

INTRUSION DETECTION SYSTEM FOR CLOUD BASED ON NAIVE BAYES AND HASHING

¹Amruta Deshmukh, ²Kirti Girdhani, ³Nayan Keskar, ⁴Prajakta Gite

BE Computer Engineering
LGNSCOE, Nashik

Abstract: Network traffic in the cloud computing environment is characterized by large scale, high dimensionality, and high redundancy, these characteristics pose serious challenges to the development of cloud intrusion detection systems. Deep learning technology has shown considerable potential for intrusion detection. Therefore, this study aims to use deep learning to extract essential feature representations automatically and realize high detection performance efficiently. An effective stacked contractive autoencoder (SCAE) method is presented for unsupervised feature extraction. By using the SCAE method, better and robust low-dimensional features can be automatically learned from raw network traffic. We are creating a system that allows user to provide security to their files and protect them from hacker and avoid the malicious attacks, we are encrypting the password by hash and also if the hacker break are hash code it will get only the dummy data, OTP will also will there for authentication.

Keywords: Cloud computing, Data security, encryption and decryption, data storage in cloud.

I. Introduction:

Security issues have brought about serious harm to the distributed computing climate, antagonistically influencing the sound and economical improvement of distributed computing. Interruption recognition is one of the advancements for shielding the distributed computing climate from malignant assaults other local computers. Cloud computing is the information technology services and product. It support the virtualized resources, which is based on the reusability of IT infrastructure. Cloud Computing is the sequence of all required hardware, software, platform, applications, infrastructure and storage only with online identification. This project is been introduce Security issues have brought about serious harm to the distributed computing climate, antagonistically influencing the sound and economical improvement of distributed computing. Interruption recognition is one of the advancements for shielding the distributed computing climate from malignant assaults.

II. Literature Survey:

In literature survey we learn guides or helps the researcher to define/find out/identify a problem. It is something when you look at a literature in a surface level, or an Ariel view. It includes the survey of place people and publications is context of research.

[1] Medical organizations find it challenging to adopt cloud-based electronic medical records services, due to the risk of data breaches and the resulting compromise of patient data. Existing authorization models follow a patient centric approach for EHR management where the responsibility of authorizing data access is handled at the patients' end. This however creates a significant overhead for the patient who has to authorize every access of their health record. This is not practical given the multiple personnel involved in providing care and that at times the patient may not be in a state to provide this authorization. Hence there is a need of developing a proper authorization delegation mechanism for safe, secure and easy cloud-based EHR management. We have developed a novel, centralized, attribute based authorization mechanism that uses Attribute Based Encryption (ABE) and allows for delegated secure access of patient records. This mechanism transfers the service management overhead from the patient to the medical organization and allows easy delegation of cloud-based EHR's access authority to the medical providers. In this paper, we describe this novel ABE approach as well as the prototype system that we have created to illustrate it.

[2] The rapidly growing demand for cloud services in the current business practice has favored the success of the hybrid clouds and the advent of cloud federation. The available literature of this topic has focused on middleware abstraction to interoperate heterogeneous cloud platforms and orchestrate different management and business models. However, cloud federation implies serious security and privacy issues with respect to data sovereignty when data is outsourced across different judicial and legal systems. This column describes a solution that applies encryption to protect data sovereignty in federated clouds rather than restricting the elasticity and migration of data across federated clouds.

[3] For building a secure cloud storage service on top of a public cloud infrastructure, attribute-based encryption (ABE) has been a preferred solution due to its flexible access control. ABE, however, incurs heavy computation cost on users during decryption. Thus, previous studies solved this problem by enabling cloud servers to perform a part of decryption operations on behalf of the users. In order to empower users to verify the correctness of the delegated decryption by the cloud, they employed a cryptographic commitment or message authentication code (MAC) to enable users to check the correctness of partial decryption of the cloud. However, the previous schemes fail to ensure the correctness of computation in the presence of malicious cloud servers. In this paper, we propose a novel and generic commitment scheme for ABE, which is secure against tampering attacks by malicious cloud servers. According to the performance analysis, the proposed scheme is only 0.5 ms slower on average than the previous commitment-based schemes and two to three times faster than the MAC-based scheme.

