Air journal of Artificial Intelligence

ISSN: 3106-7743 | 3106-7735
Volume 2, Issue 4, 2025

ACCESS CONTROL MODEL FOR CLOUD DATA

Waseema Batool

Lecturer (IT), Department of Information Technology, Shaheed Benazir Bhutto University, Shaheed Benazirabad, Pakistan

waseemabatool@sbbusba.edu.pk

Keywords
Cloud Computing, Deployment Models, Data Security, Consumer Service, Trust Provider

Article History
Received: 10 October 2025
Accepted: 15 December 2025
Published: 31 December 2025

Copyright @Author

Corresponding Author: *
Waseema Batool

Abstract

Cloud computing is an internet-based technology offering shared, flexible infrastructure as a service. It combines hardware and software delivered over the internet, gaining popularity due to its low cost, scalability, and adaptability. This research focuses on securing user data in cloud environments, particularly storage security and preventing unauthorized access through a proposed access control model. Existing models were reviewed, but many failed to meet the security needs of service providers, leaving data vulnerable to attacks. The proposed model addresses these gaps by enhancing data integrity, availability, and confidentiality, encouraging hesitant users to adopt cloud services with a clearer understanding of associated risks.

Air journal of Artificial Intelligence

INTRODUCTION

It's the era of information technology dominating extensively in public. It has turned out to be imperative additionally key part of our life atmosphere it's close to individuals or professionals. Internet help the information technology of its peak. The computers and internet noticeably famous the necessities and manners of utilizing this innovation changed rapidly, especially online direct has been changed drastically since last decade [1]. Clients require versatility with the flexibility of information accessibility anyplace on the world. C1oud computing (CC) has made this solution available for everyone with the flexibility [2]. So clients are utilizing cloud benefits in frame, platform and infrastructure as a service at the same time.

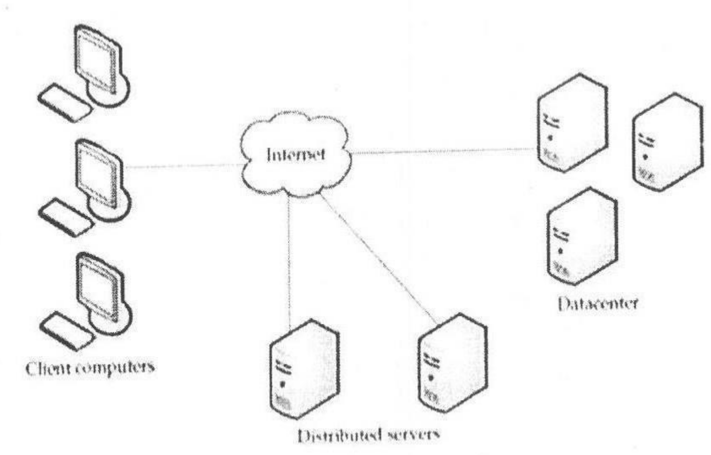
Cloud Computing

Due to the recent innovations and development cloud computing has gained tremendous attention from researchers, individual and organizations. It has encouraged the whole ICT users the way it shifting computer archetype from traditional to new era of cloud computing [3]. Cloud computing facilitates virtualization and internet de1ivery of services, and open source software. The cloud computing design of a cloud answer that the structure of the system, that contains on preface and cloud assets, administrations, middle ware and code parts, geo-location, the ostensibly apparent premises of these and along these lines the connections across them. Several organizations are seeing the advantages of cloud computing since they're ready to expand their atmosphere while not having to put a vast budget on direct server and knowledge center prices [4]

Figure 1.1 Cloud Computing Concept

Cloud comprises of three major parts those are internet, data center and geographically distributed servers. Each of these segments has a different characters and assumes a crucial part in cloud to give services to clients [5].

Figure 1.2 Cloud Components



Deployment Models of Cloud

Infrastructure as a service (IaaS)

Infrastructure as a service (IaaS) is a type of virtualized computing that gives resources over the internet. Additionally, supplies a scope of administrations to go with those parts. These can inc1ude detailed billing, checking, security, load balancing and clustering, additionally capacity flexibility, reinforcement, replication and recuperation. These administrations are increasingly policy, enab1ing IaaS clients to actualize more prominent levels of automation and organization. For instance, a client can actualize strategies to drive stack adjusting to keep up application accessibility and execution [6].

Platform as a service (PaaS)

Platform as a service (PaaS) gives as the required framework to set up application and administration by using the internet. It offers outlining of software evolution, examination, usage and testing. It is the client by giving group participation, database work together and visioning etc. PaaS don't offer simple exchange starting with one specialist organization then onto the next specialist organization. In the event that the specialist organization isn't working appropriately the client data will endure seriously [7].

Software as service (SaaS)

In software as a service (SaaS) approach, the client get assistance by various software applications facilitated on topographically isolated separates by utilizing internet. The client doesn't need to make a big deal about change in software, rather they can utilize the product as it is facilitated on cloud. A wide range of up degrees are given by cloud specialist providers while keeping in the view smooth running of assistance. The customer needs to pay in like manner according to use of the administrations. The product that facilitate the working without perusing to connect with other machine, rank it as best need for client. Client who are not willing in the advancement of their own product require ultra-performing applications they can be assisted from SaaS. The greatest preferred standpoint of SaaS is that it is financially savvy. The organizations don't need to contribute vigorously to purchase their own particular programming or to get the administrations of an engineer group to build up their own product [8]. The organization basically gets the software from the cloud and begin utilizing it. The organization may likewise does not need to keep up colossal staff to run its software. All safety effort would be taken by the hunk specialist organization. SaaS isn't the perfect decision when organizations are having particular software demands. The client needs to pay moving cost while exchanging its administration starting with one cloud supplier then onto the next, along these lines expanding the operational cost. As more open-source programming and minimal effort equipment are accessible in the market, SaaS is confronting intense difficulties [9].

