence on document to confirm search results.

Public Verification Key: Public verification key is a safety quantity planned to make sure that your document outsourced in cloud doesn't get hacked. By confirming public key, the Data Owner and the Data User adding added cover of defence to documents or files in the cloud by authorising each other's identities.

Data User: Data User send a appeal to the cloud server.After request granted from the Cloud, the Data User receiving the Public Verification Key from the Cloud generated by Data Owner. The Data User now decrypts and downloads the encrypted documents, after verifying with the Public Verification Key. After receiving verification from cloud, the data user will download the file within a particular time limit.

Verification with Proof Index: It is a proof generating system for verifying cloud search by Public Verification Key; here data users or others can confirm accuracy of search result by Verification key

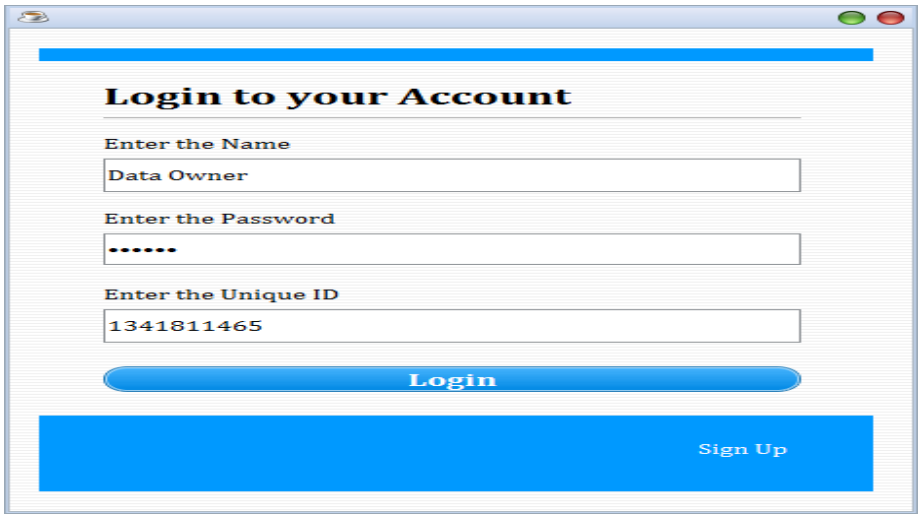


Fig.2 Registration

International Journal of Research

p-ISSN: 2348-6848

e-ISSN: 2348-795X

Volume 08 Issue 03

March 2021

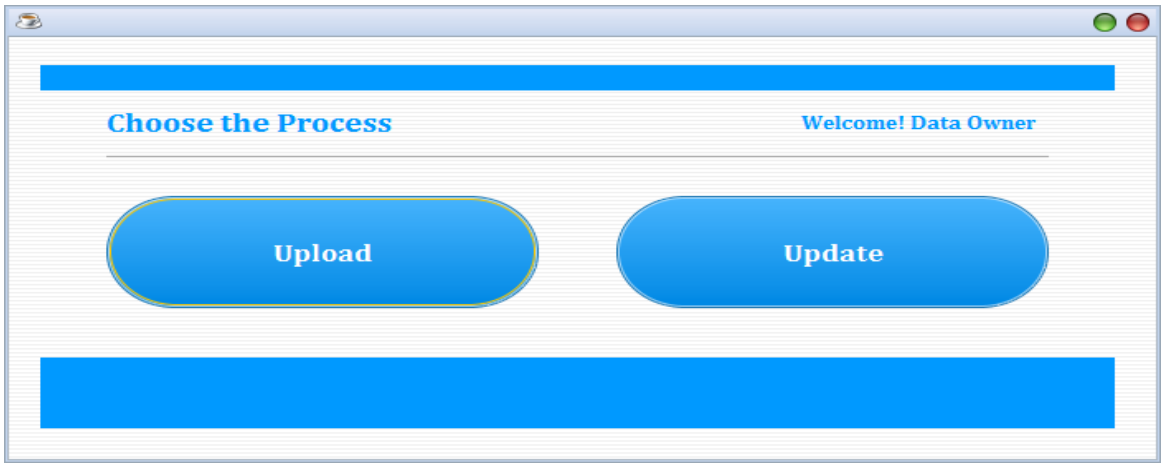


Fig.3 Upload file

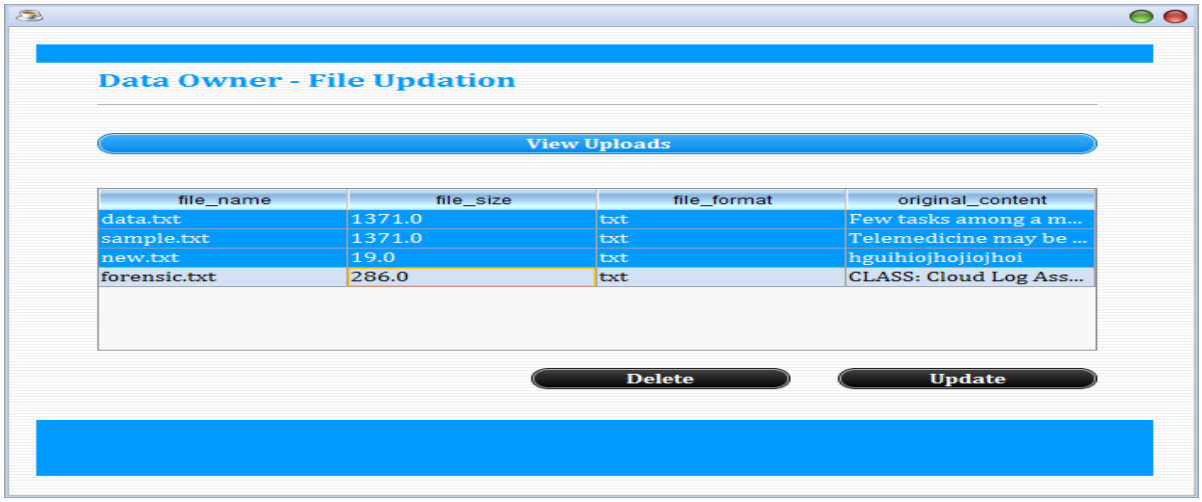


Fig.4 File updation

International Journal of Research

p-ISSN: 2348-6848

e-ISSN: 2348-795X

Volume 08 Issue 03

March 2021

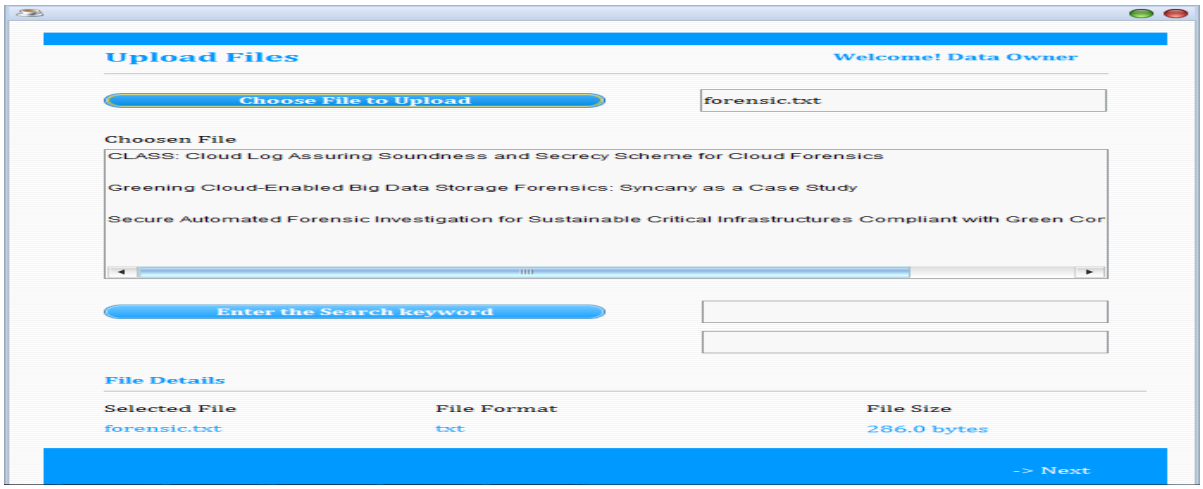


Fig.5 Upload data

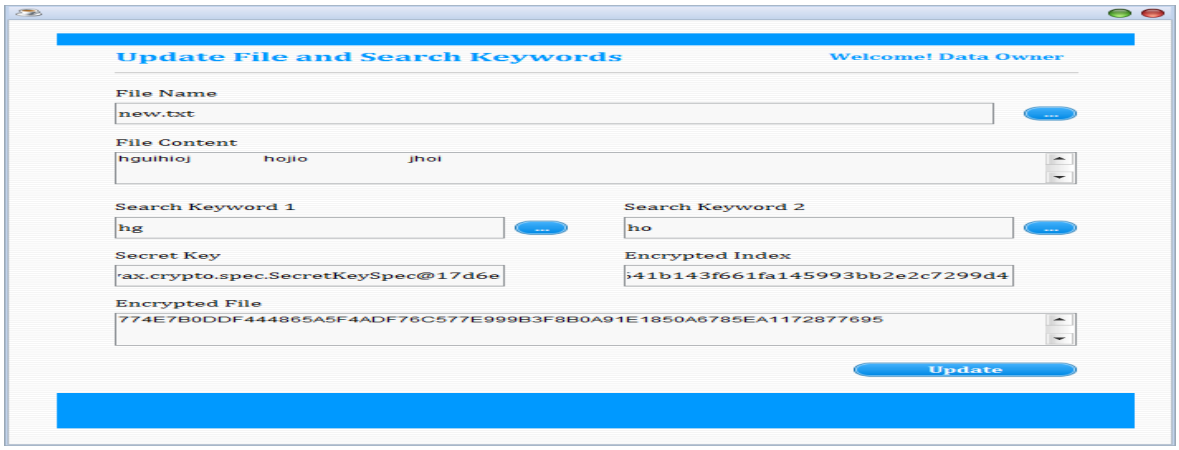


Fig .6 Search Keywords for Upload File