[4] Storage-as-a-service is an essential component of the cloud computing infrastructure. Database outsourcing is a typical use scenario of the cloud storage services, wherein data encryption is a good approach enabling the data owner to retain its control over the outsourced data. Searchable encryption is a cryptographic primitive allowing for private keyword based search over the encrypted database. The setting of enterprise outsourcing database to the cloud requires multi-user searchable encryption, whereas virtually all existing schemes consider the single-user setting. To bridge this gap, the system propose a practical multi-user searchable encryption scheme, which has a number of advantages over the known approaches.

[5] Cloud computing is a new technology that transfer the computing process from personal computers into cloud servers over the internet. Nevertheless, as the client information data is stored in the cloud provider servers, the confidentiality of the information become a new concern. Different algorithms based on Encryption is presented previously to provide cloud clients with confidentiality. The main idea of encryption algorithms for cloud data is to permit cloud clients queries to be handled using encrypted data without decryption. This paper presents a new security mechanism using hybrid method of encryption algorithms and a distribution system to enhance cloud database confidentiality. A vertical fragmentation technique is adopted from alsirhani's model for distributing data over clouds. However, to overcome a weakness in alsirhani's model where compromises to a fragment can still make data meaningful. Instead, the proposed model uses a hybrid fragmentation technique to make data on fragments meaningless if compromised. The proposed model distributes the cloud database among the clouds using the provider views and level of confidentiality that is delivered by the employed encryption algorithms. To evaluate the proposed searchable encryption and hybrid fragmentation model, the study developed a Java application for simulating the hybrid cloud. The simulation combines public and private clouds; as essential processes is conducted inside the private cloud. The evaluation of the work was conducted by comparing the proposed model with existing solutions in query response and security characteristics. Preliminary results showed that the proposed searchable encryption and hybrid fragmentation model provides a secure mechanism that enhances data confidentiality in terms of faster response and additional security

III. System Architecture:

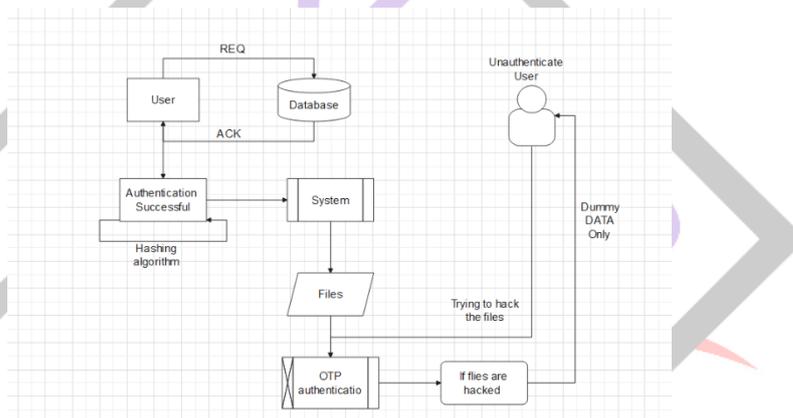


Fig.4. System Model

Network traffic will continue to increase dramatically and will inevitably encounter malicious attacks. Network attacks not only result in severe damage to the cloud environment but also cause tenants to lose confidence in cloud computing itself, which will adversely affect the healthy and sustainable development of cloud computing. Intrusion detection is one of the technologies for protecting cloud computing from malicious attacks.

A. System Model: A user sends a request to Management Centre and encrypts the file, then it results as the cipher text to CSP. Users who belong to completely different role groups owning the corresponding role keys, with the role keys the user access cloud server, the user will upload or transfer the files from Cloud Service Provider. And user can download the file from the cloud server. A Cloud Service Provider is mainly for data storage, management and verification. Cloud Service Provider stores and manages the uploaded files from authorized user Management Centre is the trusted third party that is for the authorized user and for the role key management.

B. Adversary Model: A1 may has the communications between CSP and also the user to induce the transmitted info and plays a job of the user to act with the CSP. A2 may listen the communications between CSP and also the user to urge the transmitted info, and cloud exchange S min bytes info with the user. A3 might discard the user's knowledge that haven't been accessed or rarely accessed, and should tamper the user's knowledge to take care of reputation. A role authorized tree to manage the user's role and implement the role re-encryption key updating and revoking with efficiency that satisfies the change of authorized user's privilege. Once performing the secure knowledge deduplication, CSP will check the ownership of the licensed user. Security analysis shows that our proposed system is secure beneath the proposed security model, and performance analysis demonstrates the effectiveness and efficiency of our proposed system.