Data Security in Cloud Computing

Cloud is cost effective as it is versatile in nature so capital and operational costs for giving resources less as a result of its on request features. It's pervasive in nature as it can be utilized by numerous machines like desktop, workstation, PDA, advanced cell, tablet PC's,

Google glass etc. It can satisfy requirements of client from various perspectives. The cloud has two closures i.e. back end and the front end. The front end is mentioned as client as it utilizes the services that is given by back end that is chiefly cloud end of the cloud computing [10]. The both two ends are associated through internet. It lies the information security issue when the two ends linked with exchange, delete, update, and share the information. At the point when client needs to control the information in an capacity then security issue emerges from numerous points of view, For instance if a client needs to store information on cloud it might be traded off in center and can be perused and exchanged too at another area also or it has been put away and now it's defenseless against hackers for unapproved access. Client needs to impart information to somebody however it's appeared on wrong stage where it ought to never be, with this security issue emerges for client. Client has put away information however when it recovers a similar it's not the precisely that which has been put away [11]. These are a few situations which may prompt genuine legitimate issues, security violation, break of protection and cybercrimes.

Access Control Model

An access control model (ACM) is a collection of components and techniques which decides the authenticity of client activities by the legitimate clients in light of pre-designed access consent and benefits depicted in the entrance security policy [12]. The fundamental goal of any access control model is to limit a client precisely where he has the capacity to perform normal activities and secure data from unapproved access [13]. There is a tremendous assortment of strategies, models, technologies and administrative capabilities used to design and propose access control model. Therefore, each access control model has its own characteristics, strategies and capacities, which get from either an arrangement or an arrangement of approaches [15].

Traditional Access Control Model

A background about traditional access control models and why they can't be deployed in the cloud are being exhibited. It also explains fundamental requirement for cloud based access control models and existing proposed solutions. Access control model is utilized to control and reduce the unauthorized access to stored data [14]. There are numerous control models available for this reason, however most importantly it should be resolved that why they can't be utilized in cloud?

There are many reasons for that why traditional models cannot be used in cloud, some noticeable causes are enlisted here.

- Heterogeneity, omnipresent and assortment of administrations [17]
- Assorted variety of assortment of access control policies and different access control interfaces can cause despicable interoperability [16].
- Managing a substantial number of clients, distinctive grouping, high unique execution, versatility highlights and changes in high recurrence is a piece of cloud [19]
- Cloud is very complex and sophisticated because of the dynamic in nature of clouds resources [18].
- Diverse access authorizations to same cloud users and giving him ability to utilize multiple services concerning validation and login time.
- Entitles those are cloud based are likely to occupy in assorted trust domain and might be located in various nations that have different rules and regulations. Along these lines, they may not believe each different according to requirement [20].
- Conventional access control models in cloud should experience the lack of flexibility in scalability and attribute management.

Mandatory Access Control (MAC) Model

A central authority that giving instructions for access choices to a subject that demand access to items or data in objects. With a specific end goal to secure access to objects and the data that streams between objects, MAC doles out an entrance class to each subject and protest in system. An entrance class is a security level that is utilized to secure the flow of data between subjects and objects with strength relationship. Question groupings are security labels that are utilized to arrange objects base on the affectability of data they have. Subject clearances are security levels used to reflect the reliability or rules of subjects. The early formula and most well relationships were proposed by Bell and LaPadula in 2013. This model is also called multilevel security and uses only two properties no-write-down and no-read- up properties. The Bel1-LaPadula model has focused on securing and controlling information flow, however ensuring the confidentially in a framework isn't the main objective in securing data. Thus, Biba (2007) utilized similar standards used by Bell and LaPadula model to propose a model for ensuring the objects integrity.

Although obligatory access disp1ay gives insurance against data stream and indirect data leakages, it doesn't ensure complete mystery of the data either in the Bell-LaPadula model the Biba model both are vulnerable. For instance, any ungrouped subjects can compose into top mystery objects, and cloud make improper alterations to objects and violate their virtue (Ray and Kumar, 2006). Indeed, this model is extremely costly and difficult to deploy and does not assist partition of obligations, minimum privileges and delegation or legacy principles. Dynamic actuation of access rights for specific functions isn't upheld in this model. Besides, it doesn't bolster time and location constraint. It needs an exact administration system for dealing framework segments that are either outside or inside of model. Procedures and libraries are examine as trusted parts, however in some cases they have to break MAC standards (Jiang et al., 2004). Hence, they may need to resist outside of the MAC show. Besides, finished group objects or subjects can occur in it.

The BLP still does not manage the creation or demolition of objects or subjects. Security labels are not flexible and advantageous for tasks execution. It requires a focal expert to figure out what data should be made accessible and by whom. For instance, a manager should need to get data about staff, however he/she should not have the capacity to have full access to part document she/she could get to and reveal delicate data of part, for example, financial balance points of interest. As cloud computing will utilize current web applications to deliver services to clients, MAC needs to manage an absence of refined semantic models, which represent to and impart benefits and limitations that are given through access control strategies [16].

Discretionary Access Control (DAC) Model

The Discretionary Access Control (DAC) model, allows the owner of object the ability to limit access to their items, or data in the items in view of client identification or membership in certain gathering. DAC model is generally less secure than obligatory access control model i.e. DAC is less secure as compared to MAC, so it is utilized as a part of situations that don't require an abnormal state of assurance. Thus it is the most utilized model in commercial working frameworks, for example, UNIX and Windows based stages since it is more f1exible and less demanding to be used than different models. There are two approaches to execute a discretionary access contro1 (DAC) model, this can be accomplished through character based access control or by methods for an access control network or abilities [17].

