International Journal for Rapid Research in Engineering Technology & Applied Science
Vol IX Issue VII July 2023
ISSN Online:- (2455-4723)

Cloud Data Security and privacy based on AES and SHA hash -256 Based Technique

Poonam Singh rajput ,M.Tech. Scholar
Deepak Mishra ,Assistant Prof.
Department - Computer Science Engineering
VNS Faculty of Engineering Bhopal

Abstract: Cloud data security and privacy are crucial concerns for individuals and organizations as they entrust their sensitive data to third-party cloud service providers. Encryption is one of the commonly used techniques for ensuring cloud data security, and Advanced Encryption Standard (AES) and Secure Hash Algorithm (SHA) are widely used cryptographic algorithms for securing cloud data. AES is a symmetric-key block cipher encryption algorithm that provides a high level of security. It works by transforming plaintext into ciphertext using a symmetric key, making it unreadable to anyone without the key. On the other hand, SHA-256 is a hashing algorithm that generates a unique 256-bit hash value for a given input. This hash value can be used to verify the integrity of the data and ensure that it has not been tampered with. This paper presents a simulation-based study of cloud data security and privacy based on AES and SHA-256 techniques. The simulation is done in NetBeans, an integrated development environment (IDE) that allows developers to write, compile, and test code. The simulation involves writing a program to encrypt data using AES and generate a SHA-256 hash value for the encrypted data. The effectiveness of the AES and SHA-256-based technique in securing cloud data is evaluated based on several parameters, such as encryption and decryption time, throughput, and the quality of the generated hash value. The simulation results show that the AES and SHA-256-based technique provides a high level of security and is efficient in securing cloud data.

Keywords: AES-**, SHA hash -256, Paper Specifications,** Cloud Data Security, encrypted data

I INTRODUCTION

The term "cloud computing" refers to a type of utility computing that uses an unlimited number of virtualized resources to build a custom infrastructure or platform that can be used to run applications or full parts of services on a pay-per-use basis. Cloud computing has made the traditional way of putting systems in place obsolete. Advanced system implementations can be hidden from the end user by using virtualization techniques. When resources are virtualized, it makes it seem like the system can grow and be used everywhere [1,2]. Cloud computing makes the long-held dream of utility computing a reality by using a pay-as-you-go pricing model and systems that can be expanded indefinitely and are available everywhere. Developers who have new ideas for new Internet services don't have to spend a lot of money to put up the hardware and software they need. Computing in the cloud refers to all of the applications that are offered as a service over the internet, as well as the hardware infrastructure and platform on which these applications are built. Formally, the hardware infrastructure is called a "data centre," and it includes a wide range of physical devices, from personal computers all the way up to high-end server machines [3].

Many of us have foolishly accepted as true the idea that "cloud computing" is nothing more than the Internet with a fancy new name. Most of the time, this is caused by multiple drawings of a web-based app, which is usually shown as a cloud. The idea of computing in the cloud is based on the idea that real-world resources can be combined and shown as if they were virtual. This new way of thinking makes it possible to stage applications and give freelance users access to platform services. When you look at the history of cloud computing up until now, it's clear that the development of the technology itself is the result of a lot of different standards coming together. Cloud computing promise of measurable results changes the way that services and apps are made available in a fundamental way. Even though they are not standards, the industry makes their own systems that lock in the merchandiser. Since customers don't have to be locked into a single system, there is a strong push in the industry to develop cloud computing based on industry standards. The cloud computing industry now works with these standards in place: Some of the things that will be talked about in this presentation are platform virtualization of resources, service-oriented design, Web-application frameworks,

preparation of open-source software systems, standardized Internet services, and involuntary systems. One of the best things about cloud computing is that it has led to a shift away from capital investments and towards operating expenses. This has the benefit of making growth independent of having money on hand or the need to have access to capital. In addition, the cloud hosting provider takes on the risk instead of the company.SLAs, which stands for "Service Level Agreements," is an important part of cloud computing. SLAs are basically a running agreement you have with any provider [4]. The ability of cloud computing to turn capital expenses into operational expenses by using an elastic usage rating system that can be scaled to the right level is a big part of cloud computing price proposition and makes this model very appealing. The process of turning physical assets into their digital counterparts protects against having either too little or too much infrastructure. By putting spending in the operational costs section of the budget, a company can basically pass the risk on to the cloud computing provider[5-9].

The problem of how to divide up resources has been talked about in many different areas of computing, such as operating systems, grid computing, and the management of data centres. In cloud computing, a Resource Allocation System (RAS) is often defined as any way to make sure that the infrastructure provided by a service provider meets the needs of an application in the right way. In addition to giving the developer this guarantee, the systems that handle resource allocation should also take into account how each resource in the cloud environment is doing right now. This will make it possible to use algorithms to better assign physical and/or virtual resources to the apps that developers make, which will save money on keeping the cloud environment running. Most of the time, there are two parts to how virtual machines are given out: In the first part of the process, the most recent requests for virtual machines and the placement of virtual machines on hosts are accepted. The second part is to find the best way to use the virtual machines that are already being used. The allocation part of the algorithm is as complicated as n times the number of hosts, where n is the number of virtual machines that need to be given a place and m is the number of hosts. Optimizing the resources that are currently available for virtual machines (VMs) is done in two steps. In the first step, virtual machines that need to be moved are chosen. In the second step, an allocation algorithm puts the chosen virtual machines on the host machine. The virtual machine placement algorithm makes sure that virtual machines are put on real host machines in the most efficient and cost-effective way possible.[10-12]