C. Design Goal: The main goal of the system is to protect the data from the cloud storage and the cloud server should be secure from the unauthorized user. So, then there will not any leakage in the cloud server.

D. Convergent Encryption: The same keys are always obtaining the same cipher text that can be by the two users with the new plaintext without the encryption keys.

E. Role Key Update: In role key updating, the generation of role keys is done in the management Centre. The user can perform updating, downloading using the role re-encryption. And the management Centre supports the role authorized tree.

IV. Algorithm and Methods:

[I]Cryptography: is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process A new key (KEY1) using a hash function with stored KEY and delivers to the user/client by a secured channel (email, mobile etc.). User will enter KEY1 into the system. System will match this KEY1 with its previously generated KEY. Successfully matched, system will generate again a KEY using anti-hash function from KEY1 and matched with its stored KEY. If matched again successfully, then system will treat this user as a valid user. This authentication system works in three steps. Firstly, supplying user ID and Our main goals are to secure stored data and authentication system in cloud environment. Many researchers tried to secure various credentials of users such as secure login, storing data/file with encryption, key management etc. By any means, if a hacker enters into the system, he may steal data/files from could end. If one intruder may successfully enter to cloud environment, then there is no way to detect him as a thief. By his credential he may access all data of the system. The system has offered such a system/environment that if any person enters into cloud end by any means, he will not succeed to get data/files from the cloud end. He will be caught. The procedures are described in next section.

A. Users Authentication:

When any clients/users will access his data/files or send new files, he has to login with his credential (user ID and password). If his credential is valid, then he will enter into next step of authentication. By this time, system will generate

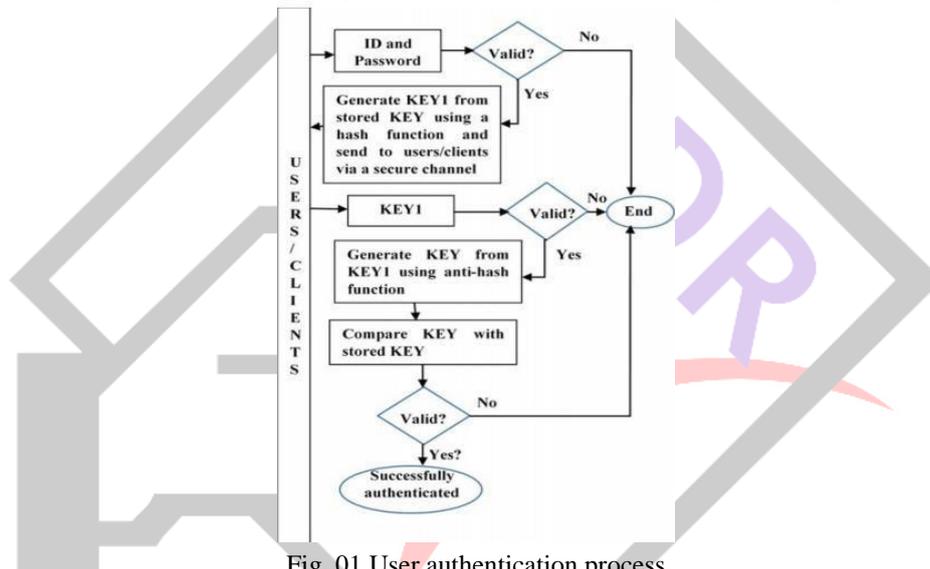


Fig. 01 User authentication process

using a hash function with stored KEY). This KEY1 will be sent by a secured channel to the user. Thirdly, verifying stored KEY with newly generated KEY using anti-hash function with KEY1 (user supplied KEY1). As the system has stated earlier that, hackers will be caught even he supplies valid user ID and password. He will also be caught even while accessing the file that stored KEYS. As system will generate KEY1 using a hash function with stored KEY and sends KEY1 to the user by a secure channel, the invalid users/ hackers will not be able to access this KEY1. So, he will not be able to supply new KEY1. So there is no way to access data/file by an invalid user. An extra protection is also available by verifying stored KEY with newly generated KEY using anti-hash function with supplied KEY1. This system is described in Fig. 1 and Algorithm 1. After successfully login, user will able to access his data/file or send new file to cloud. Encrypted files/data will be decrypted using valid KEY and will send to the users.