The DAC relies upon enabling proprietors of the objects to control access approval to objects, it has numerous disadvantages when it is used in cloud. There is no component or strategy to encourage the administration of dishonorable rights, which proprietors of object can provide for clients. At times utilizes are required to use benefits that reveal data about items to outsiders. A client cab just read a record in an organization, and after that he/she can duplicate document substance to another record to pass it to another client. The DAC have not the capacity to control data stream or manage Trojan steeds that can acquire get to consents On the opposite side, a client may pass their rights to another client, and that can abuse the trustworthiness and secretly of objects. At last, it can't be sufficiently scaled for cloud computing[11]

Attribute Based Access Control (ABAC) Model

The Attribute Based Access Control (ABAC) model depends on an arrangement of characteristics related with a requester to be access to settle on construct access choices. There are numerous approaches to characterize or utilize qualities in this model. A characteristic can be a client's work begin date, an area of a client, a part of a client or every one of them. Attributes could possibly be identified with each other. Subsequent to characterizing traits that are utilized as a part of the framework, each characteristic is considered as a discrete utility, and estimations of all qualities are analyzed against set of desirability by an approach or basic leadership point to deny or give access (Yuan and Tong, 2005).

These sorts of models are a1so called either Policy Based Access Control (PBAC) or C1aims Based Access Control (CBAC). However, a subject does not need to be known ahead of time to the framework, it simply needs to confirm itself to the framework at that point give its characteristic simply. Thus, achieving an understanding about what sort of traits are utilized, and what number of characteristics are considering for settling on access decision is a complex task in cloud computing. This model has not been exhibited and executed for surely understood working frameworks. Proposing a security strategy that can work precisely with this kind of access control model is essential, in light of the fact that the security approach is in charge of choosing the essential credits that are utilized to settle on get to choices (Hu et al., 2015).

Risk Based Access Control (RBAC) Model

RBAC model was proposed to manage multinational companies that face different sorts of policies and regulations (Atlam et al., 2017). This model endeavor to utilize various types of risk levels with environmental conditions and utilize the guideline of "operational need" keeping in mind the end goal to access decisions. In quantified risk adaptive access contro1 (QRAAC), risk is calculated as risk ¼ V*P, where V is the data va1ue that reflects the affectability level of the asset, and P is the probaility of unapproved disclosure, which reflects the responsibility of the client. The security policy in this model is dynamic; it is changed by an assortment of risk levels expressed in the security policy.

This model is difficult to establish in cloud due to the measure of analysis required and number of frameworks to be converged to process risk levels. It needs aptitude level that can manage this model. Finally, security policies and environmental conditions should be standardized as they play a crucial role on deployed access decisions (Celikel et al., 2009).

Requirements for Cloud Based Access Control Model

Computational complexity of access control rules is still a hard undertaking for all access control models that is capable of implementing any access control policy. The computational complexity can influence the proficiency and quality of service as it may delay making on choice process and rejected different parts inside the system (Younis et al., 2014). In cloud computing, each service provider has its own specialty and ability to give services to all its users. Hence, depending on user's requests and demands, diverse specialist organizations frequently collaborate by taking part their assets. In any case, the decent variety of access control arrangements and interfaces can cause irregular interoperability, which oppose any mix or development starting with one service provider to another service provider.

Proposed access control models for cloud must be versatile regarding number of clients, policies and rules assessment and implementation focuses. Moreover, scalability should also be considered as operational, support and administration costs. These cost should not be incremented when the quantity of access framework segments (clients, applications) increase. To coming to on an assertion about what sort of characteristics should be utilized and number of traits should be considered for settling access decision is complex task (Shen and Hong, 2006).

Cloud computing is a dynamic and scalable environment, which also support remote access to its sources. So any proposed access control model for this condition needs to depict these characteristics and need to meet the focused on customers. Cloud computing has initiated another trust relation among clients and cloud suppliers. Trust relationship in cloud based access control frameworks needs to get more consideration as far as characterizing the trusted conduct for either client or service providers, and assessing those practices keeping in order to be considered in the further access determination.

One of the primary issues with access control systems is to confirmation. Cloud based framework needs reliable component for demonstrating client's personalities and validating them. Besides, time of validation and login should be considered as it might be effect the execution of the systems and the following steps like approval. A solid client validation instrument for cloud computing with numerous security components, for example, to mutual authenticate, character administration, coordinated with approval systems implemented by the upper layers and lower layers, session key assertion between the clients and the cloud server is necessary.

MATERIALS AND METHODS

Access Control Model

An access control system is an accumulation of parts and strategies that decide the right admission to activities by authorized users in view of pre-designed access consents and benefits laid out in the access security arrangement (Anderson, 2011). The principal objective of any access control system is confining a client to precisely where he/she should have the capacity to do his obligation and shield data from unapproved access. There is a wide assortment of strategies, models, advances and regulatory parts used to propose and configuration access control system. Along each access control system has its own properties, strategies and capacities, those are acquired from either a policy or set of policies.

Architecture of Proposed Access Control Model for Cloud

Based on the evaluation of research carried out in the area, the architecture for access control model in cloud computing conditions are shown in fig. 3.1.

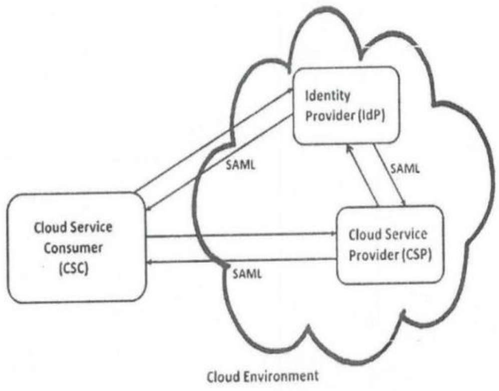


Figure 3.1 Architecture of Access Control Model for Cloud

Cloud Service Consumer (CSC)

