International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/IJSRCSEIT

A Cloud Based Dispersion and Encryption Based for Storage Mechanism

P. Munijyothika[1], Mr. A. Murali Mohan Kumar[2]
MCA Student[1], Associate Professor[2]
Department of MCA[1&2]
Mother Theresa Institute of computer Applications , Palamaner- S. V University, Tirupati, India

Article Info

Publication Issue :
Volume 8, Issue 5
September-October-2022

Page Number : 251-260

Article History
Accepted: 10 Oct 2022
Published: 22 Oct 2022

ABSTRACT

Cloud storage service has shown its great power and wide popularity which provides fundamental support for rapid development of cloud computing. However, due to management negligence and malicious attack, there still lie enormous security incidents that lead to quantities of sensitive data leakage at cloud storage layer. From the perspective of protecting cloud data confidentiality, this paper proposed a Cloud Secure Storage Mechanism named CSSM. To avoid data breach at the storage layer, CSSM integrated data dispersion and distributed storage to realize encrypted, chucked and distributed storage. In addition, CSSM adopted a hierarchical management approach and combined user password with secret sharing to prevent cryptographic materials leakage. The experimental results indicate that proposed mechanism is not only suitable for ensuring the data security at storage layer from leakage, but also can store huge amount of cloud data effectively without imposing too much time overhead. For example, when users upload/download 5G sized file with CSSM, it only takes 646seconds/269seconds, which is acceptable for users

Keywords : Cloud computing, data dispersion, data encryption, key management, storage security.

I. INTRODUCTION

Cloud computing has shown remarkable development in recent decades. When the storage as a service, it occupies the center stage and backbone for many applications, such as pattern recognition image forensic and forgery detection. As a result, larger volumes of data will be a part of the cloud area. In the cloud industry, Amazon Web Service (AWS) has become the de facto standard. As the core component of the Opens tack that follows this standard, Swift has become one of the most popular cloud storage mechanism. However, Opens tack Swift mechanism still faces many real security threats while providing convenient services. According to Cloud Security Alliance's top threat case analysis report released in 2018, two thirds of the cases will cause user data leakage, mainly due to management negligence and malicious attacks. For instance, under default configuration, OpenStack Swift mechanism typically stores data in plaintext for the sake of performance.

That will lead unauthorized access to user data at storage layer. In addition, Security Report released by Openstack Vulnerability Management Team VMT, the Swift mechanism may leak user data or configuration information in virtue of security vulnerabilities.

Shah et al proposed a cloud-oriented data security storage mechanism under the framework of Apache Spark, which prevents data leakage and improves the security of Apache Spark framework. To protect user data on the cloud, different encryption schemes have been adopted to avoid information leakage during machine learning process. Nevertheless, above researches require secure key management mechanisms to prevent cryptographic materials exposure. Zerfos et al.constructed a secure distributed storage system based on Hadoop system, which keep the confidentiality of cloud data through data dispersion and encryption. It performs the data decryption and assembly tasks before reading data. To prevent the keys from being stolen, this method requires key cache server and all keys should be stored in memory only. Some approaches introduced independent third party to manage the key. It is assumed that third parties stay trusted. However, the assumption cloud not always exists in the real cloud storage environments. Wang et al. presented a data privacy preserving scheme for sensor-cloud system, based on edge computing and differential storage method. In this scheme, user data would be divided into different parts and stored in local, edge and cloud layer respectively. But the scheme relies on the characteristics of data from wireless sensor networks, and requires skilled users to manage the edge servers. To improve the efficiency and decrease the redundancy, Zheng et al. provided a cloud data duplication scheme to detect and remove identical user data in the cloud. However, from the perspective of preventing data loss due to disaster, a certain number of copies should be sent to multiple regions. In a word, to protect cloud data from leakage at storage layer, this paper presents CSSM, a Cloud Secure Storage Mechanism. CSSM combines data dispersion with data encryption, so that large-scale cloud data and keys would be stored in chunked cipher texts. On this basis, user password and secret sharing are introduced to further protect keys security. We implemented CSSM based on OpenStack Swift mechanism and made several tests. The major contributions of this work are listed below:

1) Data Secure Storage: In order to prevent data leakage and increase the difficulty of attack, this paper presents a method combining data distribution and data encryption to improve data storage security.

2) Hierarchical Key Management: To protect the key and prevent the attacker from using the key to recover the data, this paper introduces secret sharing and key hierarchy derivation algorithm in combination with user password to enhance key security.