II RELATED WORK

Thangavel M, Varalakshmi 2019 cloud Computing enables the remote users to access data, services, and applications in on-demand from the shared pool of configurable computing resources, without the consideration of storage, hardware and software management. On the other hand, it is not easy for cloud users to identify whether (CSP) tag along with the data security legal expectations. So, cloud users could not rely on CSP's in terms of trust. So, it is significant to build a secure and efficient data auditing framework for increasing and maintaining cloud users trust with CSP. Researchers suggested introducing Third Party Auditor (TPA) on behalf of cloud user for verifying the outsourced data integrity, which may reduce the computation overhead of cloud users. In this work, we proposed a novel integrity verification framework for securing cloud storage based on Ternary Hash Tree and Replica based Ternary Hash Tree (R-THT), which will be used by TPA to perform data auditing. Differing from existing work, the proposed framework performs Block-level, File-level and Replica-level auditing with tree block ordering, storage block ordering for verifying the data integrity and ensuring data availability in the cloud. We further extend our framework to support error localization with data correctness, dynamic updates with block update, insert and delete operations in the cloud. The structure of THT and R-THT will reduce the computation cost and provide efficiency in data updates compared to the existing schemes.security analysis of the proposed public auditing framework indicates the achievement of desired properties and performance has been evaluated with the detailed experiment set. The results show that the proposed secure cloud auditing framework is highly secure and efficient in storage, communication and computation costs.[13].

Shilpi Mishra et.al. (2021) : Amazon gives businesses a wide range of IT solutions that allow them to build their own private virtual clouds while still having full control over their infrastructure. Amazon Web Services can be used by both businesses and people working on their own IT projects. Security professionals are drawn to the cloud because it is easy to use and can save them money. However, the cloud also poses a number of security and compliance challenges. As part of Amazon Web Services' (AWS) effort to make cloud computing easier for businesses in terms of security and compliance, EC2 instances have been created. People say that these instances can make cloud computing safe for businesses that have to follow a lot of rules. The use of cloud

computing has some problems, but these problems also give us a chance to learn more about a wide range of topics that are related to cloud computing. The security of users' private information and sensitive data while it is being processed and stored on the servers of cloud service providers is a major concern. In this paper, we talk about some of the research that has already been done on the safety and privacy of cloud computing. In this article, we learned more about the security problems that come with cloud computing and about the strategies and solutions that the cloud service industry has put in place to deal with them. The goal of this research was to shed light on the rapidly growing cloud services market as well as the different possible problems, such as network problems [14-16] .

III PROPOSED SYSTEM

In the proposed system there are some changes. Firstly we have to create virtual cloud environment to protect data with policy based management and valid solutions. Then before storing data on cloud we encrypt that and then implement AES algorithm for encryption.

Cloud data security is an important concern for both data owners and data users, as sensitive information can be at risk of theft or unauthorized access. One solution for protecting cloud data is to use encryption, and the Advanced Encryption Standard (AES) is a widely recognized encryption algorithm that can provide strong protection for data. In a proposed cloud data security system using AES, the data owner would encrypt their data using the AES algorithm before storing it in the cloud. The encryption process would use a secret key that is known only to the data owner and authorized data users. This key would be used to encrypt and decrypt the data, so only those with the key can access the data. To ensure the security of the data owner's key, it would be encrypted using a key management system. This system would store the key in an encrypted form and only release it to authorized data users upon request. The key management system would also monitor and log all key requests and key usages to ensure that only authorized users are accessing the data. Data users would need to be authorized by the data owner to access the encrypted data. They would be granted access to the encrypted data through the key management system, which would provide them with the decrypted key to access the data. Once they have the decrypted key, they can decrypt the data and access it.

A proposed cloud data security system using AES and a key management system can provide strong protection for cloud data, ensuring that only authorized users can access the data and that the data is secure both at rest and in transit.

With cloud computing, it is possible to store data and make keys. So, in our line of work, the person who owns the data uses that key to encrypt the important information based on the rules for access, and then stores that information in the cloud. The user is then responsible for decrypting the data. Before decryption can happen, the client must first prove who they are in the cloud. Then, the SHA algorithm is used to compare the keys. If they are the same, decryption is done. In the last phase, we'll figure out how well it works by looking at things like how long it takes to encrypt and decrypt 30 times. We were able to get around both the revocation problem in public key cryptography and the key escrow problem in identity-based encryption by using this method.

User Authentication and Authorization-The system authenticates and authorizes the user accessing the cloud storage to ensure that only authorized users can access the data. The system uses industry-standard authentication mechanisms such as username/password combinations or two-factor authentication for added security.

Data Encryption and Decryption-The system encrypts all data using the AES algorithm with a strong encryption key. This ensures that even if someone gains unauthorized access to the data, they will not be able to read it without the encryption key. The system uses a symmetric encryption model where the same key is used for both encryption and decryption. When a user uploads a file to the cloud, the system encrypts the file before storing it. When a user requests to download a file, the system decrypts the file using the encryption key and sends it to the user

Multi-User Support: The system supports multiple users accessing the same cloud storage. Each user has their own set of files that they can access. The system ensures that each user can only access their own files and cannot access files belonging to other users.

