International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488|

|| Volume 8, Issue 6, June 2020 ||

Emotion Aware Multimedia Security using Role Base Access Control in Public Cloud Environment

Vaishali Uday Gaderao[1], Dr. Sunil D. Rathod[2]

P.G. Student, Department of Computer Engineering, Dr. D. Y. Patil School of Engg, Pune, India[1]

Assistant Professor, Department of Computer Engineering, Dr. D. Y. Patil School of Engg, Pune, India[2]

ABSTRACT: Multi-cloud storage provides a solution to the risks and challenges of cloud computing by storing data via various cloud service providers (CSPs), including vendor lock-in, and data privacy. CSB is Software-as - a-Service (SaaS) third-party cloud storage service provider that manages the relationship between one or more CSPs and cloud clients. Cloud is an emerging technology and cloud based storage is a new concept that allows users not only to upload data to the internet, but also to easily access available resources and share data with anyone at any time. But cloud is a technique that generates a restore feature that enables clients to go back to a previous one attack state or Computer catastrophe provides an easy way to remove malware and computer security. The attackers have short- term windows where they should be trained and targeted for remote start-up and stoppage of VM. This is an extremely effective tool for defense. Because the hypervisor operates from Virtual Machine it is possible to control malware. VM Infrastructure will secure itself as a physical server infrastructure for such purposes. In this paper we describe literature study of user activity base cloud attack detection and prevention techniques using machine learning techniques. We also proposed an approach to forensic investigation, using Log Information and VM logs of the malicious activities in the cloud environment. To ensure the security of Log files we aim to apply Encryption algorithms to Log information, which will be helpful for further investigation.

KEYWORDS: Access control, Attributes-Based Encryption, data storage, Multi-Authority.

I.INTRODUCTION

Cloud storage is an significant amenity of cloud computing, which delivers services for data owners to subcontract data to collection in cloud via Internet. As cloud storage abstains several benefits, there is quiet remainders numerous challenges amongst which, privacy as well as security of users' data need major issues in public cloud storage. Usually, a data owner stores users data in trusted servers, organized by a totally trustworthy administrator [3]. Attribute-based Encryption (ABE) is observed as one of the utmost appropriate arrangements to bearing data access control in public clouds aimed at it can promise data owners direct control over their data and provide a fine-grained access control service. In further most present CP-ABE [1], [2] arrangements there is only one expert witness accountable for attribute management as well as key distribution. This only-one-authority consequence can carry a single-point bottleneck on both security and performance. Currently we use threshold multi authority CP-ABE access control system, named RAAC, to treaty with the single-point bottleneck on together security as well as performance in greatest present schemes. RAAC is Threshold Multi-Authority Access Control System. In RAAC, multiple authorities together accomplish the entire attribute set but no one devises full control of any precise attribute.

II.LITERATURE SURVEY

According to Apolinário et.al [1] S-AUDIT is a platform that provides quality control of the data stored in business clouds. S-AUDIT uses homomorphic, digital signature authentication to prevent secure cloud access to data. To demonstrate how it can be used in real life, the software was combined with a cloud-backed file system called shared cloud backed file system (SCFS). Commercial cloud storage services like the Dropbox, Google Documents, Microsoft One Drive and Amazon S3 are widely accepted. Digital signatures are used for collective storage when data is exchanged between multiple cloud users, whereas digital certificate are used to validate the single cloud user authentication.

Author Hussein, NehadH. [2]. The cloud-based secure storage and medical image sharing using Secured Hashing Algorithm(SHA) and Elliptical curve cryptography(ECC) encryption algorithm on cloud environment. The suggested solution is based on the number of cryptography techniques needed to create better protection over the transmission

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488|

|| Volume 8, Issue 6, June 2020 ||

path on the cloud for medical images. The following algorithms can be used here: Elliptic Curve Cryptography (ECC), Advanced Encryption Standard (AES), and Safe Hash (SHA-3). Once they are processed in the cloud, the third-party auditor is used to check the validity and reliability of medical images to reduce the computing burden on the computers of the clients. It also generates a digital signature to ensure whether the data source is secure and robustness for attack detection when any data modification done by unauthorized user. The results show that the algorithm verifies data protection at a high level by encryption analysis.

Jeong, Junho, et al. [3] A secure IoT-based cloud Storage technology focused on a validated data-possession model, using Bloom filters. The experimental results have shown that the proposed method saves time and has no significant differences with existing methods in the verification rate although the Bloom filter results in false positives. IoT technology allows a variety of devices to access the Internet, such as small sensors in a network.

Cui, Bo, ZhikunLan et.al [4] Improved RBAC type called ET-RBAC. ET-RBAC incorporates environment module and time module constraints according to the original RBAC model in order to accomplish complex authorization and resource allocation of tasks. The non-relevant revocation approach is practiced for resource revocation and approvals, to minimize the effect of dynamic changes on next-level task permits at the top-level feature. This system also design and implement the ET RBAC model including feature design, user design, authorization design, family group design, and resource allocation process design system.