3) Experimental Evaluation and Analysis: The security analysis and experimental results show that CSSM can effectively guarantee the security of data storage, and the increased performance cost is acceptable.

II. RELATED WORKS:

A. Bhardwaj, F. Al-Turjman, M. Kumar, T. Stephan, and L. Mostarda, "Capturing-the-invisible (CTI): Behavior-based attacks recognition in IoT-oriented industrial control systems," IEEE Access, vol. 8, pp. 104956–104966, 2020: Industrial Control Systems monitor, automate, and operate complex infrastructure and processes that integrate into critical industrial sectors that affect our daily lives. With the advent of networking and automation, these systems have moved from being dedicated and independent to centralized corporate infrastructure. While this has facilitated the monitoring and overall management using traditional detection methods, Web Application Firewalls or Intrusion Detection Systems has exposed the networks subjecting them to Behaviour-based cyber security attacks. Such attacks alter the control

flow and processes and have the malicious ability to alter the functioning of these systems altogether. This research focuses on the use of process analytics to detect attacks in the industrial control infrastructure systems and compares the effectiveness of signature-based detection methods. The proposed work presents a pattern recognition algorithm aptly named as "Capturing-the-Invisible (CTI)" to find the hidden process in industrial control device logs and detect Behaviour-based attacks being performed in real-time.

M. Kumar, A. Rani, and S. Srivastava, "Image forensics based on lighting estimation," Int. J. Image Graph., vol. 19, no. 3, Jul. 2019, Art. no. 1950014: Computer generated images are assumed to be a key part in each person's life in this era of information technology, where individuals effectively inhabit the advertisements, magazines, websites, televisions and many more. At the point when digital images played their role, the event of violations in terms of misrepresentation of information, use of their wrong doings winds up and also becomes easier with the help of image editing application programs. To be legitimate, if anyone does wrong anything then the proposed method can be used for a correct identification of the forgery and the imitations in the digital images. In existing techniques, researchers have suggested most well-known types of digital photographic manipulations based on source, meta-data, image copying, splicing and many more. The proposed approach is inspired by physics-based techniques and requires less human involvement. The presented approach works for images having any type of objects present in the scene, i.e. not only limited to human faces and selection of same intensity regions of the image. By assessing the lighting parameters, the proposed technique identifies the manipulated object and returns angle of incidence w.r.t light source direction. The demonstrated result produces forgery recognition rate of 92% on an image dataset comprising of various types of manipulated images.

J. Li, Y. Zhang, X. Chen, and Y. Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing," Comput. Secur., vol. 72, pp. 1–12, Jan. 2018: Data sharing becomes an exceptionally attractive service supplied by cloud computing platforms because of its convenience and economy. As a potential technique for realizing finegrained data sharing, attribute-based encryption (ABE) has drawn wide attentions. However,most of the existing ABE solutions suffer from the disadvantages of high computation overhead and weak data security, which has severely impeded resource-constrained mobile devices to customize the service. The problem of simultaneously achieving fine-grainedness, high efficiency on the data owner's side, and standard data confidentiality of cloud data sharing actually still remains unresolved. This paper addresses this challenging issue by proposing a new attribute-based data sharing scheme suitable for resource-limited mobile users in cloud computing. The proposed scheme eliminates a majority of the computation task by adding system public parameters besides moving partial encryption computation offline. In addition, a public ciphertext test phase is performed before the decryption phase, which eliminates most of computation overhead due to illegitimate cipher texts. For the sake of data security, a Chameleon hash function is used to generate an immediate cipher text, which will be blinded by the offline ciphertexts to obtain the final online ciphertexts. The proposed scheme is proven secure against adaptively chosen-ciphertext attacks, which is widely recognized as a standard security notion. Extensive performance analysis indicates that the proposed scheme is secure and efficient.

Y. Zhang, X. Chen, J. Li, D. S. Wong, H. Li, and I. You, "Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing," Inf. Sci., vol. 379, pp. 42–61, Feb. 2017: Although many users outsource their various data to clouds, data security and privacy concerns are still the biggest obstacles that hamper the widespread