International Journal of Research

p-ISSN: 2348-6848

e-ISSN: 2348-795X

Volume 08 Issue 03

March 2021

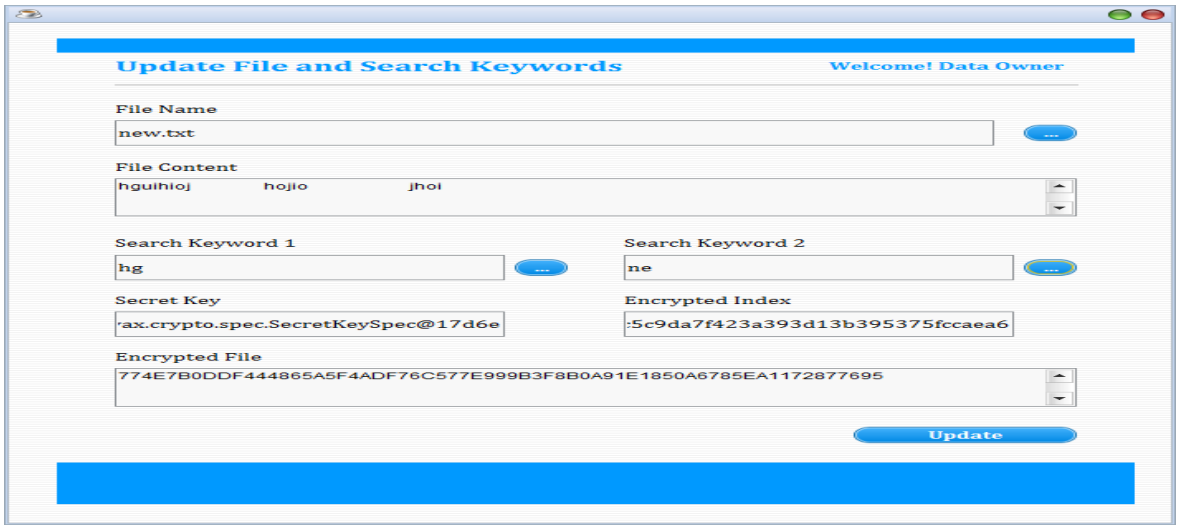


Fig.7 Upload File And Search Keywords

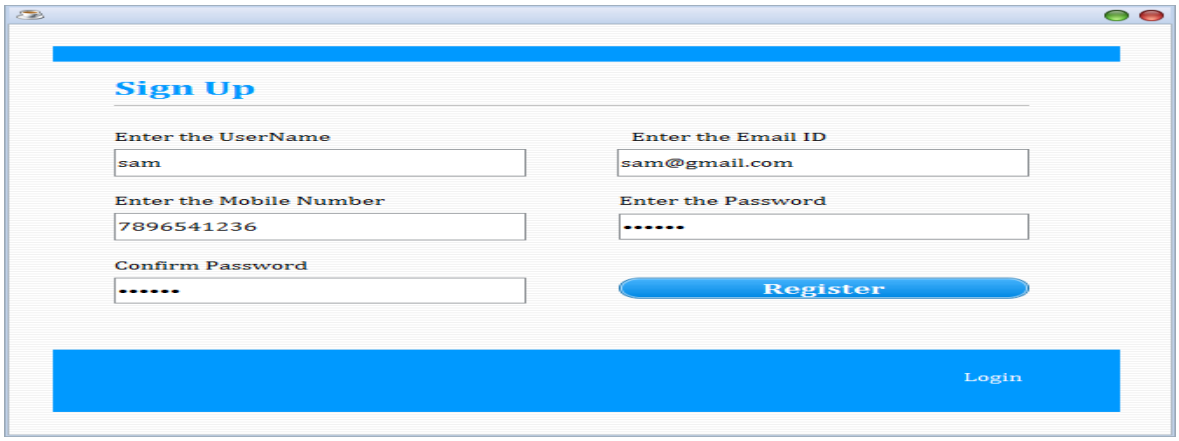


Fig.8 Signup

International Journal of Research

p-ISSN: 2348-6848

e-ISSN: 2348-795X

Volume 08 Issue 03

March 2021

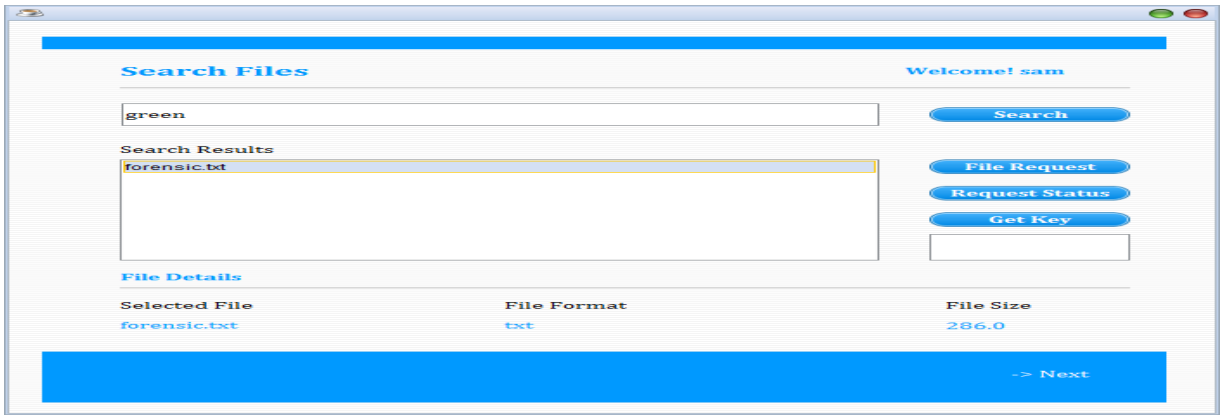


Fig .9 Search File

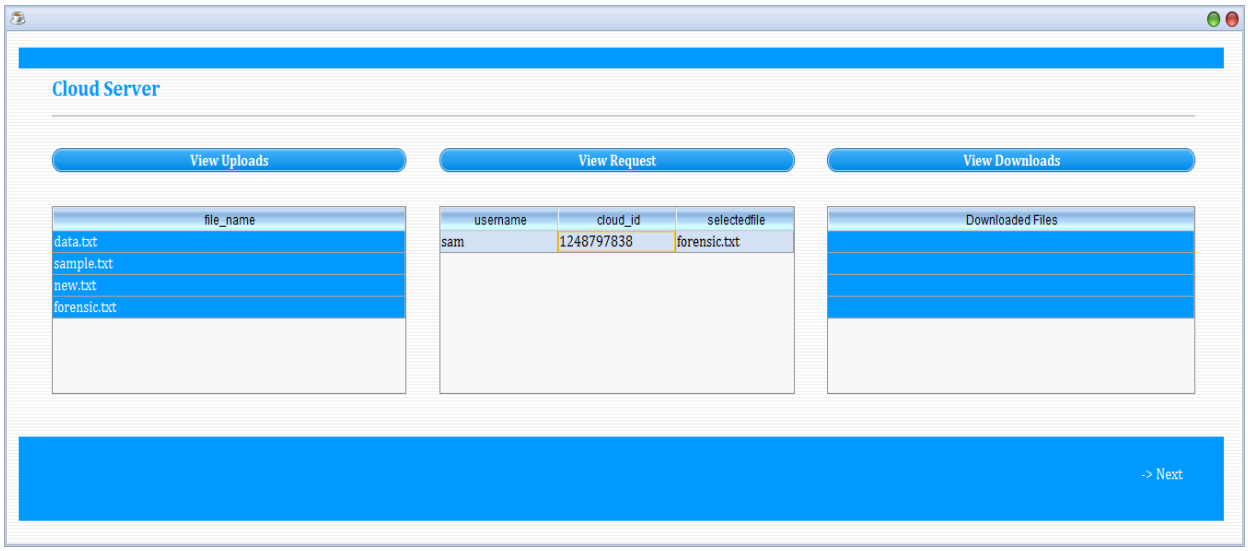


Fig.10 Cloud Server

International Journal of Research

p-ISSN: 2348-6848

e-ISSN: 2348-795X

Volume 08 Issue 03

March 2021

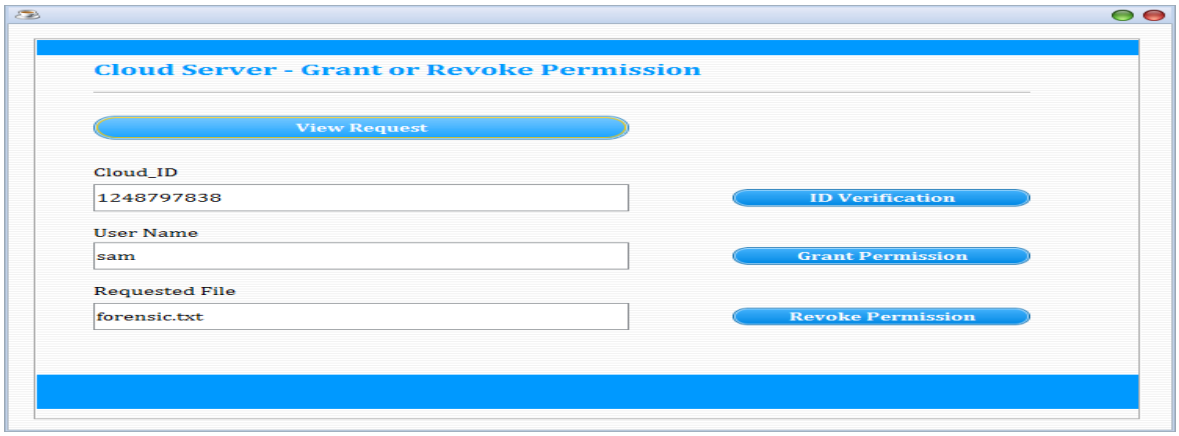


Fig .11 Cloud Server Grant Revoke

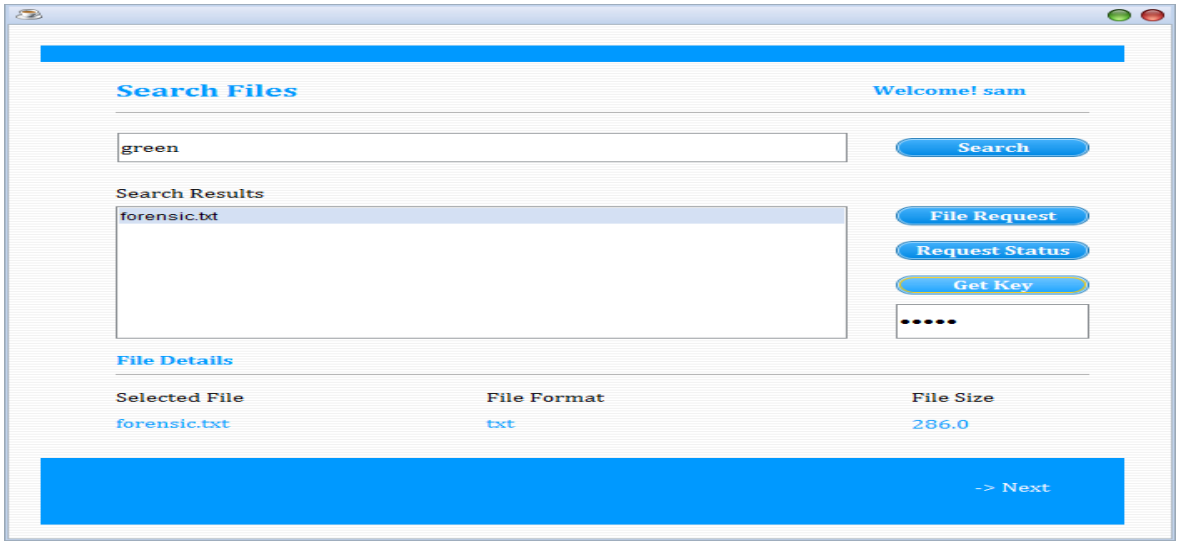


Fig.12 Authentication

International Journal of Research

p-ISSN: 2348-6848

