

# An Efficient Implementation Of Validating The Client Level Security Factors For The Cloud Applications

\* Poorvadevi. R,  
Assistant Professor,  
SCSVMV University,  
Kanchipuram.

\*\* Dr. K. Ramar,  
Principal,  
Einstein College of Engg,  
Tirunelveli

**Abstract-** Server can effectively validate the client using multimedia mining extraction and classifier analysis process. Fuzzy logic can set the strong security state for the user access credential over the client server, client trusted service maintenance through multimedia combined login form and multilevel security analysis process. Difficulties in the maintenance of key pairs are rectified through mining techniques.

Client level security issues in the cloud computing became a major challenge in service access process in cloud environment. Day by day number of threats over the network increasing because of the huge demand for the cloud product and service. The existing authentication systems are unable to provide the sufficient security and user Identification techniques. The proposed scheme, trying to provide the Optimistic user signature identification through mining analysis and also using Fuzzy logic based user classification module provide the sufficient security for the cloud service access. This scheme reduces the complexity involved in the key exchange process in cryptographic techniques. With the help of strong mining tools and fuzzy computations, trying to prove that proposed scheme will provide sufficient user classification and security.

MultiMedia Mining is the most recent trend in data mining techniques that will contains following aspects. Data collection is the starting point of a learning system, as the quality of raw data determines the overall achievable performance. Then, the goal of data pre-processing is to discover important features from raw data. Data pre-processing includes data cleaning, normalization, transformation, feature selection, etc. Learning can be straightforward, if informative features can be identified at pre-processing stage. Detailed procedure depends highly on the nature of raw data and problem's domain. In some cases, prior knowledge can be extremely valuable. For many systems, this stage is still primarily conducted by domain experts.

The demand of better quality cloud service and effective client validation techniques leads different levels security analysis on cloud environment. Many Organizations and cloud service vendors and end users need for optimum client validation and minimize risk in the service management. hackers those trying to access the data by proving themselves as a authorized client become challenge for the cloud vendors as well as for organization.

**Keywords-** Cloud Computing, Multimedia Mining, Fuzzy based Signature, Cloud storage Server.

## I. INTRODUCTION

It is efficient and cost economical for consumers to use computing resources as much as they need or use services they want from Cloud Computing provider.

In this paper, we propose a method that enables Cloud Computing system to achieve both effectiveness of using the system resource and strength of the security service without trade-off between them.

Especially, Cloud Computing has been recently more spotlighted than other computing services because of its capacity of providing unlimited amount of resources. Moreover, consumers can use the services wherever Internet access is possible, so Cloud Computing is excellent in the aspect of accessibility.

Cloud Computing systems have a lot of resources and private information, therefore they are easily threatened by attackers. Especially, System administrators potentially can become attackers. Therefore, Cloud Computing providers must protect the systems safely against both insiders and outsiders. User authentication Systems are one of the most popular devices for protecting Cloud Computing systems from various types of attack. Because an IDS observes the traffic from each VM and generates alert logs, it can manage Cloud Computing globally.

Another important problem is log management. Cloud Computing systems are used by many people, therefore, they generate huge amount of logs. So, system administrators should decide to which log should be analyzed first. In This paper, We propose Multi-level user authentication system by using fuzzy based approach and log management method based on consumer behaviour for applying IDS effectively to Cloud Computing system.

## II. RELATED WORK

### A. Cloud Computing

Cloud Computing is a service that assigns virtualized resources picked from a large-scale resource pool, which consists of distributed computing resources in a Cloud Computing infra, to each consumer. Cloud Computing is a fused-type computing paradigm which includes Virtualization, Grid Computing, Utility Computing, Server Based Computing(SBC), and Network Computing, rather than a entirely new type of computing technique. It shows the description of each computing technique. Cloud Computing provider can assign large-scale resources to each consumer using these techniques. Cloud computing is a style of computing in which dynamically scalable and oftenly virtualized resources are provided as a service over the Internet.

There is a wide variety of Cloud security validation methods available for applications on any cloud products which meets the requirement of user, supplier or manufacturer and make the product more secure. Increasing security issues and hackers in the network the cloud environment requires strong mining analysis techniques to replace cryptographic key pair maintenance problems. However, over the past service exchange in the cloud computing can be analyzed effectively

### Challenges in Cloud

- Security issues in related to the cloud service
- Reliability (service outage)
- Definition of SLAs (Service Level Agreement)
- Service management (LCM), Monitoring
- Customization

virtual hardware platform for operating guest OSs. Therefore, guest OSs are operated in each VM environment instead of real hardware. A host OS which provides the image of original OS to guest OS, can assign various type of OS other than the type OS of host itself. Figure 1 conceptually describes the organization of hypervisor, host OS, and guest OS.