Cloud Service Consumer (CSC) set forward the demand for the required resources or administrations facilitated by the cloud service providers. Appropriate verification of the cloud service consumer is important to guarantee that unapproved clients can't access the administrations from the cloud service providers. The cloud clients may buy in to an assortment of administrations relying upon their hierarchical structure and prerequisites and regularly they are charged in light of an as pay-per-utilize model.
The fundamental practical modules/parts of the Cloud Service Consumer (CSC) segment are:

Trust Provider (TP)

Cloud computing includes multi-domain situations and the trust is an imperative part which should be worked between the specialist organization and service consumers. The shared trust between the service provider and service consumers furthermore between the providers of different services and the identity providers has center significance particularly on account of distributed computing like cloud computing or other computing services. The trust supplier module on the purchaser side monitors the trust estimation of specialist organizations and gives a refreshed confide in an incentive to the service customers. In the cloud computing situation, the trust is dynamic as a similar element could have various trust in an incentive at various purposes of time. Trust Provider ascertains the trust value in estimation of the service providers, considering different parameters, like the past conduct and the historical backdrop of past exchanges with a similar service provider. This module likewise considers the trust esteems or data of the substance from other Trusted Third Parties (TTP).

Access Control Request Handler (A.C.R.H)

This module manages the access demands when the cloud service consumer tries to access the services facilitated by the service providers. It additionally then set up contact with the Identity Provider Selector (IdPS) module so the Identity Provider (IdP) could be chosen to meet the character administration necessities for the correspondence between the elements.

Identity Provider Selector (IdPS)

The service consumer must need to choose an appropriate Identity Provider (IdP) so as to get the recognizable identification token, with the goal that it can be utilized to access the different administrations facilitated by the Cloud Service Providers (CSP). This choice of the IdP among the accessible ones depends on parameters like the required service write for instance the subtle elements of the supplier and confirmation, its approval mechanism and the security and privacy issues of the cloud users in uncovering their character tribute or Personally Identifiable Information (PII).

Workflow Model for Access Control in Cloud Environments

U898The model of workflows for the access control in cloud computing situations is shown in the fig. The distinctive steps performed by the CSCs, CSPs and the IdPs amid the contact are given below:

- A cloud service consumer i.e. CSC needs to access and utilize the service hosted by the cloud service provider and initiate the access request.
- In the initial step dynamic trust estimation of the CSP is figured by the CSC which depends on the
past transaction performed and the data gave by the trusted third parties (TTP).
- The authentication request for is sent to cloud service consumer (CSC) by the cloud service provider (CSP).
- The CSC communicates with the CSP to choose the reasonable IdP in light of the sort of service request and the security preferences. It is expected that the cloud service provider (CSP) chooses the IdPs in which is accessible in its

trusted area depending on the confide estimations of various IdPs, and furthermore in view of the past history of correspondence and the trust as well as reputation value gave by other trusted entities.

- The CSC at that point speaks with the selected IdP to get the security tokens (e.g. SAML affirmations).
- CSP verifies and run the authentication procedure of the CSC by interfacing with the IdP.

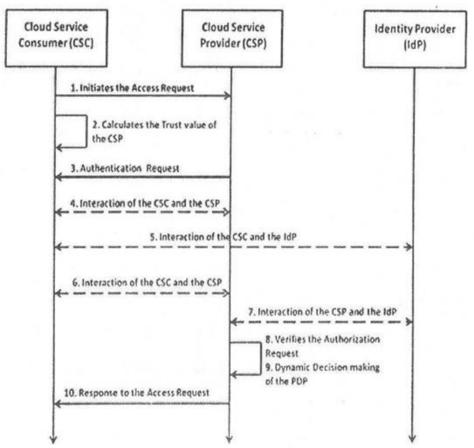

Cloud Service Consumer (CSC)
Cloud Service Provider (CSP)
Identity Provider (IdP)
1. Initiates the Access Request
2. Calculates the Trust value of the CSP
3. Authentication Request
4. Interaction of the CSC and the CSP
5. Interaction of the CSC and the IdP
6. Interaction of the CSC and the CSP
7. Interaction of the CSP and the IdP
8. Verifies the Authorization Request
9. Dynamic Decision making of the PDP
10. Response to the Access Request

Figure 3.2 Work Flow Model for Cloud

Implementing Private Cloud

To set up a trustable third party in role of EaaS, we should complete three stages: initially, implementing private cloud; second, giving encryption algorithm; and, last, multi-threading attributes in view of various virtual memory cores. To have an EaaS, the initial step is implement private cloud. A private cloud enables the clients to have more control over the infrastructure and security because of more confinement on the network and users access. Besides, in a private-basedcloud, the prepared information inside the association are secured against lawful issues and are not influenced by organize data transmission's confinements amid processing time. They don't get benefits by the vast number of computing resources, as public cloud may offer; they are still sufficiently large enough to appreciate the upsides of cloud computing. In the private cloud, it is conceivable to distribute the clients' workloads on various resources relying upon enterprises size.

Air journal of Artificial Intelligence

From a different view, in a private cloud, there are a group of clients that offer the virtual instances, while they are checked always in correlation with heterogeneous clients in the public cloud. Besides, accessibility of services might be ensured in a private cloud, which has been intended for the particular reason for the venture. For actualizing a private cloud, we require using a system for outlining and executing a laaS (Infrastructure as a service). Some of the well- known systems for the reason for existing are Open Nebula, Nimbus, OpenStack and Eucalyptus.

