JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Securing Data in Cloud Using Data Dispersion and Encryption

Mr. P.V.S. Satyanarayana Varma (M.C.A). Rajeev Gandhi Memorial college Of Engineering and Technology, Nandyal

***Mrs. Dr. Chaitanya Nukala (MTech, (Ph.D.). Rajeev Gandhi Memorial college Of Engineering and Technology, Nandyal**

***Corresponding Author**

Abstract

In other words, this study introduces CSSM, a Cloud Secure Storage Mechanism, to safeguard cloud data from leaking at the storage layer. In order to store large-scale cloud data and keys in chunked cipher texts, CSSM combines data dispersion with data encryption. In order to further safeguard the security of keys, user passwords and secret sharing are implemented. We tested CSSM after implementing it using the OpenStack Swift protocol. The following is a list of this work's main contributions: 1) Safeguarded data storage This study provides a system that combines data distribution with data encryption to strengthen data storage security, reduce data leaking, and make attacks more difficult. 2) Key management that is hierarchical In order to strengthen key security, this work introduces secret sharing and key hierarchy deriva-tion algorithms in conjunction with user passwords. These techniques protect the key and stop the attacker from using it to recover the data. 3) Evaluation and analysis of experimental data: The results of the experiments and security analysis demonstrate that CSSM can effectively guarantee the security of data storage, and users are willing to pay the higher performance cost..

1. INTRODUCTION

1.1 Introduction

In recent years, cloud computing has grown remarkably. When using storage as a service, numerous applications, like pattern recognition [1], image forensic [2], and forgery detection [3], take center stage and rely on it as their backbone. Larger amounts of data will therefore be included in the cloud area. Amazon Web Service (AWS) has taken over as the industry standard in the cloud. Swift has emerged as one of the most well-liked cloud storage mechanisms as the central element of the OpenStack that adheres to this standard [4], [5]. Although it offers practical services, Openstack Swift's mechanism nevertheless faces a number of serious security risks [6] [8]. The top threat case analysis report [9] from the Cloud Security Alliance, published in 2018, claims that two thirds of the User data leakage will occasionally occur, usually as a result of management incompetence and malevolent attempts. For instance, OpenStack Swift's default configuration often keeps data in unencrypted for performance reasons. This will result in storage layer user data being accessed without authorization. Additionally, according to Security Report [10] from Openstack Vulnerability Management Team VMT, due to security flaws [11], [12], the Swift mechanism may leak user data or configuration information. In the Apache Spark framework, Shah et al. [13] introduced a cloud-oriented data security storage mechanism that stops data leakage and enhances the security of Apache Spark. Different encryption techniques [14] [17] have been used to protect user data in the cloud to prevent information leaking during machine.

2. Literature Survey

Cloud computing has advanced significantly in recent years. Storage as a Service is the foundational element and core of many. applications including counterfeit detection, photo forensics, and pattern recognition. There is a lot of data kept on the cloud as a result of this. Amazon Web Services (AWS) is now the industry standard for cloud computing. Because of this, Open, a Swift-based cloud storage system, has swiftly risen to the top of the list in terms of usage. Even though it raises serious security issues, Swift's open nature nonetheless enables the provision of useful services. According to a study, client data is lost in two-thirds of incidents, typically as a result of managerial incompetence and hostile actions. Due to this, the storage layer's security is jeopardized, and the user's information is at risk of being misused. Additionally, Swift protocol weaknesses could allow user data or configuration information to be stolen. According to a security report published by the OpenStack VMT Vulnerability Management Team, to leak. The usage of Shaw et al.'s cloud-based data security storage approach may help prevent data leaks and enhance Apache Spark's security. User data saved in the cloud is protected using a number of techniques to prevent sensitive information from escaping throughout the ML process. But the aforementioned research needs secure key management methods to protect cryptographic data. A Hadoop-based distributed storage system that safeguards the confidentiality is created by Zerfos et al. by distributing and encrypting the information kept in the cloud. For more accurate reading, it executes data compilation and decoding procedures in advance. There Since there is no permanent storage for keys outside of memory, this technique requires a key cache server to function. Thus, the goal of this research is to introduce CSSM, a cloud secure storage method, in order to stop cloud data leaks at the storage layer. By combining data hashing and data encryption, CSSM is able to store vast amounts of cloud data as well as keys in hashed ciphertexts. User passwords and secret sharing are used to increase the security of keys. The OpenStack Swift protocol was used in the development and testing of CSSM.