TABLE 1. USER RISK LEVEL

Technology	Definition
Virtualization	The creation of a virtual version of something, such as an operating system, a server, a storage device or network resources
Grid Computing	The virtualized combination of computing power from multiple domain getting high capacity of computing resource(distributed computing architecture).
Utility Computing	Consumers pay for computing resources as much as they use without buying them.
Server Based Computing (SBC)	Any applications and data exist in server. Clients access the server and utilize them using server's computing power.
Network Computing	It is similar to SBC, but client loads applications and data from server and utilizes them using local computing power.

### B. Importance of Media Mining

Multimedia mining deals with the extraction of implicit knowledge, multimedia data relationships, or other patterns not explicitly stored in multimedia files. Multimedia mining is more than just an extension of data mining, as it is an interdisciplinary endeavor that draws upon expertise in computer vision, multimedia processing, multimedia retrieval, data mining, machine learning, database and artificial intelligence.

The existing methodology for client validation process using cryptographic techniques and, its development and evaluation will be studied. Literature survey will be carried out in the relevant area such as public key and private key process are analyzed. effect on environment and system tools and techniques used. Attributes of different subsystems are to be identified for incorporating in proposed model.

In this regard, this paper proposes a strong user authentication framework for cloud computing, as well as where user legitimacy is strongly verified before enter into the cloud. The proposed framework provides identity management, user authentication, Rule set approach establishment between the users and the cloud server for verification purpose.. A user can change his/her password, whenever demanded. Furthermore, security analysis realizes the feasibility of the proposed framework for cloud computing and achieves efficiency with more security.

Second, in Cloud Computing systems, it is difficult to analyse logs because communication between many system and many consumers generate large amount of logs. Finally, Cloud Computing services are to provide their resource to consumers, therefore effective resource management is greatly desirable. we propose the method for maintaining strength of security while minimizing waste of resources and analysing logs efficiently.

### III. MULTI-LEVEL AUTHORIZATION AND ACCOUNTABILITY SERVICES

We propose the Fuzzy based signature ID's (video, audio inputs, biometrics input status) for implementing effective IDS in Cloud Computing system. Multi-level IDS method leads to effective resource usage by applying differentiated level of security strength to users based on the degree of anomaly. It is true that Cloud Computing is easy to be target of attack.

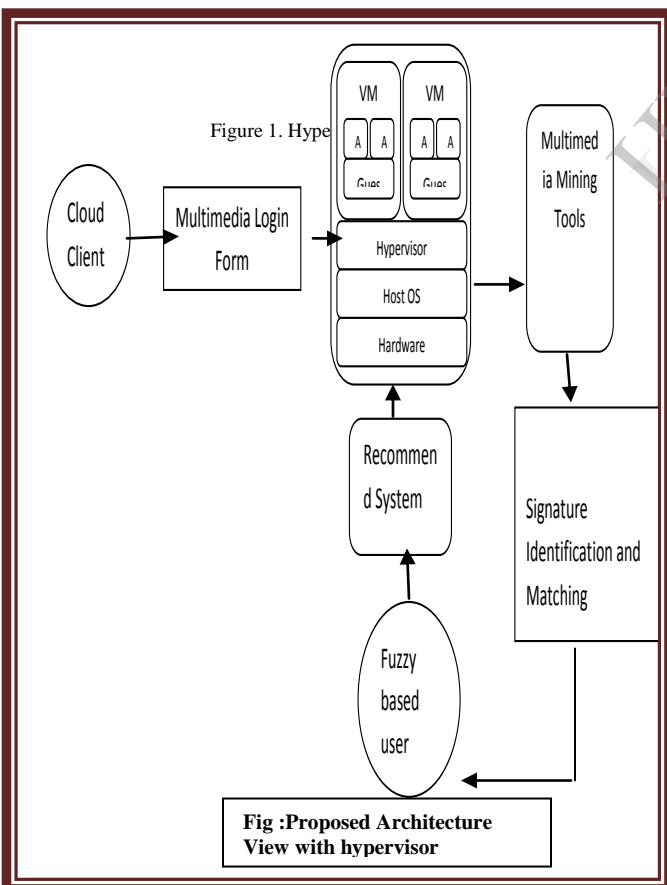
For this reason, it is possible to judge all users and administrators as potential attacker and apply strong security policy to all traffic, but it is not efficient at all. So we propose the method that binds users to different security group in accordance with degree of anomaly, called anomaly level .