Data Integrity and Availability: The system ensures the integrity and availability of data by storing multiple copies of each file in different locations. This ensures that even if one copy of the file is lost, there are other copies available. The system uses techniques such as RAID and data backups to ensure that data is available and can be recovered in case of data loss.

File Updates: The system allows users to update their files easily. When a user uploads an updated file, the system encrypts the updated file and replaces the old file with the new one. Overall, this system provides a secure and reliable cloud storage solution that supports multiple users and ensures data confidentiality, integrity, and availability.

Data Owner: Assuming the system is built on top of a cloud storage provider and uses Cloud ID as a means of identifying data owners; here is a possible workflow for data owners working with the cloud:

Login: The data owner logs in to the cloud storage system using their Cloud ID credentials.

Secret Key Generation: The data owner generates a secret key that will be used to encrypt their files. The secret key is generated locally and is not shared with the cloud storage provider.

Proof Index Generation: The data owner generates a proof index that will be used to verify the integrity of their files. The proof index is generated locally and is not shared with the cloud storage provider.

Upload Encrypted File: The data owner encrypts their files using the secret key and uploads the encrypted files to the cloud storage system. The data owner also uploads the proof index to the cloud storage system to allow for future verification of the file's integrity.

Delete File: If the data owner wants to delete a file from the cloud storage system, they initiate the delete process, and the file is removed from the cloud storage system. The proof index is also deleted to prevent future verification of the deleted file's integrity

Update File: If the data owner wants to update a file, they download the existing encrypted file from the cloud storage system, update the file locally, re-encrypt the file using the same secret key, and upload the new encrypted file to the cloud storage system. The proof index is updated to reflect the changes made to the file.

Data User : Assuming the system is built on top of a cloud storage provider and uses Cloud ID as a means of identifying data users; here is a possible workflow for data users working with the cloud.

Registration: The data user registers with the cloud storage system by providing their details, including their Cloud ID, and creating a password.

Login: The data user logs in to the cloud storage system using their Cloud ID and password.

View File: The data user can view the list of files available to them in the cloud storage system.

Request File: If the data user wants to download a file, they select the file they want to download and initiate a request for the file.

View Status: The data user can view the status of their file request, such as whether it has been approved or denied.

Proof Verification: Once the data user's file request is approved, they can download the encrypted file from the cloud storage system. The data user then verifies the integrity of the file using the proof index provided by the data owner.

Download Decrypted File: After verifying the proof index, the data user can decrypt the file using the secret key provided by the data owner and download the decrypted file to their local system.

Simulation Procedure

- The data owner creates a new file object and uploads it to the cloud storage system.
- The cloud storage system receives the file and encrypts it using AES encryption.
- The cloud storage system generates a proof index and sends it to the data owner to verify the integrity of the file.
- The data owner receives the proof index and verifies the integrity of the file.
- The data user requests to download the file from the cloud storage system.
- The cloud storage system sends the encrypted file and the secret key to the data user.
- The data user receives the encrypted file and the secret key.
- The data user verifies the proof index to ensure the integrity of the file.
- The data user decrypts the file using the secret key and downloads the decrypted file.

Modules:

- Registration
- Data Owner
- Cloud Service Provider
- Data User

Registration

The registration module would typically include a user interface for users to enter their information, such as name, email address, and other relevant details. The module would then validate this information to ensure that it is accurate and complete. Once the information has been validated, the module would create a unique user ID or cloud ID for the user, which would be used to identify the user in the system.

The registration module may also include features such as email verification or two-factor authentication to ensure that the user's account is secure. Additionally, the module may allow users to manage their account settings, such as changing their password or updating their contact information.