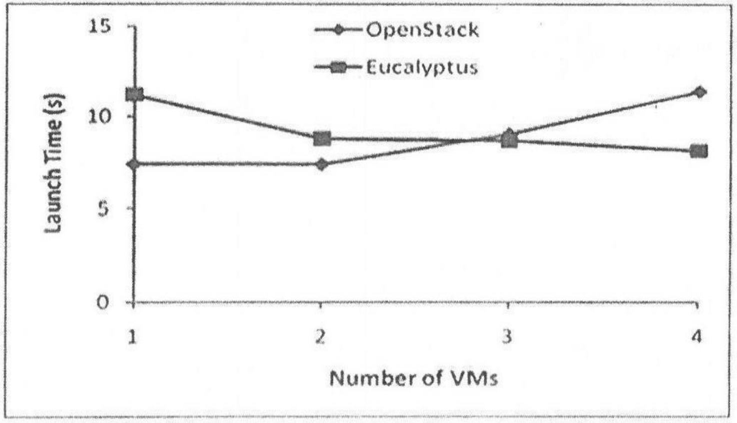


Figure 3.3 VM Parallel Launch Time

Cloud Security Framework

The security layer is based over the Open Nebula system, an open-source cloud computing toolbox for overseeing heterogeneous distributed data centers infrastructures. The system coordinates the arrangement and administration of Virtual Machines, and is overseen by means of a CLI, a web service and language particular bindings (Ruby, Java and Python).

The Open Nebula cloud computing stage offers a few application programming interfaces: XML-RPC API, Ruby Open Nebula Cloud API, Java Open Nebula Cloud API, Ruby Open Nebula Zone API, Ruby Statistics API and Sunstone Plug-ins API. The proposed security layer utilizes the Open Nebula Cloud API (OCA) and verifiably the XML-RPC API to access the usefulness of the cloud system over the Open Nebula Cloud API.

Air journal of Artificial Intelligence

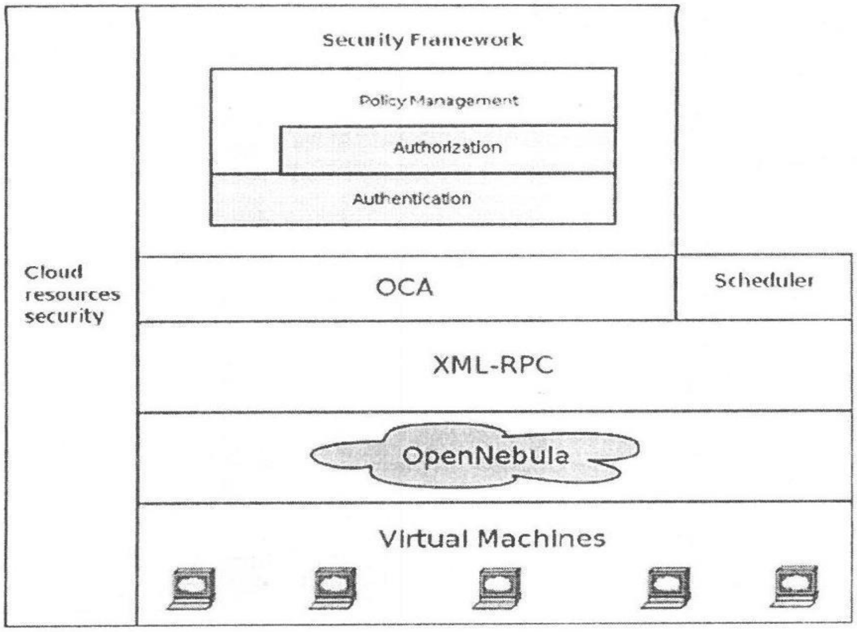


Figure 3.4 Architecture of Cloud Security Framework

Open Nebula commands are encapsulated in HTTPS messages that are routed to the server running on the frontend. The client is confirmed if the handshake protocol phase is effective. After the server identifies the sender, his authorizations are evaluated. If this step is successful, at that point the demand is signed so as to permit the security approach motor to track malicious requests. After all these steps are validated, the demand is de-capsulated and the relevant info is separated. Utilizing the Open Nebula Cloud API (OCA), a new request is issued, this time coordinated to the Open Nebula core. The proposed security system in this way goes about as an extra layer over Open Nebula, through which all requests must pass. The whole arrangement management module empowers the framework to naturally take measures against security assaults and to bring down the helplessness level of the cloud environment. The proposed system depends on two parts which keep running toward the front end. A logger and an analyzer. The collaboration between them is outlined in Figure 3.5.