#### Cloud Characteristics

- On-demand self-service
- Ubiquitous network access
- Location independent resource pooling
- Rapid elasticity
- Pay per use

After that, AAA chooses suitable IDS which have the security level correspondent to the user's anomaly level. Then AAA requests the host OS, in which the chosen IDS is installed, to assign guest OS image for the user.

Efficient Strategies for Many-task Frequent Pattern Mining in Cloud Computing Environments papers deals on the services which frequently user by the client can be extracted based on the frequent set mining analysis this leaves the key concept for the relation analysis techniques between the different multimedia contents



As figure 1, resource, instruction, and traffic of guest OSs in a hypervisor are mapped to a physical hardware through host OS

Cloud Computing is a set which consists large amount and various types of computing resource, hypervisor, and data. Therefore Cloud Computing providers should own database centers to maintain their resources and data. Cloud Computing service is very attractive to consumers in the aspects of infinite scalability and payment cost in accordance with the amount of computing resource they used, however there also exists the risk that personal and private data are stored in uncontrolled place themselves

Cloud Computing offers wide range of services for the clients who request service from anywhere. The availability and the greater flexibility in cloud most of the organizations are included the cloud services as a part of their major task.

Pay for use service management Client level security issues in the cloud computing became a major challenge in service access process in cloud environment. Day by day number of threats over the network increasing because of the huge demand for the cloud product and service.

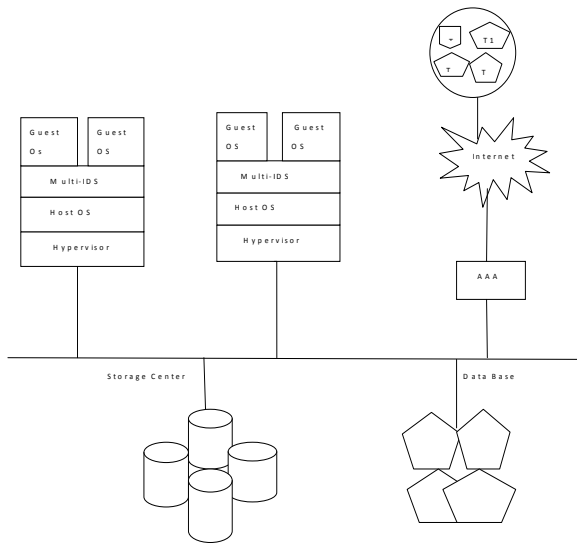


Fig: Proposed Level of Multi-IDS Architecture

It will be used networking System Broadcast more efficient to use it is used Where ever in wired and wireless networking Network always used consequently.

**Merits**

- Large about of extension applied to detect in Cloud computing services.
- Easy Detection and Log Management in Cloud possibility to detect the network in the environment is more.
- Multilevel log management is possible
- Allows to classify the attackers in cloud environment
- Future alerts can be easily made by monitoring the activity.

Each approach has its strengths and weaknesses. A truly effective intrusion detection system will employ both technologies. We discusses the differences in host and network-based intrusion detection techniques to demonstrate how the two can work together to provide additionally effective intrusion detection and protection.

- i) Security issues in Cloud service accessibility
- ii) Difficulties in Server level client validation system
- iii) Insufficient techniques

These attempts may take the form of attacks, as examples, by crackers, malware and/or disgruntled employees. IDS cannot directly detect attacks within properly encrypted traffic. Inefficient techniques to resolve log management in the administrator end .. Identifying efficient mining algorithm for intrusion detection and the process

**Gap in existing Schemes**

It is clear from the literature review that the existing scheme, the server level validations are performed based on the encryption and decryption of the given password. Server can randomly selects private key. The user not allowed selecting their own key for the security. Mistrusted data storage and unauthorized service access are open to the hackers to achieve their goals. In proposed scheme, client set their multi valued login attributes as per their security concerns.

For instance, when a user access Cloud Computing system first time, Multi-level IDS judges anomaly level of user using following matters: the user's IP coverage, vulnerable ports to attack, the number of IDIPW failure, and so on. The most important element for estimating anomaly level is how fatal it is. The rest of judgment criteria are possibility to attack success, possibility to attack occurrence, and so on [1]. The fatal grade of an attack is the degree of impact to systems of the attack, which includes from personal information extortion to system control and destruction. Possibility to attack success is an experimental value which indicates the probability of success for an attack. Possibility to attack occurrence is a value based on the frequency of specific attack. Table 2 shows user risk level.