adoption of cloud computing. Anonymous attribute-based encryption (anonymous ABE) enables fine-grained access control over cloud storage and preserves receivers' attribute privacy by hiding attribute information in ciphertexts. However, in existing anonymous ABE work, a user knows whether attributes and a hidden policy match or not only after repeating decryption attempts. And, each decryption usually requires many pairings and the computation overhead grows with the complexity of the access formula. Hence, existing schemes suffer a severe efficiency drawback and are not suitable for mobile cloud computing where users may be resource-constrained. In this paper, we propose a novel technique called match-then-decrypt, in which a matching phase is additionally introduced before the decryption phase. This technique works by computing special components in ciphertexts, which are used to perform the test that if the attribute private key matches the hidden access policy in ciphertexts without decryption. For the sake of fast decryption, special attribute secret key components are generated which allow aggregation of pairings during decryption. We propose a basic anonymous ABE construction, and then obtain a security-enhanced extension based on strongly existentially unforgeable one-time signatures. In the proposed constructions, the computation cost of an attribute matching test is less than one decryption operation, which only needs small and constant number of pairings. Formal security analysis and performance comparisons indicate that the proposed solutions simultaneously ensure attribute privacy and improve decryption efficiency for outsourced data storage in mobile cloud computing.

Z. Liu, Y. Huang, J. Li, X. Cheng, and C. Shen, "DivORAM: Towards a practical oblivious RAM with variable block size," Inf. Sci., vol. 447, pp. 1–11, Jun. 2018: Oblivious RAM (ORAM) is important for applications that require hiding access patterns. Many ORAM schemes have been proposed but most of them support only storing blocks of the same size. For the variable length data blocks, they usually fill them up to the same length before uploading, which leads to an increase in storage space and network bandwidth usage. To develop the first practical ORAM with variable block size, we proposed the "DivORAM" by remodeling the tree-based ORAM structure. It employs an additively homomorphic encryption scheme (Damgård–Jurik cryptosystem) executing at the server side to save the client computing overhead and the network bandwidth cost. As a result, it saves network bandwidth 30% comparing with Ring ORAM and 40% comparing with HIRB ORAM. Experiment results show that the response time of DivORAM is 10 × improved over Ring ORAM for practical parameters.

III. Methodology

Proposed system:

This paper proposed a Cloud Secure Storage Mechanism named CSSM. To avoid data breach at the storage layer, CSSM integrated data dispersion and distributed storage to realize encrypted, chucked and distributed storage. In addition, CSSM adopted a hierarchical management approach and combined user password with secret sharing to prevent cryptographic materials leakage.

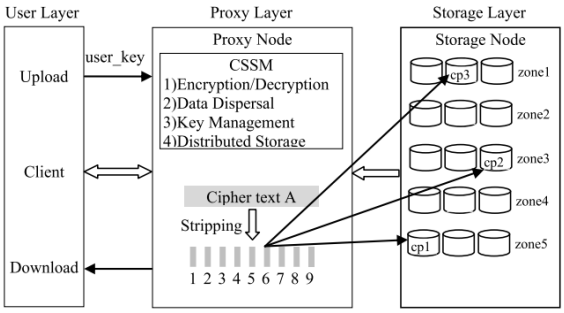


Figure 1: Fake reviews dataset block diagram

IV. Implementation

CLOUD:

Cloud includes three basic services:

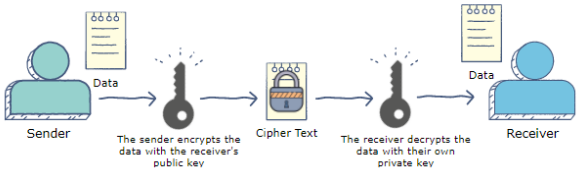
- Infrastructure as a Service (Iaas),

- Platform as a Service (PaaS), and
- Software as a Service (Saas).

Software-as-a-service (SaaS) involves the licensure of a software application to customers. Licenses are typically provided through a pay-as-you-go model or on-demand. This type of system can be found in Microsoft Office's 365

Infrastructure-as-a-service (IaaS) involves a method for delivering everything from operating systems to servers and storage through IP-based connectivity as part of an on-demand service. Clients can avoid the need to purchase software or servers, and instead procure these resources in an outsourced, on-demand service. Popular examples of the IaaS system include IBM Cloud and Microsoft Azure

Platform-as-a-service (PaaS) is considered the most complex of the three layers of cloud-based computing. PaaS shares some similarities with SaaS, the primary difference being that instead of delivering software online, it is actually a platform for creating software that is delivered via the Internet. This model includes platforms like Salesforce.com and Heroku.



DATA ENCRYPTION:

Data encryption translates data into another form, or code, so that only people with access to a secret key (formally called a decryption key) or password can read it. Encrypted data is commonly referred to as ciphertext, while unencrypted data is called plaintext. Currently, encryption is one of the most popular and effective data security methods used by organizations. Two main types of data encryption exist - asymmetric encryption, also known as public-key encryption, and symmetric encryption.