3. OVERVIEW OF THESYSTEM

3.1 Existing System

Nishide et al. presented the first work that took user privacy into account, in which the access policy was partially hidden by splitting an attribute into two parts—value and name—while only concealing the value. The adversary cannot obtain any user data because of the disguised policy. However, because of the very high cost of calculation, their plan is unfeasible. A CP-CSSM approach with dual system encryption was proposed by Waters in 2009. It offered a fresh method for maintaining privacy in CP-CSSM. Then Lai et al. applied this method to create two HP-CP-CSSM hidden access policy CP-CSSM schemes. It has been demonstrated that both of them provide total security. The second one supports linear secret whereas the first one simply supports AND gate..

3.1.1 Disadvantages of Existing System

- The current work's approach lacks ciphertext-policy attribute-based encryption (CP-CSSM), which guarantees data secrecy.
- While CPABKS schemes are capable of one-to-many encryption and expressive access control in the current work, they are unable to detect data users who are disclosing the secret keys if the 'culprits' share the same subset of qualities as other honest data users..

3.2 Proposed System

We offer an HP-CP-CSSM system allowing efficient authority identification, which is utilized to help the user establish whether he or she is permitted or not, motivated by the aforementioned difficulties and based on. The auxiliary information is used to generate the test parameters in Abdalla's verifiable random functions, which is where the test technique originates. The suggested method may fix the ciphertexts verification without revealing the users' privacy.

3.3 Methodology

Healthcare Service Provider

In this module, Provider has to register to cloud and View all the CDA received and request to the cloud to access the generated CDA from hospital - A & hospital - B. Once the access request is granted by the cloud the provider will write the reply letter for corresponding CDA reports and sends.

Patient/End User

In this module, the user/patient Registers to cloud and

is authorized by the cloud and Logs in the user/ patient has to request the search key to search the patient CDA and also request for the view permission from the cloud. If the permission is provided by the cloud the corresponding user/patient can view the CDA generated and the corresponding reply from the doctor.

Hospital - A

4 In this module, CDA is generated, encrypted as hospital-A document and then uploaded to cloud, also can view the CDA replies from Healthcare service provider and can view all the generated CDA's.

Hospital - B

In this module, CDA is generated, encrypted as hospital-B document and then uploaded to cloud, also can view the CDA replies from Healthcare service provider and can view all the generated CDA's.

Cloud Server

In this module the cloud will authorize both the doctor and the patient/user. Receive all CDA generated from the hospitals and store, Select the doctor and Sends the CDA report for corresponding doctor. Provide permission for the CDA requests requested by the provider and also generates the search key.

5 Architecture

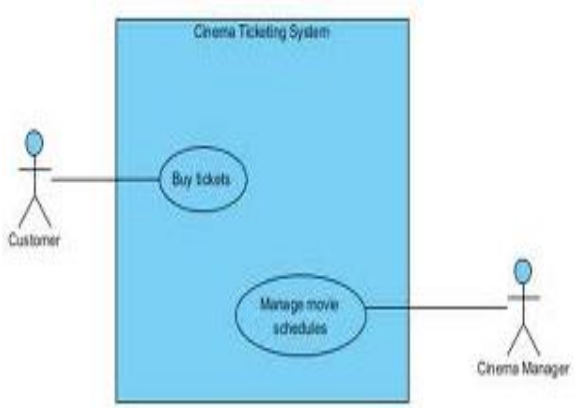
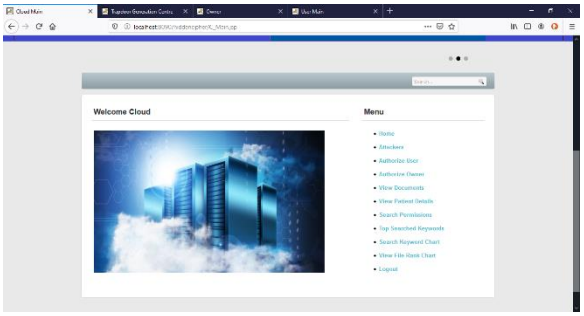