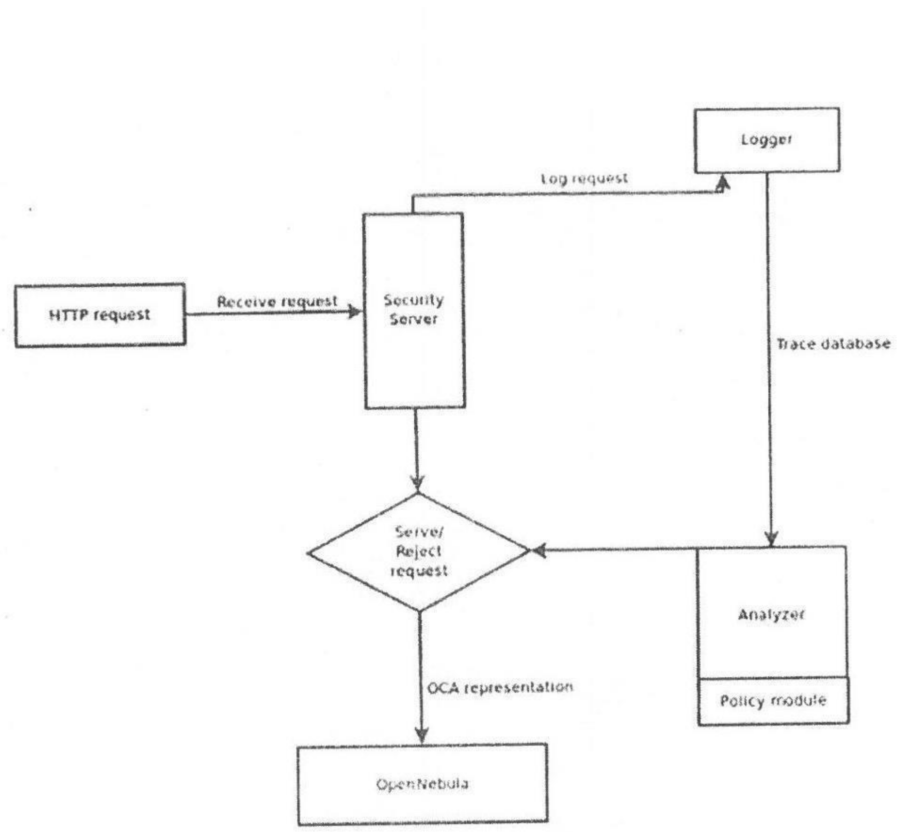


Figure 3.5 Privacy Policy Mechanism

Each of the components runs freely, so the front-end keeps up availability during the analysis procedure. In this way, all requests coming from the clients are productively served. The logger module gathers client action data. The information is utilized both by the security server with a specific end goal to choose whether the demand is sent to the Open Nebula core or dropped, yet in addition by the analyzer, as an policy matcher. The analyzer contains the core of the policy management engine. This module covers the whole life cycle of a security policy, distinguishing client activity which coordinates the states of an arrangement and taking the actions specified by the policy. The contribution for this module is represented by the traces identified by the logger.

RESULTS AND DISCUSSION

Evaluation of Proposed Access Control Model

The proposed model has been named access control and user authentication (ACUA) model that contains appropriate tools for validating user legal identities and procuring their access control benefits for the resources according to the role information. In the proposed model, the concepts of agents, multi-clouds and Software-as-a-Service (SaaS) have been considered to set up a secure algorithm amid client confirmation and access control processes. According to the brief introduction of the proposed model in figure, this model uses the ideas of multi-clouds for planning a cloud-based software-as-a-service and managing accesses and user authentication processes to increase the reliability of public of private cloud computing environments.

The proposed model one client-based agent and four cloud-based agents to set up a secure algorithm during procedures, services and communications. The primary objective of these operators is to expand the rate of intelligence and reliability during cloud computing communications. Accordingly, every agent has isolate execution and has been associated with different agents with ACUA software-as-a-service application. The responsibilities of each agent and ACUA have been portrayed in following tasks.

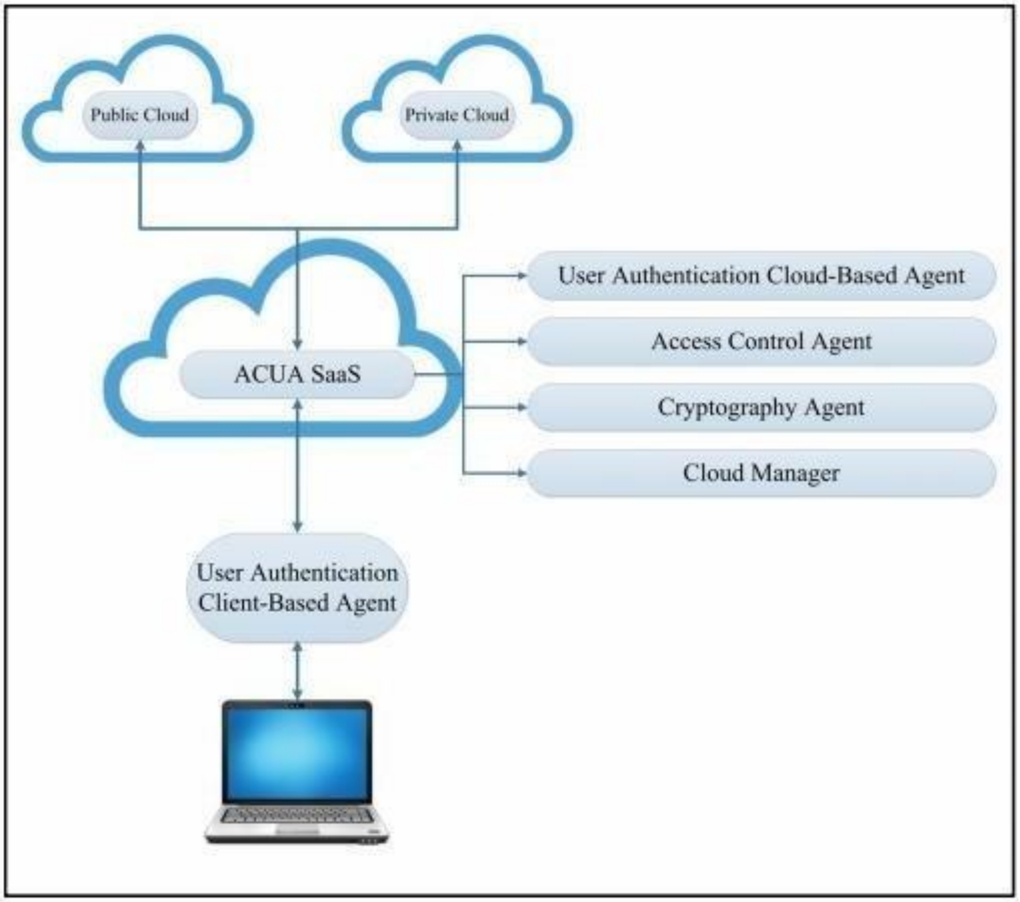


Figure 4.1 Proposed Access Control Model in a View

Client-Based User Authentication (CBUA)

In current user authentication models, the reliance of this procedure on cloud server systems is one of the the most difficult issue. As needs be, client-based user authentication agent is an application that deals with the character of clients before accessing to the cloud condition. For this intention, user's authorized devices should be registered by installing CBUA. The accompanying figure demonstrates the procedure of device registration in ACUA.