PURPOSE:

The purpose of data encryption is to protect digital data confidentiality as it is stored on computer systems and transmitted using the internet or other computer networks. The outdated data encryption standard (DES) has been replaced by modern encryption algorithms that play a critical role in the security of IT systems and communications.

These algorithms provide confidentiality and drive key security initiatives including authentication, integrity, and non-repudiation. Authentication allows for the verification of a message's origin, and integrity provides proof that a message's contents have not changed since it was sent. Additionally, non-repudiation ensures that a message sender cannot deny sending the message.

DATA DECRYPTION:

Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form. In decryption, the system extracts and converts the garbled data and transforms it to texts and images that are easily understandable not only by the reader but also by the system. Decryption may be accomplished manually or automatically. It may also be performed with a set of keys or passwords. One of the foremost reasons for implementing an encryption-decryption system is privacy. As information travels over the World Wide Web, it becomes subject to scrutiny and access from unauthorized individuals or organizations. As a result, data is encrypted to reduce data loss and theft. Some of the common items that are encrypted include email messages, text files, images, user data and directories. The person in charge of decryption receives a prompt or window in which a password may be entered to access encrypted information.

CSSM (Cloud Secure Storage Mechanism)

The proposed mechanism is to secure cloud storage against data breach, which may be the result of targeted attack (e.g. disk cloning) or management negligence (e.g. misconfiguration), in case hackers even some malicious administrator is able to steal user

data. Aiming at this goal, data dispersion or encryption is the most commonly adopted way in numerous cases. Both techniques could provide privacy-preserving, but they also come with inherent risks. Data dispersion spreads data pieces across different storage areas, but there still lies an opportunity to recover data when attackers obtain enough pieces. Data encryption technology stores data in cipher texts by encrypting data with cryptographic keys. However, attackers can still recover the original data by stealing the keys. That raises the problem of key protection and management. Therefore, to maximize the confidentiality of cloud data storage, the proposed mechanism should make full use of the advantages of the method and effectively control its disadvantages. Meanwhile, the increased cost of the mechanism should be within a reasonable range. Specifically, following properties should be met:

Property 1: From the perspective of protecting cloud data confidentiality, any user data stored in the cloud would not be released, viewed, stolen or used by unauthorized individual, such as hackers or some malicious administrator.

Property 2: On the basis of property 1, any parameters like cryptographic keys, which related to keep cloud data confidential, should also be protected.

Property 3: The additional performance overhead of deploying proposed mechanism should be within the user's acceptance.

ARCHITECTURE OVERVIEW:

To realize primary object and properties above, this paper presents CSSM, a cloud secure storage mechanism. As shown in Figure 1, CSSM could be divided into three layers: The user layer, the proxy layer, and the storage layer. Specifically, the main functions of each layer are as follows:

1) User Layer: This layer is deployed on the user's machine, and the user operates (upload, download, etc.) cloud data through the client.

2) Proxy Layer: This layer is deployed in the cloud and composed of proxy nodes with trusted execution environments, such as Intel SGX technology and ARM Trust Zone technology. In trusted execution environment, CSSM programs could perform as expected. CSSM in proxy layer includes four modules: data encryption/decryption, data dispersal, key management and distributed storage.

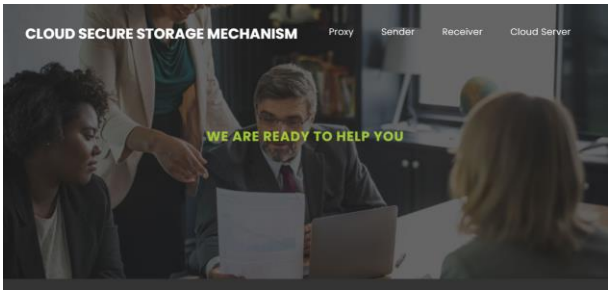
1. **Encryption/Decryption:** This module is used to encrypt user uploaded data and decrypt user downloaded data.
2. **Data Dispersal:** According to the data dispersal model, the cipher texts is divided into several small blocks.
3. **Key Management:** This module is not only responsible for the generation and maintenance of the key, but also uses the hierarchical key management approach to protect the key.
4. **Distributed storage:** This module distributes chunked and encrypted data to storage layer.