**TABLE 2 :USER RISK LEVEL**

Likelihood of incident scenario	Very Low	Low	Medium	High	Very High
	Very low				2
	Low		2	3	
Business Impact	Medium	2	3	4	
	Medium	2	3	4	
	High	3	4	5	
	Very High	4	5	6	

Cloud Computing service is very attractive to consumer in the aspects of infinite scalability and payment cost in accordance with the amount of computing resource they used, however There also exists the risk that personal and private data are stored in uncontrolled place themselves. So Cloud Computing providers must protect their Cloud Computing system against all users include administrators.

Multi- level IDS defines the anomaly behaviours by risk level policy such as table 1. The risk levels assign risk points in proportion to risk of anomaly behaviour. The criteria of behaviours for judging that some traffic is anomalous are described

The demand of better quality cloud service and effective client validation techniques leads different levels security analysis on cloud environment. Many Organizations and cloud service vendors and end users need for optimum client validation and minimize risk in the service management. hackers those trying to access the data by proving themselves as a authorized client become challenge for the cloud vendors as well as for organization. and assigned

Fuzzy state	Value Range	Access Credentials
High	Above 90% attribute satisfied	Direct access of service
Medium	Above 70% attribute satisfied	Allow Secondary level verification
Fuzzy level	Above 50% and below 70%	Apply secondary level mining Process and fuzzy logic compute
Low	Below 50% attribute	Denied the access of service

#### IV. COMBINED MULTIMEDIA LOGIN FORM

Achieved by setting the different forms of data as a user login attributes Multimedia Achieved by setting the different forms of data as a user login attributes Multimedia login form setting user credentials over the cloud server Through pixel calculation using cute click(cc) over different places in the images Audio Track Tracer(TT) used to track the play values Normal text conversions techniques can be used to hide the text values. Login form setting user credentials over the cloud server Through pixel calculation using cute click(cc)

#### V. MODELS FOR MULTIMEDIA MINING

In multimedia there is a huge numbe of schemes available. Such as follows :

- Classification Models
- Clustering Models
- Association Rules
- Prediction Models

Data mining requires numerically and statistically intensive computations on large data sets. The increasing memory and processing speed of workstations enables the mining of data sets using current algorithms and techniques t.

#### VI. EVALUATION METHOD

The research focuses on improving the security issues involved in the client and server level user authentication and identification in the cloud environment by using multimedia mining and analysis techniques with Fuzzy based user access credentials .:

1. Efficient client validation through multimedia mining analysis.
2. Fuzzy based user level credentials to access cloud services
3. Reduce the complexity in key exchange and maintenance.
4. Modeling and analysis of process of validation on server and client level.
5. Combined login form validation with different attributes
6. Utilization of strong mining algorithm for classify the users.
7. Different levels of risk analysis in cloud services
8. Performance-evaluation, analysis and modification through experiments on **MULTIMEDIA CONCLUSIONS.**

Trying to provide the efficient user signature identification technique through mining analysis, fuzzy based user authentication module, provide the sufficient security for the Cloud service Access, and also It reduces the complexity involved in the Key exchanges.

#### VIII. REFERENCES

- [1]. Face Fuzzy Vault Vrushali Joshi, Payal Sanghavi IEEE 2011 transactions.
- [2]. A Novel Frequent Pattern Mining Algorithm for Very Large Databases in Cloud Computing Environments Kawuu W. Lin, Pei-Ling Chen 2011 IEEE International Conference on Granular Computing
- [3]. Efficient Strategies for Many-task Frequent Pattern Mining in Cloud Computing Environments, by KawuuW.Lin, Yu-ChinLuo 2010 IEEE
- [4]. Multilevel Database Security Using Information Clouding Sujeet Shenoj , 1993 IEEE Transactions
- [5]. A Monitoring and Audit Logging Architecture for Data Location Compliance in Federated Cloud Infrastructures 2011 IEEE International Parallel & Distributed Processing Symposium
- [6]. A Survey of Large Scale Data Management Approaches in Cloud Environments Sherif Sakr, Anna Liu, Daniel M. Batista, and Mohammad Alomari IEEE Communications Surveys & Tutorials vol.13, 2011
- [7]. Cloud Service Delivery Across Multiple Cloud Platforms Ines Houidi, Marouen Mechtri, Wajdi Louati, Djamel Zeghlache 2011 IEEE International Conference on Services Computing
- [8].The Architecture of Cloud Manufacturing and its key technologies Research Fanghua Ning<sup>1</sup>, Weizong Zhou<sup>1</sup>, Fengying Zhang<sup>2</sup> , Qian Yin<sup>1</sup>, Xiajing Ni<sup>1</sup> *Proceedings of IEEE CCIS2011*
- [9].Multimedia mining S. Kotsiantis<sup>1</sup>, D. Kanellopoulos<sup>2</sup>, P. Pintelas<sup>3</sup> iee transaction 2003