Sukmana, Muhammad IH, et al. [5] Multi Cloud service provider(CSP) Access Control Management Integrated Cloud Access Control Framework for Centralized and Automated User Services and Abstraction. This system basically offers roles-based access control for Cloud Service Brokers (CSB). The stakeholders can access cloud resources by assigning the necessary privileges and get the access control list to cloud resources which is provided by CSB to stakeholders, respectively. This techniques design is based on compliance with the privilege separation and the least privilege principle. System integrate the unified access control and security model into a CSB system called that Cloud RAID for Business (CSB). Such approach also provides network and cloud security service evaluation centralized management of resource and access control in multiple CSPs.

According to author Soni, Kritika, and Suresh Kumar et.al [6] Cloud computing provides easy access to shared computer resources (networks, servers, storage, applications and services) on demand. RBAC and Attribute Based Access Control (ABAC) complete this work, both are effective in different environment. Basically RBAC depends on data owners priority, according to data sharing technique while ABAC is related to attribute based access control where user can access data based on combination of various attributes. Both techniques have defined for two different environments like public and hybrid cloud. ABAC basically uses for public cloud environment and RBAC effective for all environments. RBAC offers access to resources based on the functions permission. It simplifies the authorization process because many users may be given the same permission to perform the same role.

According to Yang, Kan [7] Efficient, revocable data access control scheme for multi-authority cloud storage systems where multiple authorities verify the users identity works like proxy server. This system also carried out to eliminate certificate verification based along process as well as single point bottleneck issue. System specifically suggesting a multi-authority revocable Ciphertext base Attribute base Encryption (CP-ABE) scheme and using it to develop the data access control scheme as the underlying techniques. This system revocation of attributes will achieve protection both forward and backward kind of SaaS attacks like session hijack or bypass authentication etc.

Reddy, G. Venkatakoti [8] Data Access Control and Multi-Authority Cloud Storage System called (DAC-MACS). Data Access Control managed by appropriate RBAC algorithm for data privacy . While multi-authorization with Cipher text-Policy Attribute-Based Encryption (CP-ABE) scheme has used for user authentication. Multiple Attribute Authorities (AA's) has used for user's request verification which eliminate the single point bottleneck issues in cloud environment. The effectiveness of this system also provide highest security in trusted as well as untrusted cloud platforms.

Rajput, Amitesh Singh et.al [9] provides optimized Elgamal encryption scheme based on local color correlation technique, which provides privacy preservation for or sensitive information. Additionally, this system is suggesting a block-based image encryption method using the logistic-tent scheme and the ElGamal cryptosystem. As a consequence the size of the encrypted image is significantly reduced compared with the naive approach. Photos are taken from camera sensors to monitor. The vision system for humans / machines is processed at their best.

Zhang, Yin, et al. [10] A security policy based Identity-based authentication and access control policy ensuring an integrated robot or edge system security certificate while retaining proper access control over the private data stored in the edge cloud; in particular, it adopts a polynomial-based approach control strategy and proposes a safe and effective access control scheme. This paper also introduces the identity authentication method for edge cloud systems, which can reduce overhead computation and authentication latency in a shared multi-edge cloud authentication. The Emotional computer, edge cloud, and remote cloud also store plenty of user-interacted personal data. Accordingly, the authorization to validate access to data is essential for user privacy protection. Several studies exist on access control

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488|

|| Volume 8, Issue 6, June 2020 ||

and identity protection of a new type of network architecture, such as software-identified networks or cyber-physical systems (CPS).

III.PROPOSED SYSTEM

In this proposed system, we applied a method called Multi Access Cloud Storage.. This method will overcome the disadvantage of single bottle neck problematic. This System consists of Multiple Attribute Authorities (Admin) but they are not interring linked between each other's. So the Unofficial operators cannot be negotiation the Admin for Lawful user's private key. So, the Lawful Users can get the Make available Keys by requesting a few t authorizes. So the Private Key communication is extra protected.