e-ISSN: 2348-795X

Volume 08 Issue 03

March 2021

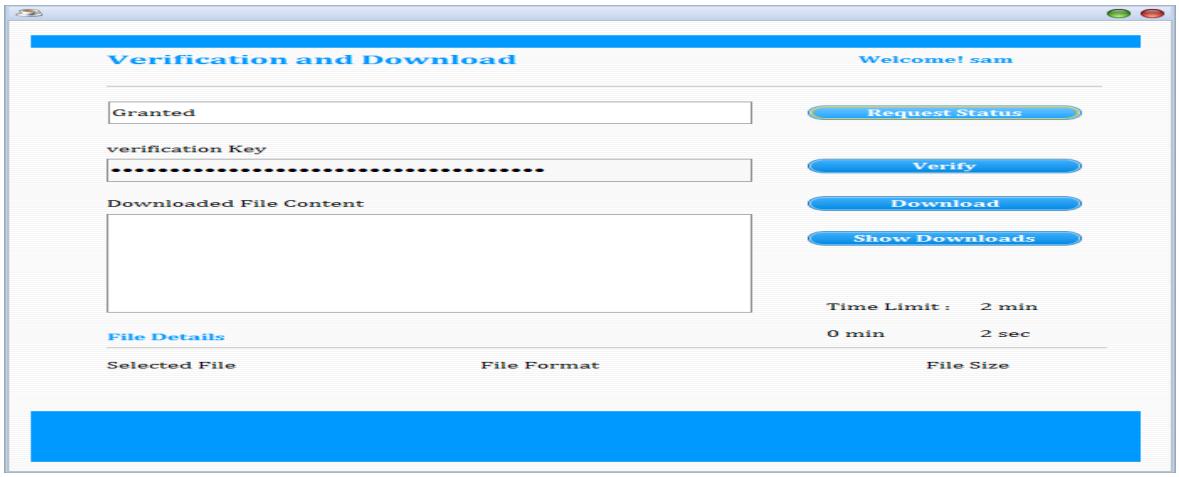


Fig 13 Data User – Received Public verification Key from CSP

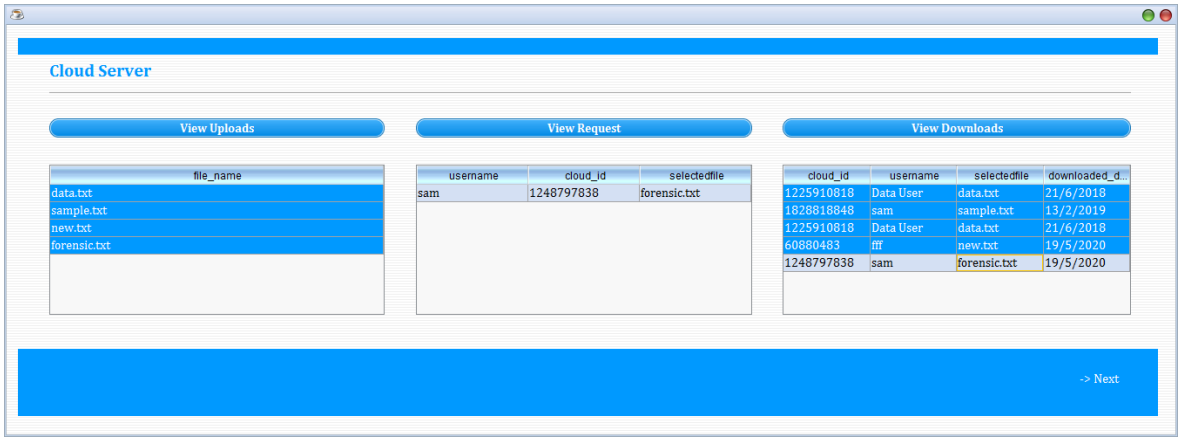


Fig 14 Cloud Server

In this work, we focus on the problem of verifiable searchable encryption under a multi-user setting. A GSSE scheme is proposed which can support verifiability of search result even when both the data owner. The experimental results denote that our scheme can achieve security goals for data owner-server collusion while maintaining a comparable performance.

Table 1 Comparison Table with Existing Technique

	Previous Work	Proposed Work
Technique	Multi-Key Searchable Encryption	GSSE

	(MKSE)	
Language	Java language	Java language