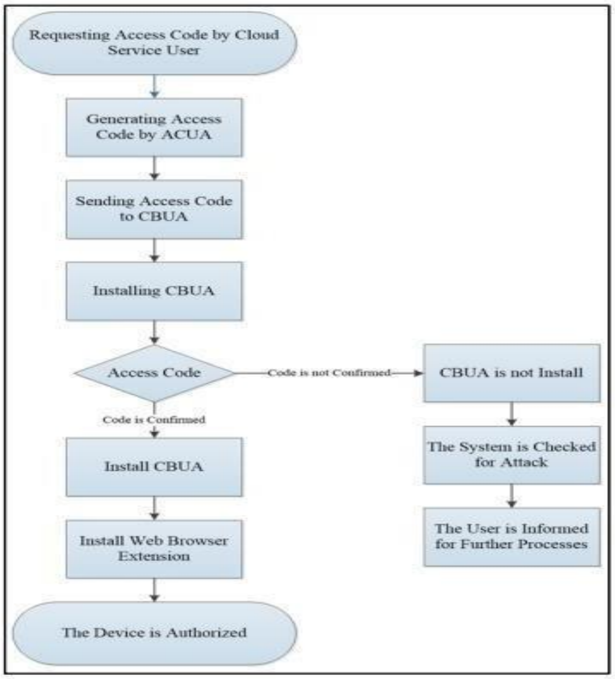

Requesting Access Code by Cloud Service User
Generating Access Code by ACUA
Sending Access Code to CBUA
Installing CBUA
Access Code
Code is not Confirmed
CBUA is not Install
Code is Confirmed
Install CBUA
The System is Checked for Attack
Install Web Browser Extension
The User is Informed for Further Processes
The Device is Authorized

Figure 4.2 Process of Device Registration

The device should be enrolled at ACUA and by enlisting an access code that will be sent to the device. The access code will be entered during the installation process and will be checked with ACUA database. After confirmation the device will be enlisted by the MAC ID and the application will be installed. Besides, the customer based application should be should install an extension on the web browser of the registered device for further processes. After registering a device by installing CBUA and affirming it, clients can access to their cloud server all the more safely. The accompanying algorithm demonstrates the execution of CBUA agent in details.

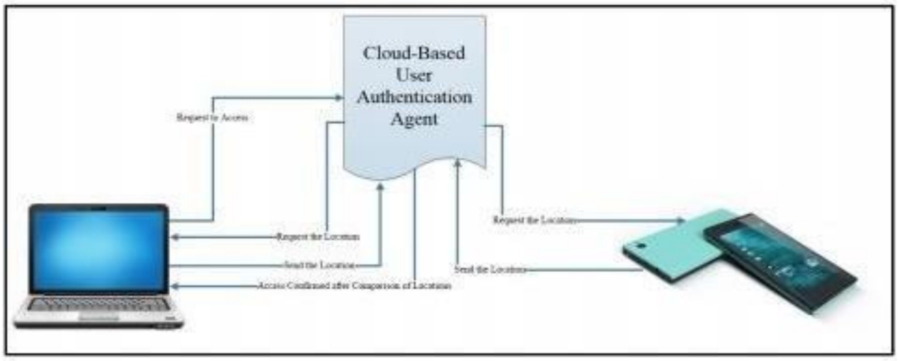


Figure 4.3 Performance of CBUA Agent

Access Control Agent

According to the analysis of performed researches managing access controls is one of the most crucial issues that decrease the reliability of cloud computing environments. Because of this, access control agent is recommended in the proposed model to increase the efficiency of managing accesses in cloud-based situations. In access control agent the reliance of managing accesses to the information will be increase by a unique data header. This implies a special data header will be characterized for managing accesses and increasing the rate of trust in cloud servers. In the proposed access control model, data will be separated to a few sections and each part will be stored on different cloud servers. In like manner, divided data will be joined at ACUA cloud server for utilizing by clients or sharers. The following steps demonstrate the performance of access control agent in details.

Upload Process

a. Data is uploaded to ACUA by the clients.

b. In ACUA, data will be isolated to a few sections and each part has an special header.

c. Separated parts will be sent to cloud storages for storing processes.

Download Process

a. Divided data will have received by ACUA from cloud storages after requesting from user.

b. Divided data will be joined in ACUA and will be sent to the user device after removing headers.

For dividing and joining processes, data header should be utilized for identification and access control. In other words, dividing data to a few sections and using data header will increase the reliability of access control processes. The accompanying figure 4.6 shows the data header in proposed model.

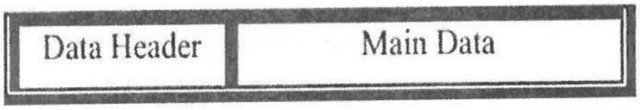
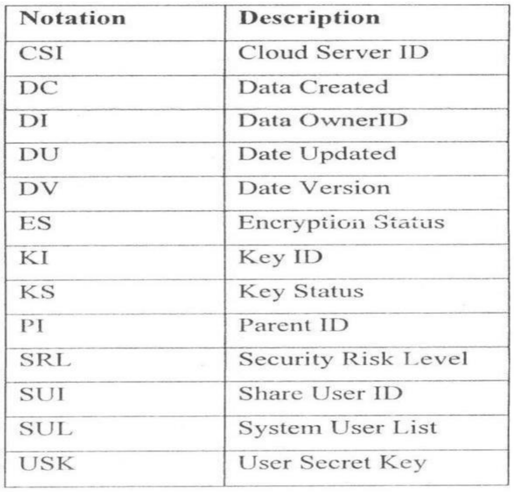


Figure 4.4 Divided Data Structure

By using data header, data will be secured after losing one of the servers as a result of an unpredictable event or attack. However, the possibility of an illegal authorization will be decrease significantly. The accompanying table shows the characterized and proposed notation of of using in data header.