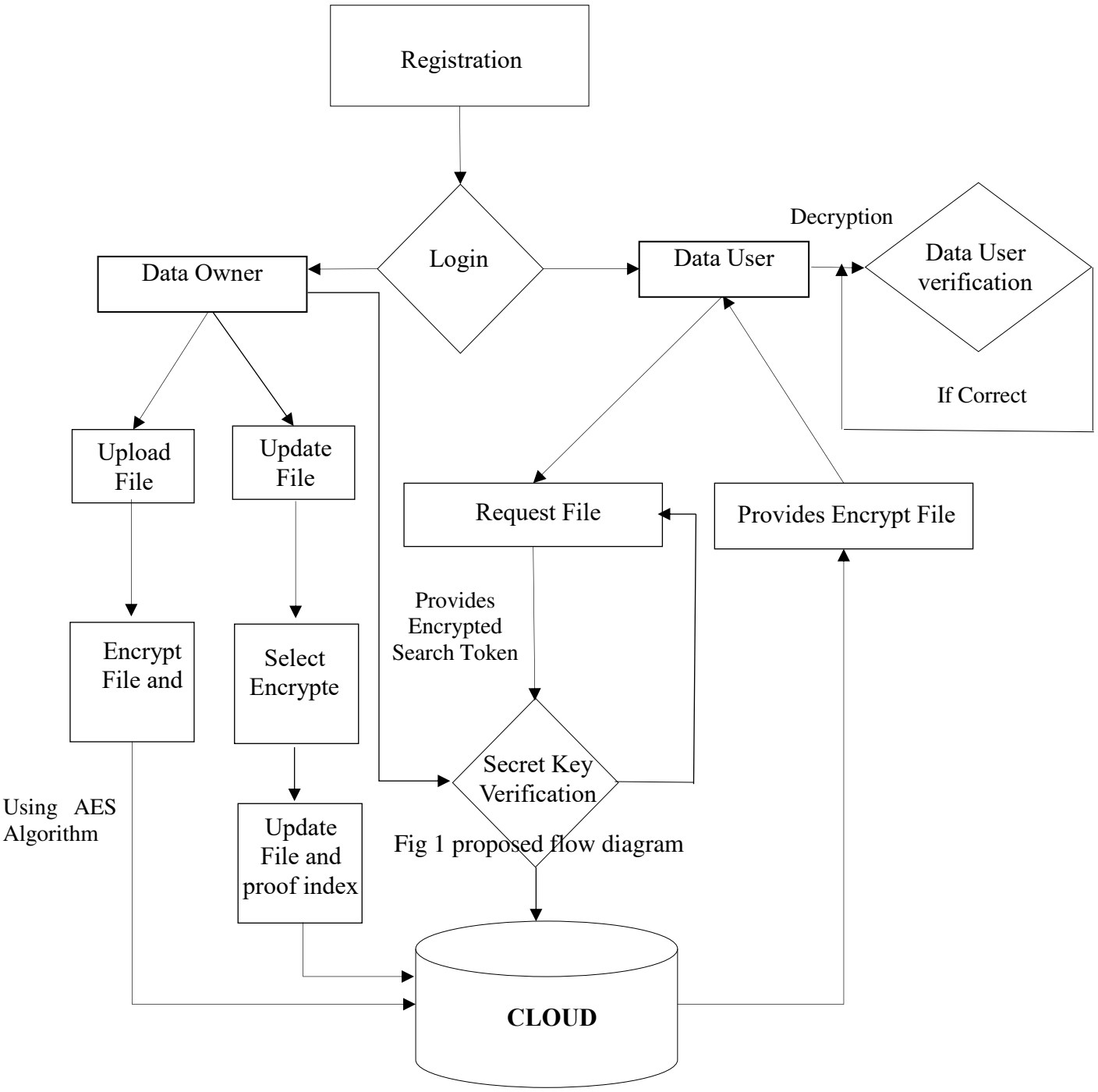

Fig 1 proposed flow diagram

Figure 1 Flow diagram

Cloud ID

The cloud ID serves as a unique identifier for each user in the cloud computing environment. It is used for authentication and authorization purposes, as well as for managing the user's access to the cloud resources and services. The cloud ID is generated during the registration process and is typically used as part of the login credentials for accessing the cloud platform

Data Owner

A data owner is a person or organization that owns or has control over the data being stored in the cloud. In the context of the system you described, the data owner is responsible for preparing the data to be stored in the cloud, including extracting keywords or creating a keyword index.

Once the data is prepared, the data owner encrypts the documents or the keyword index using a key and outsources them to the cloud for storage. The data owner also provides the public verification key and proof index to the data user via the cloud for document verification purposes. the data owner is the only authorized person to add, modify, or delete the documents from the cloud. This ensures that the data owner maintains control over their data and can prevent unauthorized access or modifications.

Public Verification Key

Public Verification Key" is actually used to verify the authenticity and integrity of the encrypted documents stored in the cloud. It is a public key that is generated by the Data Owner and shared with the Data User, who can then use it to verify that the documents retrieved from the cloud have not been tampered with or modified in any way. The Public Verification Key is a crucial component of ensuring the security and trustworthiness of the cloud-based system.

Data User

The data user sends a request to the cloud server to access the desired document. Once the cloud service provider approves the request and verifies the identity of the data user, the Public Verification Key and Proof Index are provided to the data user for document verification. The data user then uses the Public Verification Key to decrypt or download the encrypted document from the cloud. After verifying the document with the Public Verification Key, the data user can access and use the document within a specified time limit.

Verification with Proof Index

It is a proof generating organization for verifying cloud investigate by Public Verification Key, here data users or others can corroborate accuracy of search result by Verification key.