Searching for documents	Token Gen phase	Keyword generation
Time	1400ns	2 sec

V CONCLUSION

Even cloud computing offers many benefits to users, but due to safety issues, many users are still reluctant to use it or service providers may also encounter unauthorized access issues. Therefore, we propose a new framework by combining encryption and disguise technologies to address issues related to users and service providers. Before sending data via Cloud encryption, it can provide security for data converted in the network so that the users can ensure the discretion of their data. We suggest a secure storing server that can track user keys and hash values for documents uploaded by the server. For cloud providers, an effective disguise technique is proposed through which the client's secret information (such as passwords, contact information, etc.) is not controlled by a third party. The steps of the algorithm are also determined to ensure that the operation works efficiently. More and more people and communications companies are integrating data into remote servers or reducing problem of storing and maintaining local data. Uncertainty as to how to ensure security in the external computer environment has led to security issues such as authentication, licensing, existence, trust, confidentiality and anonymity. In this article, we focus on privacy, security and access to the cloud computing environment. While cloud security services can be well-designed and succeeded by experts, they can provide effective organisation or threat valuation services. Though, threats we are discussing here show that the implementation of present security mechanisms in the cloud should be carefully considered. In order to accelerate the development of cloud computing, many improvements to existing mechanics are needed, and new innovation systems need to be established. we plan to cover the planned work to other parts of cloud. Cloud computing brings various tasks for structure or submission developers, engineers, system administrators and service providers.

REFERENCES

1. Vahid Ashktorab and Seyed Reza Taghizadeh, ―Security Threats and Countermeasures in Cloud Computing, International Journal of Application or Innovation in Engineering and Management (IJAIEM), Volume 1, Issue 2, October 2018.