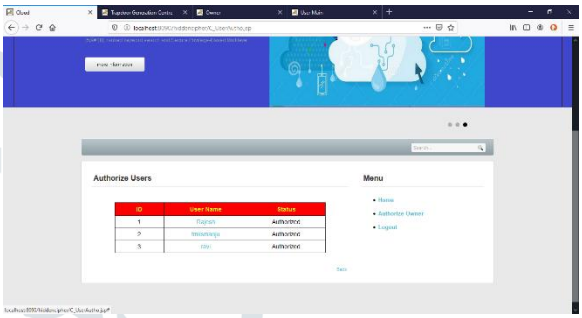
Fig 1: Frame work of proposed method

6 RESULTS SCREEN SHOTS

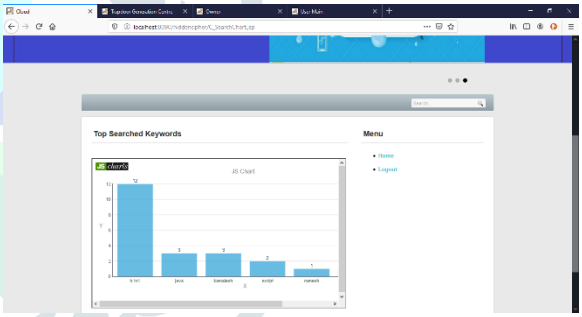
Home Page:



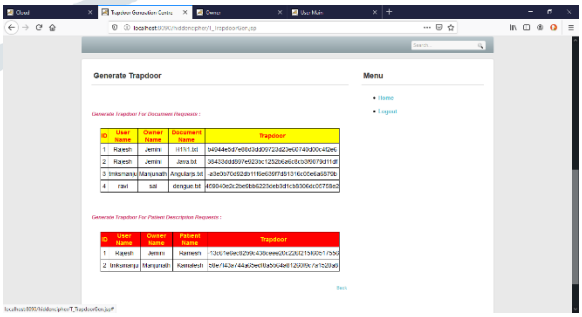
Authorized User:



File Rank:



Result:



7. CONCLUSION

✓ Using deep learning, we correctly identified the photos of a person's chest X-ray images as either pneumonia or normal in this study. We used a dataset of chest X-ray pictures of two types (pneumonia afflicted and normal) and trained it using CNN as well

as some transfer learning methods. Following the training, we tested the system by uploading a picture and classifying it.

Future Enhancement

- ✓ This can be used in the future to readily define the sorts of different infections, making it easier to identify infections in their early stages and cure them.

8. References

[1] WHO Pneumonia. World Health Organization. (2019), https://www.who.int/news-room/fact-sheets/ detail/pneumonia

[2] Neuman M., Lee E., Bixby S., Diperna S., Hellinger J., Markowitz R., et al. Variability in the interpretation of chest radiographs for the diagnosis of pneumonia in children. Journal of Hospital Medicine. 7, 294–298 (2012) https://doi.org/10.1002/jhm.955 PMID: 22009855

[3] Williams G., Macaskill P., Kerr M., Fitzgerald D., Isaacs D., Codarini M., et al. Variability and accuracy in interpretation of consolidation on chest radiography for diagnosing pneumonia in children under 5 years of age. Pediatric Pulmonology. 48, 1195–1200 (2013) https://doi.org/10.1002/ppul.22806 PMID: 23997040

[4] Kermany D., Zhang K. & Goldbaum M. Labeled Optical Coherence Tomography (OCT) and Chest X-ray Images for Classification. (Mendeley, 2018)

[5] Lal S., Rehman S., Shah J., Meraj T., Rauf H., Damasˇevičius R., et al. Adversarial Attack and Defence through Adversarial Training and Feature Fusion for Diabetic Retinopathy Recognition. w

[6] Rauf H., Lali M., Khan M., Kadry S., Alolaiyan H., Razaq A., et al. Time series forecasting of COVID-19 transmission in Asia Pacific countries using deep neural networks. Personal and Ubiquitous Computing. pp. 1–18 (2021) https://doi.org/10.1007/s00779-020-01494-0 PMID: 33456433

[7] Deng J., Dong W., Socher R., Li L., Li K. & Fei-Fei, L. Imagenet: A large-scale hierarchical image database. 2009 IEEE Conference on Computer Vision and Pattern Recognition. pp. 248-255 (2009)

[8] Dalhoumi S., Dray G., Montmain J., Derosière, G. & Perrey S. An adaptive accuracy-weighted ensemble for inter-subjects classification in brain-computer interfacing. 2015 7th International IEEE/EMBS Conference on Neural Engineering (NER). pp. 126-129 (2015)

[9] Albahli S., Rauf H., Algosaibi A. & Balas V. AI-driven dee CNN approach for multi-label pathology classification using ches X-Rays. PeerJ Computer Science. 7 pp. e495 (2021 https://doi.org/10.7717/ peerj-cs.495 PMID: 33977135.