3) Storage Layer: This layer consists of a number of storage nodes that are used to store chunked and encrypted data. Considering data loss or unavailability caused by accident like equipment damage or natural disasters, cloud service providers divide large number of storage nodes into several zones, each of which acts as a failure boundary between multiple copies of the same data.

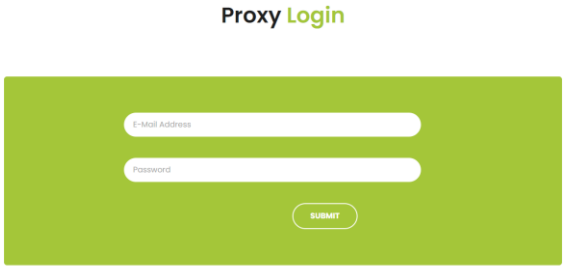
V. RESULTS AND DISCUSSION:

The following images will visually depict the process of our project.

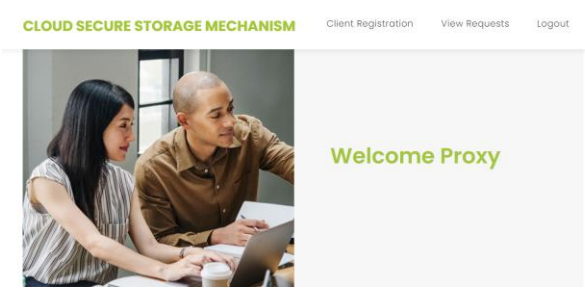
Home page: In this home page we can see the logo designing of our website and here we are detecting the fake reviews from the review entered by the user.



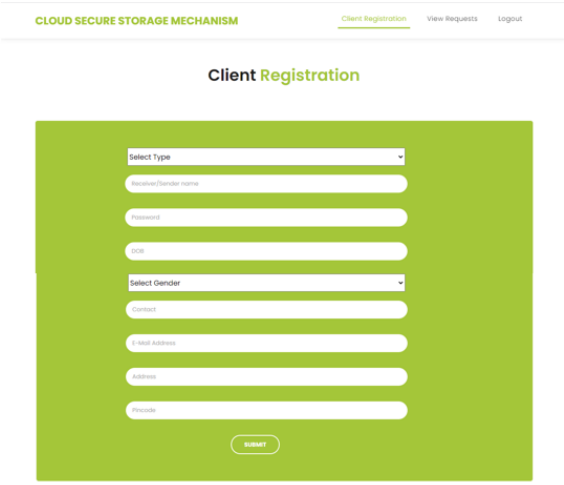
Proxy Login Page: This is login page of proxy.



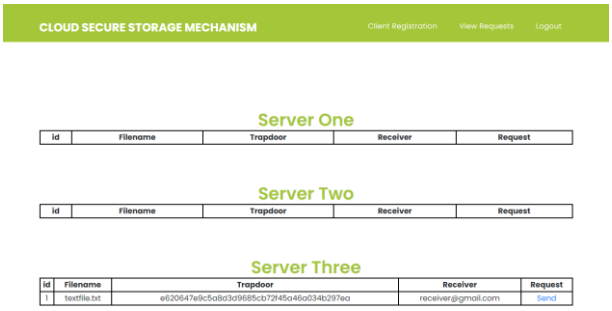
Proxy home Page: Once after login proxy will get home page as shown in below picture.



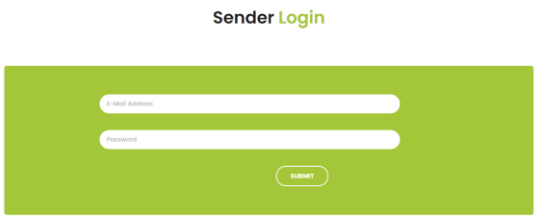
Client registration Page: This is the page where the client can register into account.



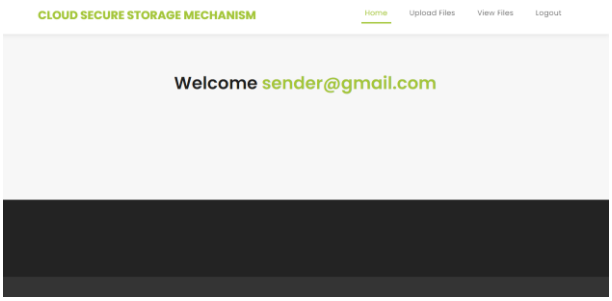
Requests: In this page the user can make requests.