2. Cloud Security Alliances, —Top Threats to Cloud Computing V1.0□, Cloud Security Alliances, Version 1, Page No. 3, March 2017.
3. Wiiliam R Claycomb and Alex Nicoll, —Insider Threats to New Research Challenges‖ , CERT. Wayne A. Janssen, —Cloud Hooks: Security and Privacy Issues in Cloud Computing —, 44th Hawaii International Conference on System Sciences, January 2015
4. Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zahria, A view of Cloud Computing ||, Communications of the ACM, Volume 53, Issue 4, April 2016
5. E. Kirda, C. Kruegel and G. Vigna, —Cross-Site Scripting Prevention with Dynamic Data Tainting and Static Analysis ||, Proceeding of the Network and Distributed System. 2014
6. Shengmei Luo, Zhaoji Lin, Xiaohua Chen, Zhuolin Yang and Jianyong Chen,Virtualization Security for Cloud Computing Services ||, International Conference on Cloud and Service Computing, December 2011.
7. Albert B Jeng, Chien Chen Tseng, Der-Feng Tseng and Jiunn-Chin Wang, —A Study of CAPTCHA and its Application to user Authentication ||, Proceeding of 2nd International Conference on Computational Collective Intelligence: Technologies and Applications, 2010
8. A. Liu, Y. Yuan and A Stavrou, ||SQLProb: A Proxybased Architecture toward Preventing SQL Injection Attacks ||, SAC, March 2009.
9. D. Gollmann, —Securing Web Applications‖ , Information Security Technical Report, Volume 13, Issue 1, 2008 153
10. Mike Ter Louw and Venkatakrishnan V.N. BluePrint: Robust Prevention of Cross-Site Scripting Attacks for Existing Browsers ||, 30th IEEE Symposium on Security and Privacy, May 2009
11. Zouheir Trabelsi, Hamza Rahmani, Kamel Kaouech and Mounir Frikha, —Malicious Sniffing System Detection Platform ||, Proceedings of the 2004 International Symposium on Applications and the Internet, 2004
12. Flavio Lombardi and Roberto di Pietro, —Secure Virtualization for Cloud Computing‖ , Journal of Network and Computer Applications, Academic Press Ltd. London, UK, Volume 34, Issue 4, July 2011.
13. Hanqian Wu, Yi Ding, Winer C. and Li Yao, ||Network Security for Virtual Machine in Cloud Computing ||, 5th International Conference Information Technology, Seoul, December 2010.
14. SAVVIS, —Securing the Cloud A Review of Cloud ComputingSecurity Implications and Best Practices ||, VMWARE WHITE PAPER, SAVVIS.
15. Ruiping Lua and Kin Choong Yow, —Mitigating DDoS Attacks with Transparent and Intelligent Fast-Flux Swarm Network ||, IEEE Network, Volume 25, Number 4, August 2011.
16. Aman Bakshi and Yogesh B. Dujodwala, —Securing Cloud from DDoS Attack using Intrusion Detection System in Virtual Machine ||, ICCSN‘ 10 Proceeding of the 2010 Second International Conference on Communication Software and Network, 2010

17. Tebaa, M.; El Hajji, S.; El Ghazi, A., "Homomorphic encryption method applied to Cloud Computing," in Network Security and Systems (JNS2), 2012 National Days of , vol., no., pp.86-89, 20-21 April 2012
18. Mather, Tim, Subra Kumaraswamy, and Shahed Latif. Cloud security and privacy: an enterprise perspective on risks and compliance. " O'Reilly Media, Inc.", 2009
19. Samyak Shah, Yash Shah, Janika Kotak, "Somewhat Homomorphic Encryption Technique with its Key Management Protocol", Dec 14 Volume 2 Issue 12 , International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC), ISSN: 2321-8169, PP: 4180 - 4183
20. Ramaiah, Y. Govinda, and G. Vijaya Kumari. "Efficient public key homomorphic encryption over integer plaintexts." Information Security and Intelligence Control (ISIC), 2012 International Conference on. IEEE, 2012.