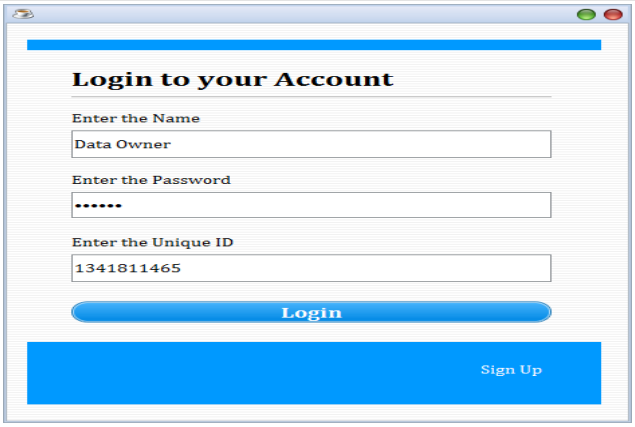

Figure 2 Registration phase

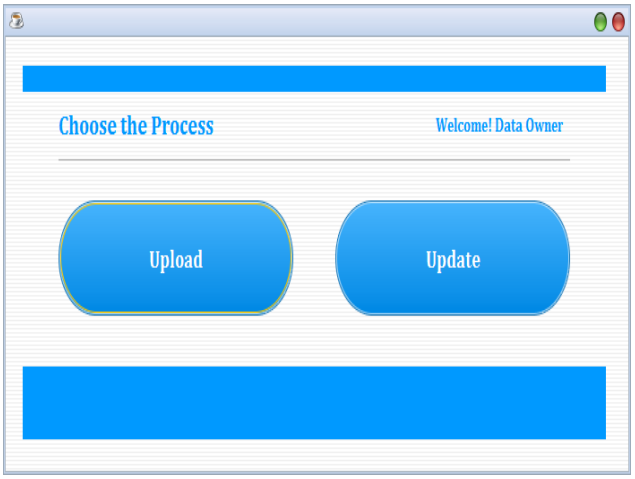

Figure 3 upload data

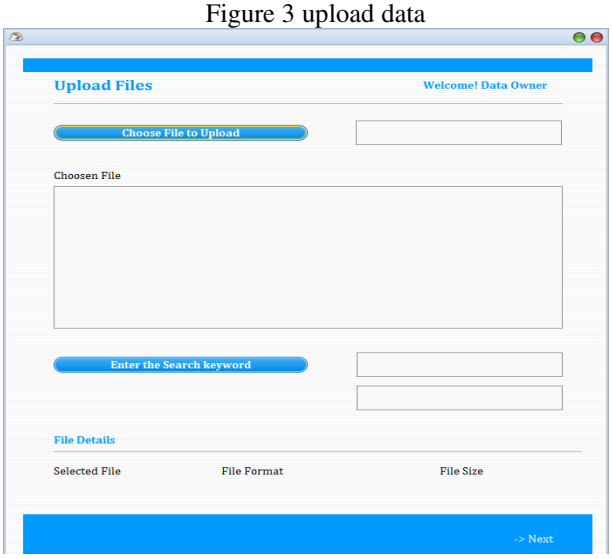

Figure 4 upload files

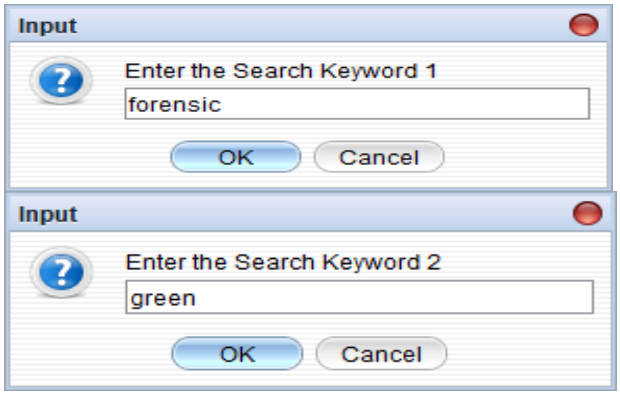

Figure 5 enter the search keyword

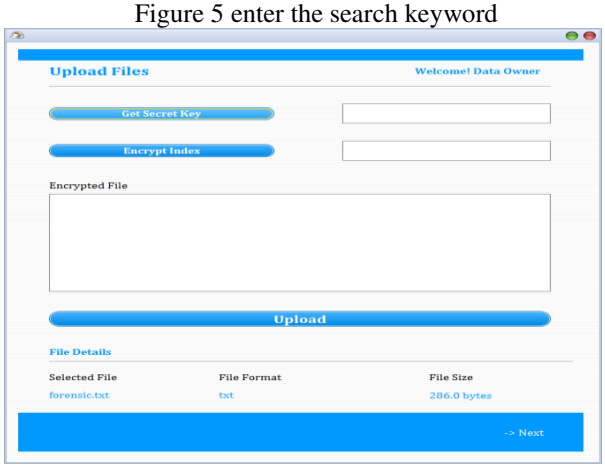

Figure 6 encrypted file

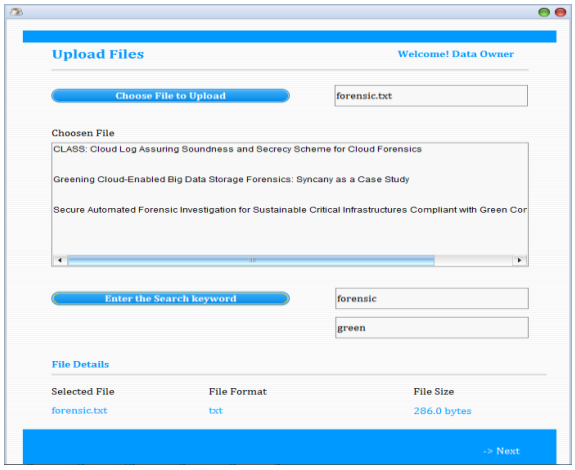

Figure 7 upload chosen file

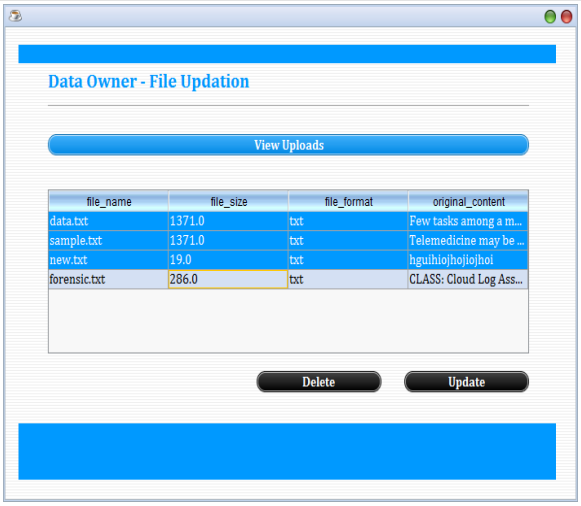

Figure 8 data owner

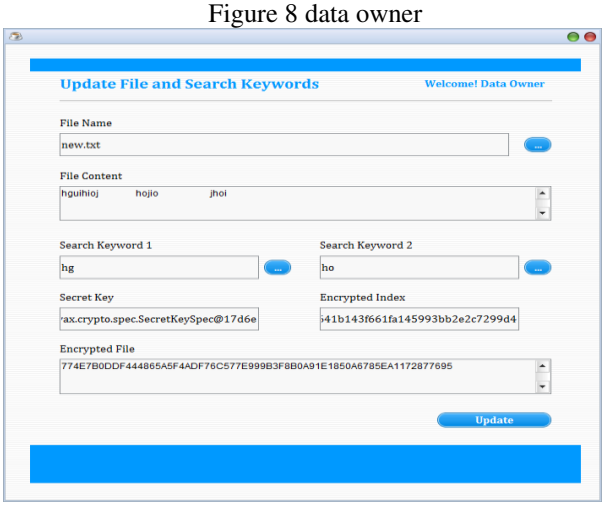

Figure 9 update file and search keywords

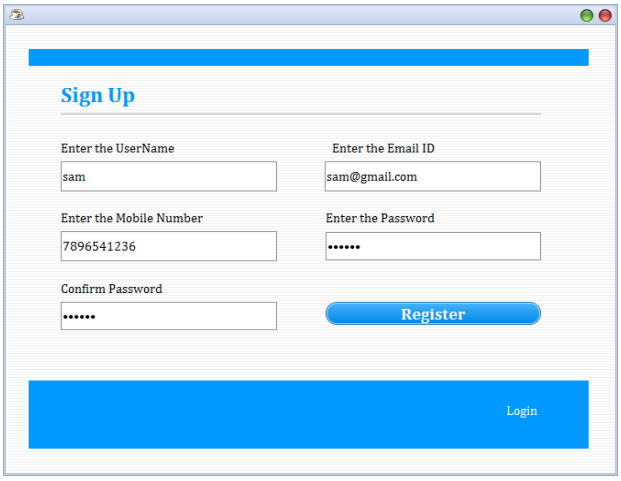

Figure 10 sign up

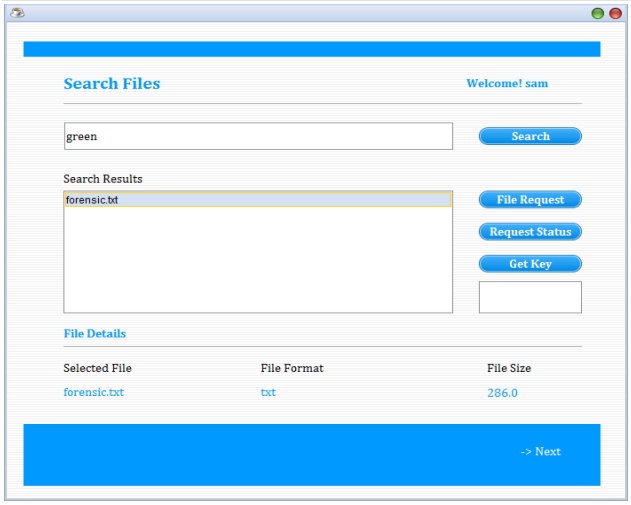

Figure 11 search files

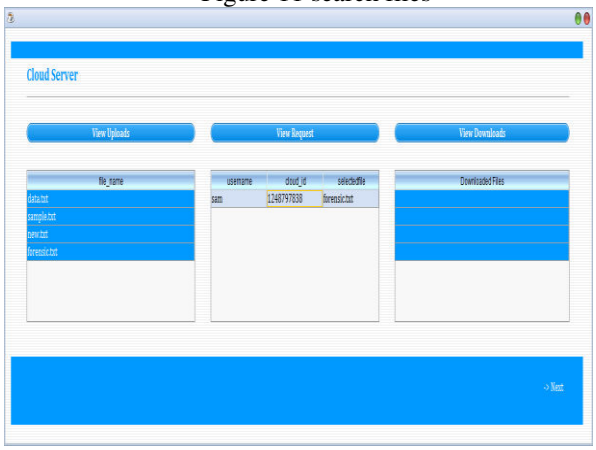

Figure 12 cloud server

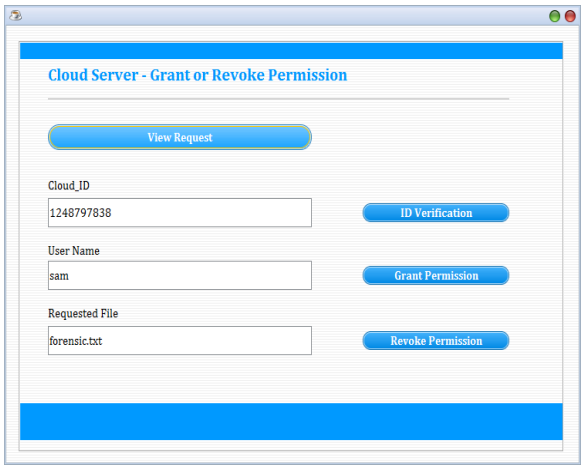

Figure 13 cloud server-grant or revoke permission

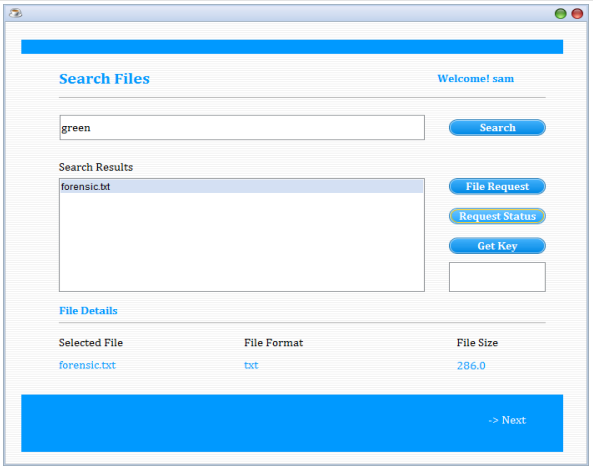

Figure 13 Data User – Request Status after CSP Authentication

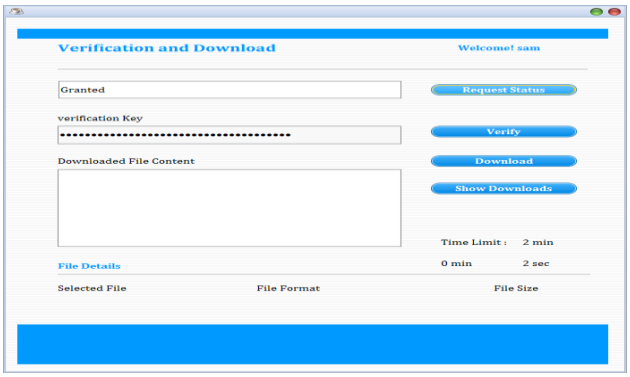