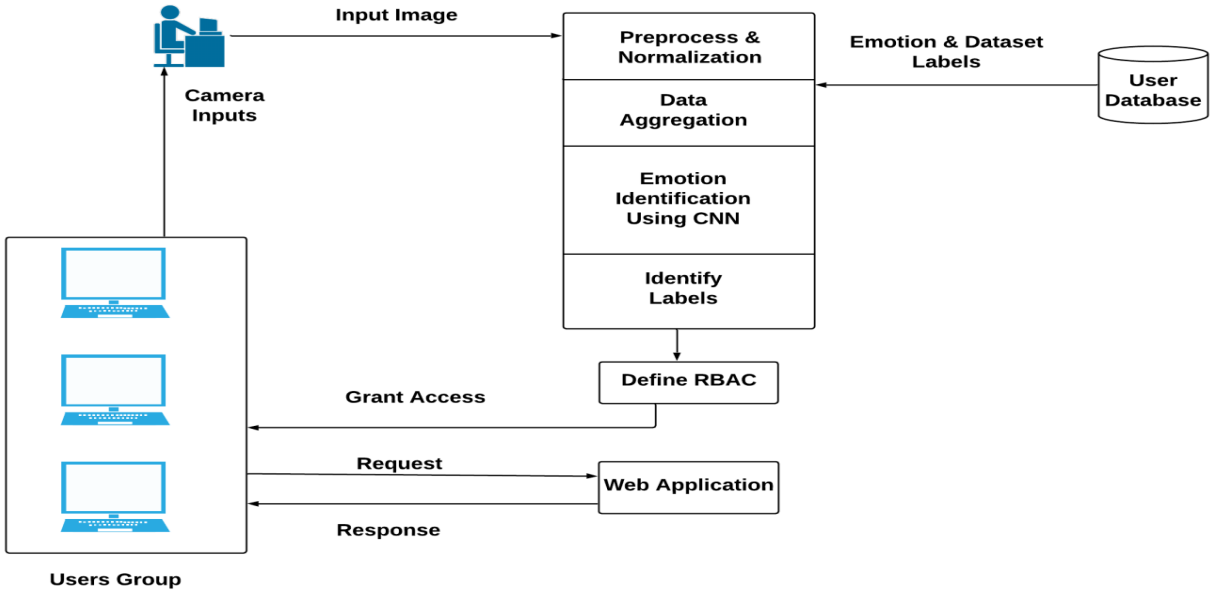

Figure 1: Proposed System architecture

System Modules

In this research we proposed emotion aware base security approach using user's interaction opinion or communication behavior with system. Such approach is similar like role base access control (RBAC) [1]. When any user communicates with system is generate malicious request and send to data server, which may harmful, using this approach we try to eliminate such malicious request using proposed RNN algorithm which effectively detect such, malicious requests and revoke it dynamically. The entire system illustrates some modules which is given in below.

Intruder Detection Systems

Intruder detection systems (IDS) are used to alert users of an attack. These systems monitor a specific system in order to gather and analyses information to determine whether there is a security threat. These security threats can range from something as begin as someone mistyping a password to something malevolent as a Denial of Service attack. In order to maximize the efficiency of checking for security threats, IDSs are specialized to handle specific components. For instance, there are network IDSs which specialize in monitoring network traffic for malicious activity.

IV.ALGORITHM DESIGN

Input: Test Dataset which contains various test instances TestDBLits [], Train dataset which is build by training phase TrainDBLits[] , Threshold Th.
Output: HashMap <class_label, SimilarityWeight> all instances which weight violates the threshold score.
Step 1: For each read each test instances using below equation

$$testFeature(m) = \sum_{m=1}^{n} (.\ featureSet[A[i] \dots \dots A[n] \leftarrow \text{TestDBLits})$$

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488|

|| Volume 8, Issue 6, June 2020 ||

Step 2 : extract each feature as a hot vector or input neuron from $testFeature(m)$ using below equation.

$$\text{Extracted\_FeatureSetx[t……n]} = \sum_{x=1}^{n}(t) \leftarrow testFeature\ (m)$$

Extracted_FeatureSetx[t] contains the feature vector of respective domain

Step 3: For each read each train instances using below equation

$$trainFeature(m) = \sum_{m=1}^{n}(.\ featureSet[A[i] \ldots\ldots A[n] \leftarrow \text{TrainDBList}\ )$$

Step 4 : extract each feature as a hot vector or input neuron from $testFeature(m)$ using below equation.

$$\text{Extracted\_FeatureSetx[t……n]} = \sum_{x=1}^{n}(t) \leftarrow testFeature\ (m)$$

Extracted_FeatureSetx[t] contains the feature vector of respective domain.

Step 5 : Now map each test feature set to all respective training feature set

$$weight = calcSim\ (\text{FeatureSetx} \mid\mid \sum_{i=1}^{n} \text{FeatureSety[y]})$$

Step 6 : Return Weight

V. DATASET USED

For this system we used only MYSQL dataset for back end execution. We used all text base dataset from uploading as well as sharing purpose. The only text base data can encrypt by PBE with MD5 and DES encryption algorithm.

VI.RESULTS AND DISCUSSION

For the Evaluation of performance of the processes, accurate measurement of matrices. The software is designed with INTEL 2.8 GHz i3 processor on java 3-tier architecture platform and 4 GB of RAM on Amazon EC2 public cloud consol. We develop 2 physical network devices with Wi-Fi, and 10 VM with Amazon EC2 as a public cloud platform for system assessment. After some part of the system was implemented we got system performance at a reasonable level. Table 1 below shows the results of the proposed cryptography algorithm for plain text conversion and encryption decryption.