B. Cloud End Auto Encryption: Auto encryption procedure is described in Fig. 2 and Algorithm 2. In the Fig. 2, the system has proposed an automated encryption system. This encryption system may be used hybrid cryptography system including RSA and AES or any other suitable encryption method. After login (described in previous section) users may access or send new data/files to store in the cloud and later he may logout. After successful logout, the system will lock those files/data, the user has been accessed or stored. Then system will create a new key (KEY2) by using a hash function with previously used KEY. Using this new key (KEY2), those files/data will be encrypted and new key (KEY2) will be replaced with previous stored KEY.

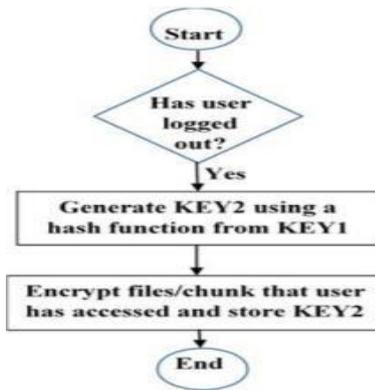


Fig. 02 Cloud end auto encryption

V. Hash algorithm:

A hashing algorithm is a mathematical algorithm that converts an input data array of a certain type and arbitrary length to an output bit string of a fixed length. Hashing algorithms take any input and convert it to a uniform message by using a hashing presented for unsupervised feature extraction.

VI. Conclusion:

An Intrusion detection system is a component of the defensive operations that complements the defenses such as firewalls. The Intrusion detection system mainly detects attack signs and then alerts the system for such instructions and send the dummy data only to attackers/ hackers. According to the detection method, Intrusion detection systems are usually categorized as misuse detection and anomaly detection systems. The operation point of view, they are be classified in network based or host based IDS. In current Intrusion detection systems information is composed from both network and host resources. In terms of presentation, an Intrusion detection system becomes more correct as it detects more attacks and send to the dummy data to hackers. Hence We are making a framework that permits client to give security to their documents and shield them from programmer and stay away from the noxious assaults , we are encoding the secret word by hash and furthermore if the programmer break are hash code it will get just the fake information, OTP will likewise will there for confirmation ,we are overcoming the drawback of existing system , and providing a smart system that will not only monitor and control our data with security but also supply it to whenever necessary.

VII. Future Scope:

With more security options and with more accuracy. Security concerns not only lead to severe losses in the cloud computing environment but also cause users to lose confidence in cloud computing itself, which will inevitably have a serious impact on the healthy and sustainable development of cloud computing. Using a stochastic approach to determine the threshold value that directly affects the accuracy of the proposed models.

VIII. Results:

A user will log-in into the system. And upload his/her documents. If a user wants to access/download his/her files then the user has to be verified with three factors i.e Email OTP, Mobile OTP and Security Question. After verifying these three things, the user will get access to the files and can download it.