Figure 14 Data User – Received Public verification Key from CSP

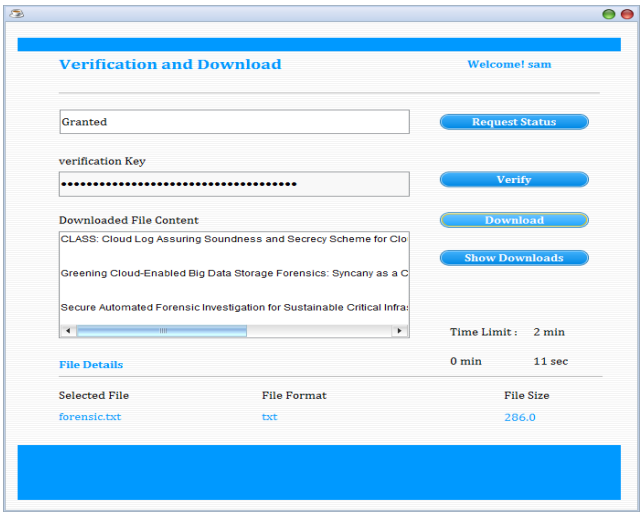

Figure 15 verification and download

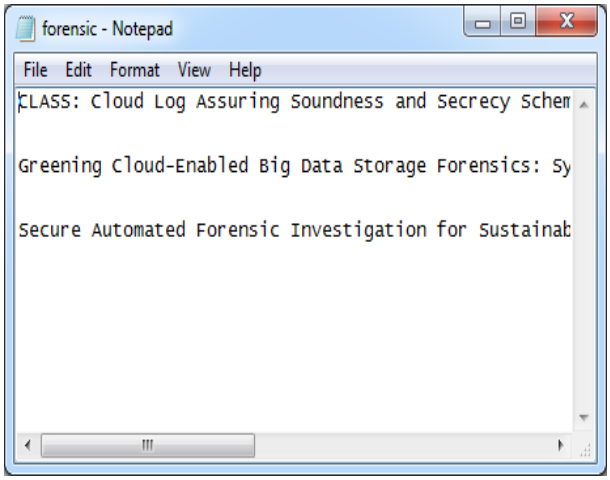

Figure 16 downloaded data

IV CONCLUSION

The purpose of this work is to ensure the secure sharing of sensitive data on public cloud platforms. To achieve this, the AES algorithm is used to encrypt the data before it is uploaded to the cloud environment. Additionally, the key escrow and revocation problem is addressed by this scheme. The Netbeans simulator is utilized to create a cloud environment for testing and implementation. Before uploading important data to the cloud, it is encrypted for protection. To further enhance security, the Private Key generated on the cloud is encrypted using the SHA algorithm before being stored alongside the encrypted data on the cloud. To decrypt the data, the user must first authenticate them on the cloud platform. Once authenticated, the key is compared to the hash code, and if they match, the data can be successfully decrypted. This ensures that sensitive data can be securely shared on public cloud platforms.

The use of cloud computing offers numerous advantages to users, but safety concerns is a major obstacle for many users to use it. Therefore, we propose a new framework that combines encryption and disguise technologies to address issues related to users and service providers. Data encryption ensures the confidentiality of the data transferred over the network, providing security for users' data. A secure storing server that can track user keys and hash values for documents uploaded by the server. An effective disguise technique is proposed for cloud providers, so that the client's secret information is not controlled by a third party. detailed analysis of the results produced by the model, and the comparison between the veiled and non-veiled models has shown that even if it is veiled, a small amount of time can be added, but for the cloud provider, given the security of user data, this time becomes negligible.