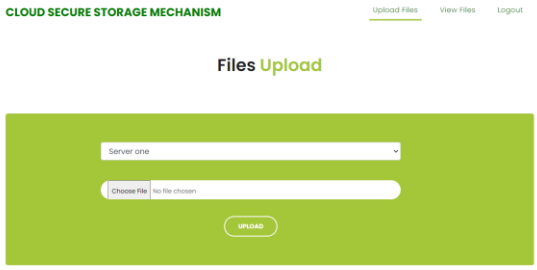
Sender Login: Here, the sender can login into account.



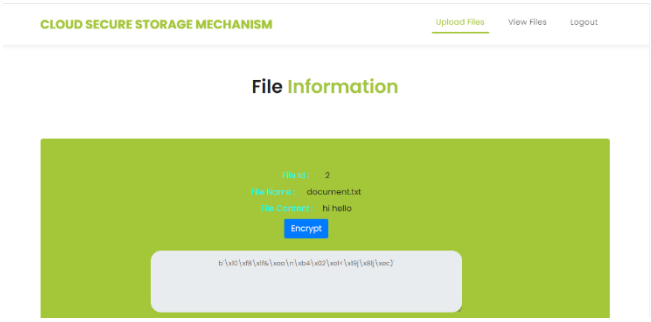
Sender home: This is the home page of sender.



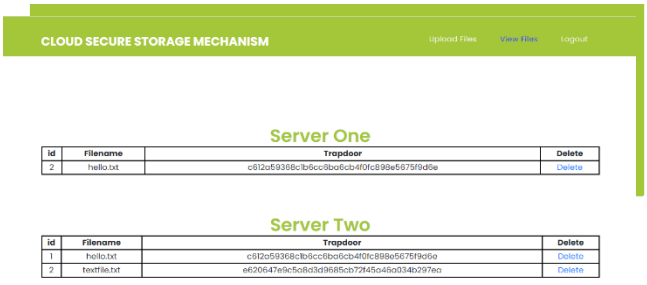
Upload Page: Here the send can upload the files.



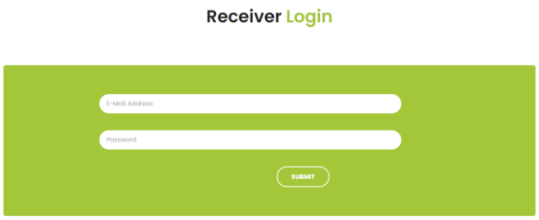
Encrypt Page: This is the data encryption page.



View files: After encryption here the files can view.

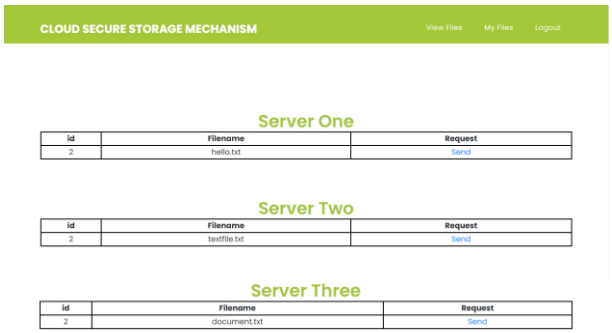


Receiver Login Page: This is the login page of receiver.

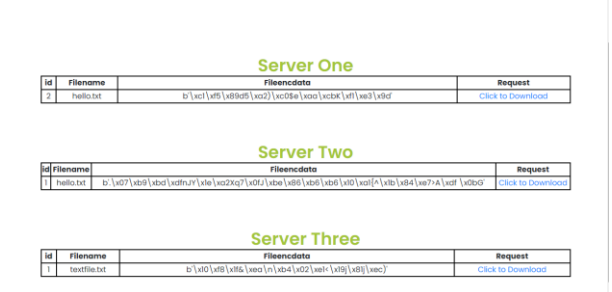


Receiver home page: This is the home of receiver.

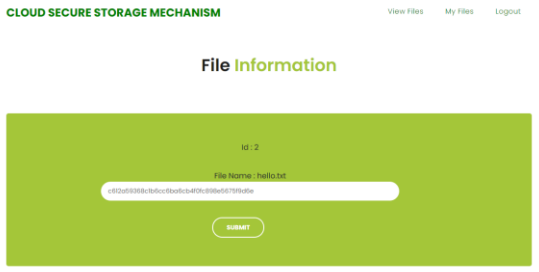
All files: This page contains all files.



My Files: Here, we can see all files of server.