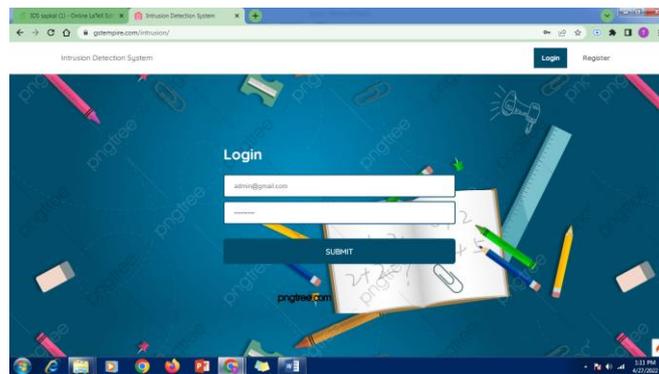


Fig: Login Page

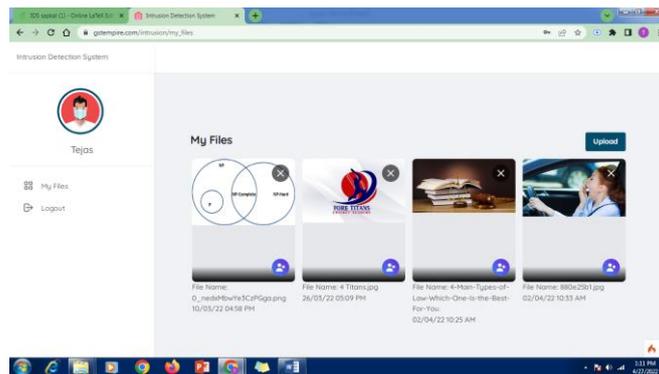


Fig: Homepage for user

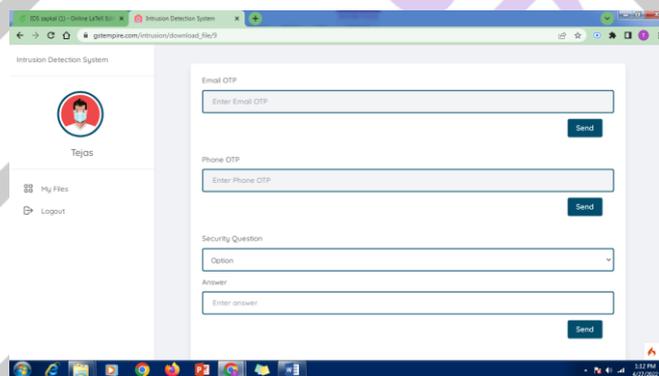


Fig: Authentication Page

References:

- [1] Maithili Arjunwadakar and R.V. Kulkarni, "The rule-based Intrusion Detection and Prevention Model for Biometric System", Journal of Emerging Trends in Computing And Information Sciences, OCT 2010.
- [2] Todd Vollmer, Jim Alves-Foss and Milos Manic, "Autonomous rule creation for intrusion detection", 2011 IEEE Symposium on Computational Intelligence in Cyber Security.
- [3] M. Sebring, E. Shellhouse, M. Hanna and R. Whitehurst, "Expert systems in intrusion detection: A case study", Proceedings of the 11th National Computer Security Conference, pp. 74-81, 1988.
- [4] T. Lunt, R. Jagannathan, R. Lee, S. Listgarten, D. Edwards, P. Neumann, et al., IDIS: The Enhanced Prototype. A Real-Time Intrusion Detection System, 1988.
- [5] D. Anderson, T. Lunt, H. Javitz, A. Tamaru and A. Valdes, Detecting Unusual Program Behavior Using the Statistical Component of the NextGeneration Intrusion Detection Expert System (NIDES).
- [6] H. Anggeriana, S. Kom and M. Kom, "Cloud Computing", Jurnal Teknik Informatika, vol. 1, 2011.
- [7] T. Velte, A. Velte and R. Elsenpeter, Cloud computing a practical approach, McGraw-Hill, Inc, 2009.
- [8] P. Mell and T. Grance, "The NIST definition of cloud computing", National Institute of Standards and Technology, vol. 53, pp. 50, 2009.
- [9] A. Yousif, M. Farouk and M. B. Bashir, "A Cloud Based Framework for Platform as a Service", in Cloud Computing (ICCC) 2015 International Conference on, pp. 1-5, 2015.
- [10] E. Hossny, S. Khattab, F. Omara and H. Hassan, "A Case Study for Deploying Applications on Heterogeneous PaaS Platforms", in Cloud Computing and Big Data (CloudCom-Asia) 2013 International Conference on, pp. 246-253, 2013.

- [11] M. O. Imam, A. Yousif and M. B. Bashir, "A Proposed Software as a Service (SaaS) Toolkit for Cloud Multi-Tenancy", *Computer Engineering and Applications Journal*, vol. 5, 2016.
- [12] M. M. Alani, *Elements of cloud computing security: A survey of key practicalities*, Springer, 2016.
- [13] A. team, *Open Source Metadata-Based Java ORM Framework for Cloud SaaS Applications*, 2011, [online] Available: <http://www.athenasource.org/java/>
- [14] S. Paliwal, "Cloud application services (SaaS)-Multi-Tenant Data Architecture", Infosys technologies limited, Sep 2014, [online] Available: http://www.cmg.org/wpcontent/uploads/2012/11/m_94_4.pdf.
- [15] S. A. Elmubarak, A. Yousif and M. B. Bashir, *Performance based Ranking Model for Cloud SaaS Services*, 2017