The security of cloud computing is a concern for many users, and there are various issues that need to be addressed, such as authentication, licensing, existence, trust, confidentiality and anonymity. While cloud security services can be well-designed and succeeded by experts, 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.

Cloud computing brings various tasks for structure or submission developers, engineers, system administrators and service providers. We need to discuss some of the tasks associated with security or privacy managing in cloud. In the future, we plan to extend our model towards secure searching with privacy preserving fundamental on the user information which is available on the Cloud premises, and apply mining techniques on user's secure data so that the output of queries that sent to Cloud server can be retrieved quickly.

This research work aims to assist new organizations in deploying cloud infrastructure by providing information on current market trends and cost-effective, reliable, time-saving, and secure technologies. However, future research should focus on experimenting with the migration of a small part of the network with public data on a cloud to explore further possibilities. Additionally, standardization of cloud computing can be extended to become part of every organization to receive feedback at domain, CSP level, and identify the attack path at a specific time with attack alerts. This can help to ensure the security and efficiency of cloud computing in the future.

Security for Hybrid Cloud: The model is considered promising as it can address security concerns related to public clouds and still offer economic benefits through inter-cloud communication. However, the success of the model requires further research, particularly in the area of gateway security. The gateway between private and public clouds must be secure enough to prevent the flow of data from private areas to public areas if the public cloud cannot guarantee the security of the systems and data. The implementation of automated information flow and security features can be a critical security measure for gateway control.

References

1. Jun Zhou, Zhenfu Cao, Xiaolei Dong, Xiaodong Lin, & Vasilakos, A. V. (2013). Securing m-healthcare social networks: challenges,

countermeasures and future directions. IEEE Wireless Communications, 20(4), 12–21.

2. Wen, Z., Yang, R., Garraghan, P., Lin, T., Xu, J., & Rovatsos, M. (2017). Fog Orchestration for Internet of Things Services. IEEE Internet Computing, 21(2)16–24.
3. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of BlockchainTechnology: Architecture, Consensus, and Future Trends. 2017 IEEE International Congress on Big Data (BigData Congress).
4. Razouk, W., Sgandurra, D., & Sakurai, K. (2017). A new security middlewarearchitecture based on fog computing and cloud to support IoT constrained devices. Proceedings of the 1st International Conference on Internet of Things and Machine Learning.
5. Yaakob, N., Khalil, I., Kumarage, H., Atiquzzaman, M., & Tari, Z. (2014). By-Passing Infected Areas in Wireless Sensor Networks using BPR. IEEE Transactions on Computers, 1–1.
6. Daoud, W. B., Obaidat, M. S., Meddeb-Makhlouf, A., Zarai, F., & Hsiao, K.-F. (2019).TACRM: trust access control and resource management mechanism in fog computing. Human-Centric Computing and Information Sciences, 9(1).
7. Borah, R. (n.d.). Cloud Computing Architecture: What is Front End and Back End? Www.clariontech.com. Retrieved February 27, 2021, fromhttps:// www. clariontech. com/blog/cloud-computing-architecture-what-is-front-end-and-back-end
8. Ahmad, R. W., Gani, A., Hamid, S. H. Ab., Shiraz, M., Yousafzai, A., & Xia, F. (2015). A survey on virtual machine migration and server consolidation frameworks for cloud data centers. Journal of Network and Computer Applications, 52, 11–25.
9. Monika Sharma. (2020). Data Encryption Standard (DES) in Cryptography. (n.d.). Www.includehelp.com. Retrieved February 27, 2021, from
10. Wang, T., Zhou, J., Chen, X., Wang, G., Liu, A., & Liu, Y. (2018). A Three-Layer Privacy Preserving Cloud Storage Scheme Based on Computational Intelligence in Fog Computing. IEEE Transactions on Emerging Topics in Computational Intelligence, 2(1), 3–12.
11. Ali, hakir, Vishal, Laghari, Asif, Karim, Shahid, & Brohi. (2019). Comparison of Fog Computing & Cloud Computing [Review of Comparison of Fog Computing & Cloud Computing]. International Journal of Mathematical Sciences and Computing, 31–41
12. Stray, V., Moe, N. B., & Noroozi, M. (2019). Slack Me If You Can! Using Enterprise Social Networking Tools in Virtual Agile Teams. 2019 ACM/IEEE 14th International Conference on Global Software Engineering (ICGSE).
13. Thangavel M, Varalakshmi P Enabling Ternary Hash Tree based Integrity Verification for Secure Cloud Data Storage Student Member, IEEE, 1041-4347 (c) 2019 IEEE. DOI 10.1109/TKDE.2019.2922357
14. ShiMa, R., Alahmadi, A. A., El-Gorashi, T. E. H., & Elmirghani, J. M. H. (2019). Energy Efficient Software Matching in Vehicular Fog. 2019 21st International Conference on Transparent Optical Networks (ICTON).
15. Tariq, N., Asim, M., Al-Obeidat, F., Zubair Farooqi, M., Baker, T., Hammoudeh, M., & Ghafir, I. (2019). The Security of Big Data in Fog-Enabled IoT Applications Including Blockchain: A Survey. Sensors, 19(8), 1788.
16. Samantha Brown. (2016). Transmit the Data With Encryption – The Secure Way ForData Sharing - SysTools Blog. (n.d.). Blog.systoolsgroup.com. RetrievedFebruary 27, 2021,