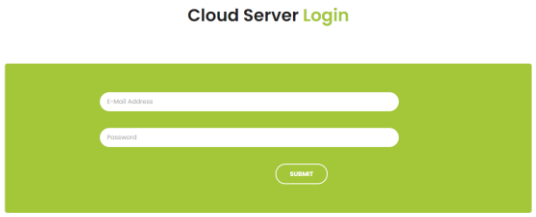


Trap Door: This is the trap door page.

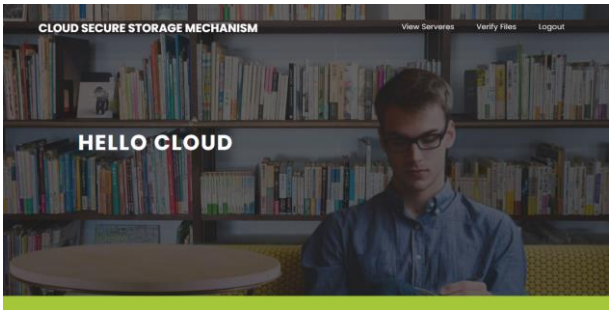


Download page: This is the page where the files gets download.

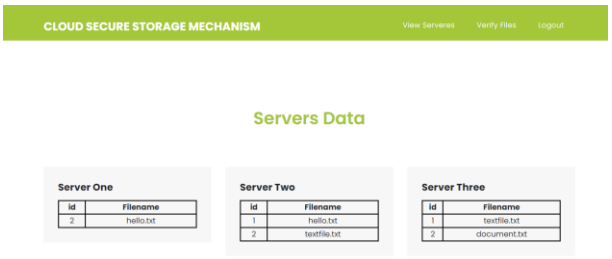
Cloud Server Login Page: This is cloud server login page.



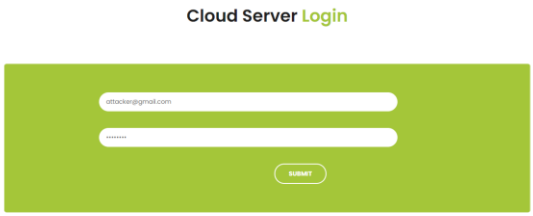
CSP home page: This is the home page of Cloud Server.



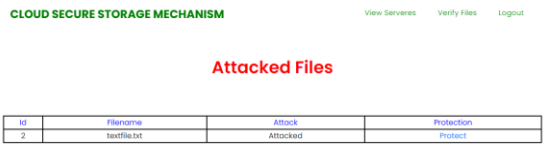
View server's data: In this page the server can view the data.



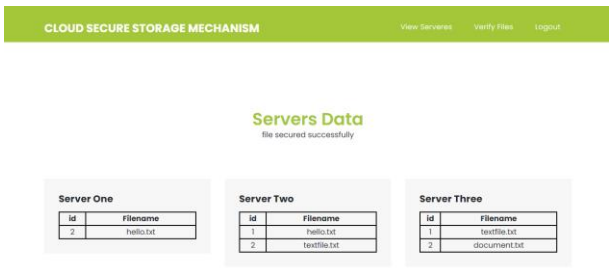
Attacker Login Page: here, the attacker can login into accout.



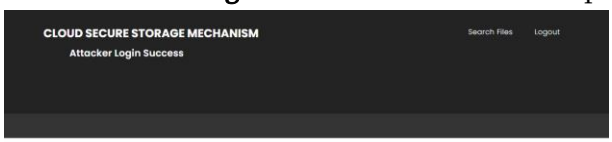
Attacked File: Here we can see the attacked file.



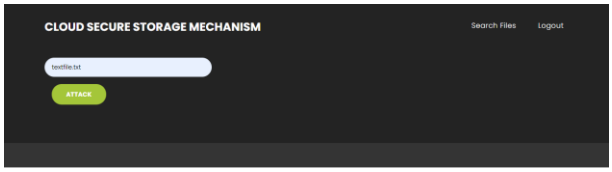
File secured: In this page we can see the secured files.



Attacker home Page: This is the attacker home page.

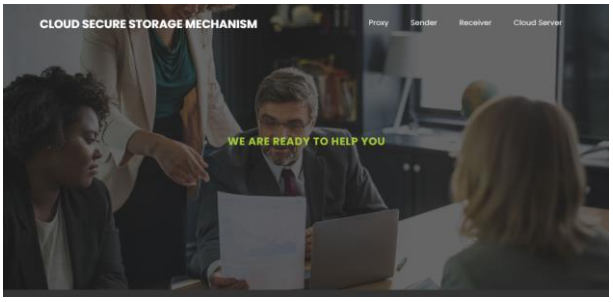


Search File: Here, the attacker can search the files.