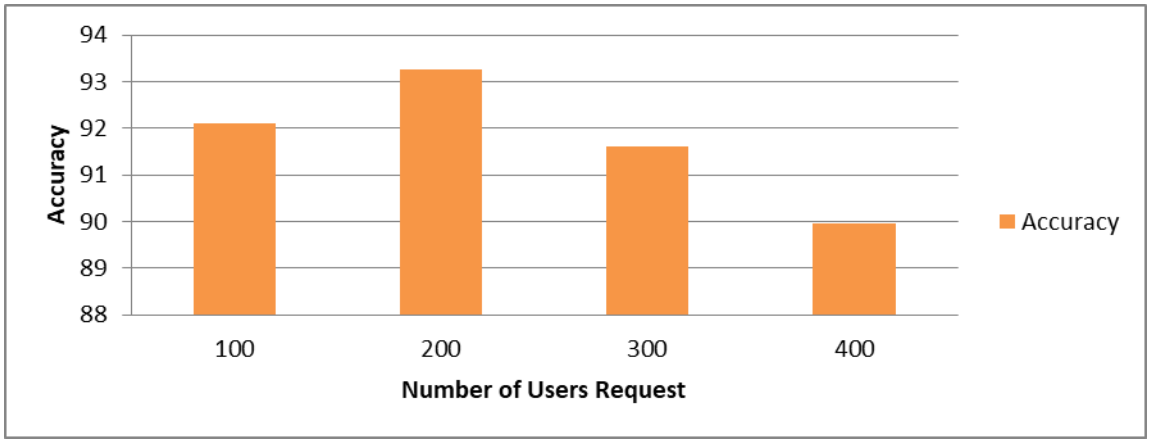

Figure 2 : malicious request detection accuracy

The above figure shows the number of malicious request successfully detected by our proposed system using designed algorithm.

VII.CONCLUSION

This work Presents an identity authentication and access control approach for emotion-conscious robot systems, and by analyzing their architecture, summarizes security concerns. This paper proposes a privacy protection of identity

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488|

|| Volume 8, Issue 6, June 2020 ||

information with low overhead computation that supports edge cloud node mutual authentication, while a universal access control system fulfills the security requirement and supports a single user's edge cloud node and multiple devices. The efficacy of the authentication system for collective identity is higher than that of traditional approaches by research on the actual tested. To evaluate the proposed system on various distributed environment in fog nodes with different input objects, and to work with unstructured large dataset will be also interesting future work for this research.

REFERENCES

[1] Apolinário, Filipe, Miguel Pardal, and Miguel Correia. "S-Audit: Efficient Data Integrity Verification for Cloud Storage." 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). IEEE, 2018.

[2] Hussein, Nehad H. "Cloud-Based Efficient and Secure Scheme for Medical Images Storage and Sharing using ECC and SHA-3." 2019 2nd Scientific Conference of Computer Sciences (SCCS). IEEE, 2019.

[3] Jeong, Junho, et al. "Secure Cloud Storage Service Using Bloom Filters for the Internet of Things." IEEE Access 7 (2019): 60897-60907.

[4] Cui, Bo, Zhikun Lan, and Xiangyu Bai. "Research on Role-based Access Control in IPv6 Smart Home." 2019 IEEE 9th International Conference on Electronics Information and Emergency Communication (ICEIEC). IEEE, 2019.

[5] Sukmana, Muhammad IH, et al. "Unified Cloud Access Control Model for Cloud Storage Broker." 2019 International Conference on Information Networking (ICOIN). IEEE, 2019.

[6] Soni, Kritika, and Suresh Kumar. "Comparison of RBAC and ABAC Security Models for Private Cloud." 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon). IEEE, 2019.

[7] Yang, Kan, and Xiaohua Jia. "Expressive, efficient, and revocable data access control for multi-authority cloud storage." IEEE transactions on parallel and distributed systems 25.7 (2014): 1735-1744

[8] Reddy, G. Venkatakoti, B. Thirumala Rao, and Naresh Vurukonda. "A review on active data access control for multi-authority cloud storage systems with users." 2017 International Conference on Big Data Analytics and Computational Intelligence (ICBDAC). IEEE, 2017.

[9] Rajput, Amitesh Singh, and Balasubramanian Raman. "Privacy-Preserving Smart Surveillance Using Local Color Correction and Optimized ElGamal Cryptosystem over Cloud." 2019 IEEE 12th International Conference on Cloud Computing (CLOUD). IEEE, 2019.

[10] Zhang, Yin, et al. "Emotion-aware multimedia systems security." IEEE Transactions on Multimedia 21.3 (2018): 617-624.