File Attacked: Here, we can see the attacked files after attack.

Logout: This is logout page.



VI. Conclusion

For the issue of cloud data leakage caused by management negligence and malicious attack at storage layer, we proposed CSSM, a cloud secure storage mechanism. CSSM adopted a combined approach of data dispersal and encryption technologies, which can improve the data security and prevent attackers from stealing user data. The experimental results show that CSSM can effectively prevent user data leakage at cloud storage layer. In terms of performance, the increased time overhead of CSSM is acceptable to users. This paper provides a feasible approach to solve the storage security problem, especially prevention from user data leakage at cloud storage layer. CSSM could also effectively protect cryptographic materials from storage perspective.

VII. REFERENCES

[1]. Bhardwaj, F. Al-Turjman, M. Kumar, T. Stephan, and L. Mostarda, "Capturing-the-invisible (CTI): Behavior-based attacks recognition in IoT-oriented industrial control systems," IEEE Access, vol. 8, pp. 104956–104966, 2020.

[2]. M. Kumar, A. Rani, and S. Srivastava, "Image forensics based on lighting estimation," Int. J. Image Graph., vol. 19, no. 3, Jul. 2019, Art. no. 1950014.

[3]. M. Kumar, S. Srivastava, and N. Uddin, "Image forensic based on lighting estimation," Austral. J. Forensic Sci., vol. 51, no. 3, pp. 243–250, Aug. 2017.

[4]. J. Li, Y. Zhang, X. Chen, and Y. Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing," Comput. Secur., vol. 72, pp. 1–12, Jan. 2018.

[5]. Y. Zhang, X. Chen, J. Li, D. S. Wong, H. Li, and I. You, "Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing," Inf. Sci., vol. 379, pp. 42–61, Feb. 2017.

[6]. The OpenStack Project. OSSA-2015-006: Unauthorized Delete of Versioned Swift Object. Accessed: Apr. 14, 2015. [Online]. Available: https://security.openstack.org/ossa/OSSA-2015-006.html

[7]. The OpenStack Project. OSSA-2015-016: Information Leak Via Swift Tempurls. Accessed: Aug. 26, 2015. [Online]. Available: https://security. openstack.org/ossa/OSSA-2015-016.html

[8]. The OpenStack Project. Possible Glance Image Exposure Via Swift. Accessed: Feb. 23, 2015. [Online]. Available: https://wiki. openstack.org/wiki/OSSN/OSSN-0025

[9]. Cloud Security Alliance. Top Threats to Cloud Computing: Deep Dive. Accessed: Aug. 8, 2018. [Online]. Available: https://downloads. cloudsecurityalliance.org/assets/research/top-threats/top-threats-to-cloudcomputing-deep-dive.pdf

[10]. The OpenStack Project. OpenStack Security Advisories. Accessed: Feb. 2, 2015. [Online]. Available: https://security.openstack.org/ossalist. html

[11]. Common Vulnerabilities and Exposures. CVE-2015-5223. Accessed: Jul. 1, 2015. [Online]. Available: https://cve.mitre.org/cgi-bin/cvename. cgi?name=CVE-2015-5223

[12]. Common Vulnerabilities and Exposures. CVE-2016-9590. Accessed: Nov. 23, 2016. [Online]. Available: https://cve.mitre.org/cgi-bin/cvename. cgi?name=CVE-2016-9590

[13]. S. Y. Shah, B. Paulovicks, and P. Zerfos, "Data-at-rest security for spark," in Proc. IEEE Int. Conf. Big Data (Big Data), Washington DC, USA, Dec. 2016, pp. 1464–1473.

[14]. Z. Liu, Y. Huang, J. Li, X. Cheng, and C. Shen, "DivORAM: Towards a practical oblivious RAM with variable block size," Inf. Sci., vol. 447, pp. 1–11, Jun. 2018.

[15]. X. Zhang, X. Chen, J. Wang, Z. Zhan, and J. Li, "Verifiable privacypreserving single-layer perceptron training scheme in cloud computing," Soft Comput., vol. 22, no. 23, pp. 7719–7732, Dec. 2018.

Cite this article as :

P. Munijyothika, Mr. A. Murali Mohan Kumar, "A Cloud Based Dispersion and Encryption Based for Storage Mechanism", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 8 Issue 5, pp. 251-260, September-October 2022.

Journal URL : https://ijsrcseit.com/CSEIT228548