Notation	Description
CSI	Cloud Server ID
DC	Data Created
DI	Data OwnerID
DU	Date Updated
DV	Date Version
ES	Encryption Status
KI	Key ID
KS	Key Status
PI	Parent ID
SRL	Security Risk Level
SUI	Share User ID
SUL	System User List
USK	User Secret Key

As indicated by table 4.1, managing accesses will be more secure and the rate of trust will be more increased by dividing data and utilizing data header in cloud computing environments. Furthermore, to establish more security in cloud servers to give a protected place for for storing divided data, a cryptography algorithm is by all accounts basic. Having stated, cryptography agent will be described and presented in next undertaking.

Cryptography Agent

Using cryptography algorithms are the most popular solution for establishing security in cloud computing conditions. There are numerous asymmetric keys and symmetric keys cryptography strategies with different specifications. Cryptography agent utilize both asymmetric keys and symmetric keys models in different circumstances.

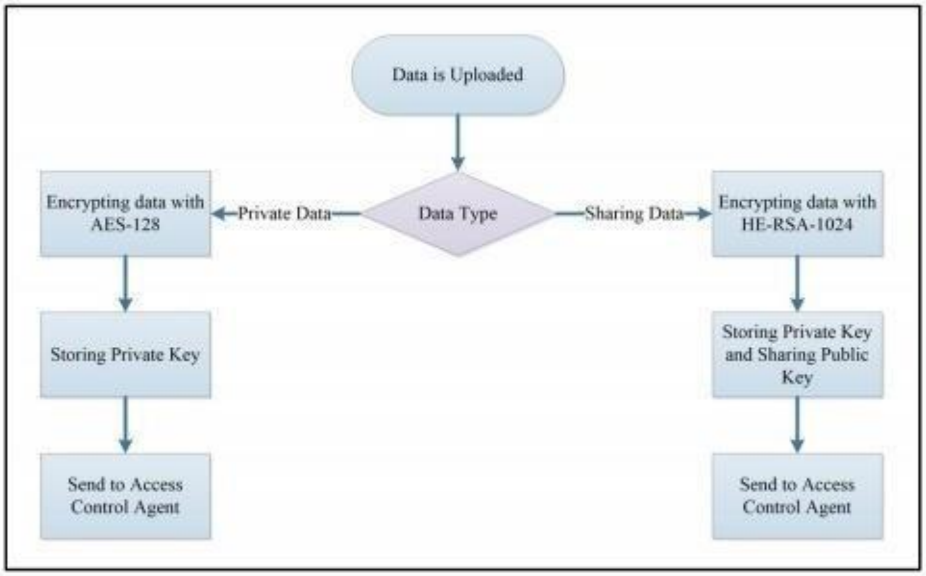

Data is Uploaded
Data Type
Private Data
Sharing Data
Encrypting data with AES-128
Encrypting data with HE-RSA-1024
Storing Private Key
Storing Private Key and Sharing Public Key
Send to Access Control Agent
Send to Access Control Agent

Figure 4.5 Cryptography Agent Performance

Cloud Manager

The fast development of using cloud services is an unquestionable fact that has occurred in the recent years. Accordingly, clients and enterprises buy in different cloud services for various purposes. These cloud servers can be private clouds or public clouds that are utilized for various purposes. According to the analysis process of current models, managing data diminishing the rate of proficiency in cloud computing situations. In like manner, cloud manager agent has been design and presented in ACUA for managing with the relations and communications between public and private clouds. The followig diagram demonstrates the execution of this cloud- based management application.

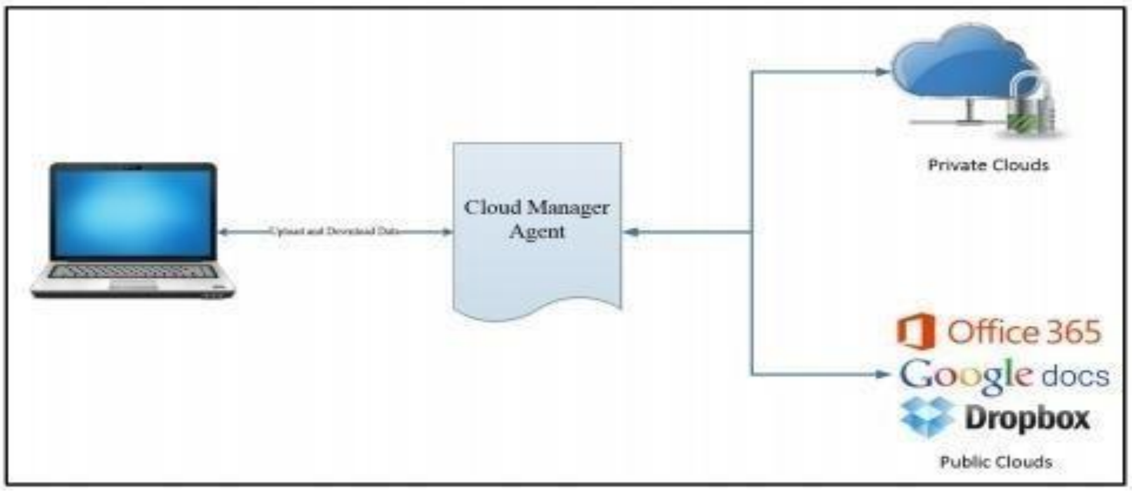


Figure 4.6 Cloud Manager Performance

Evaluation of Proposed Model

The proposed model has been evaluated by four parameters i.e. performance, compatibility, security and power of intelligence.

Performance

The brief performance of proposed model has been shown in following table.

Main Task	Sub Task	Expectation
User Authentication	Client-Based User Authentication	Reliable Authorization in client side Manage client-based user authenticatio process
User Authentication	Client-Based User Authentication	Use confirmation code for accessing fro unauthorized device. Manage cloud-base u ser authentication process.
User Authentication	Region Detection	Use location service for user authentication process.
Access Control	Access Control Agent	Dividing data to several parts and storin in various servers. Put data header wit defined notation for managing accesses.

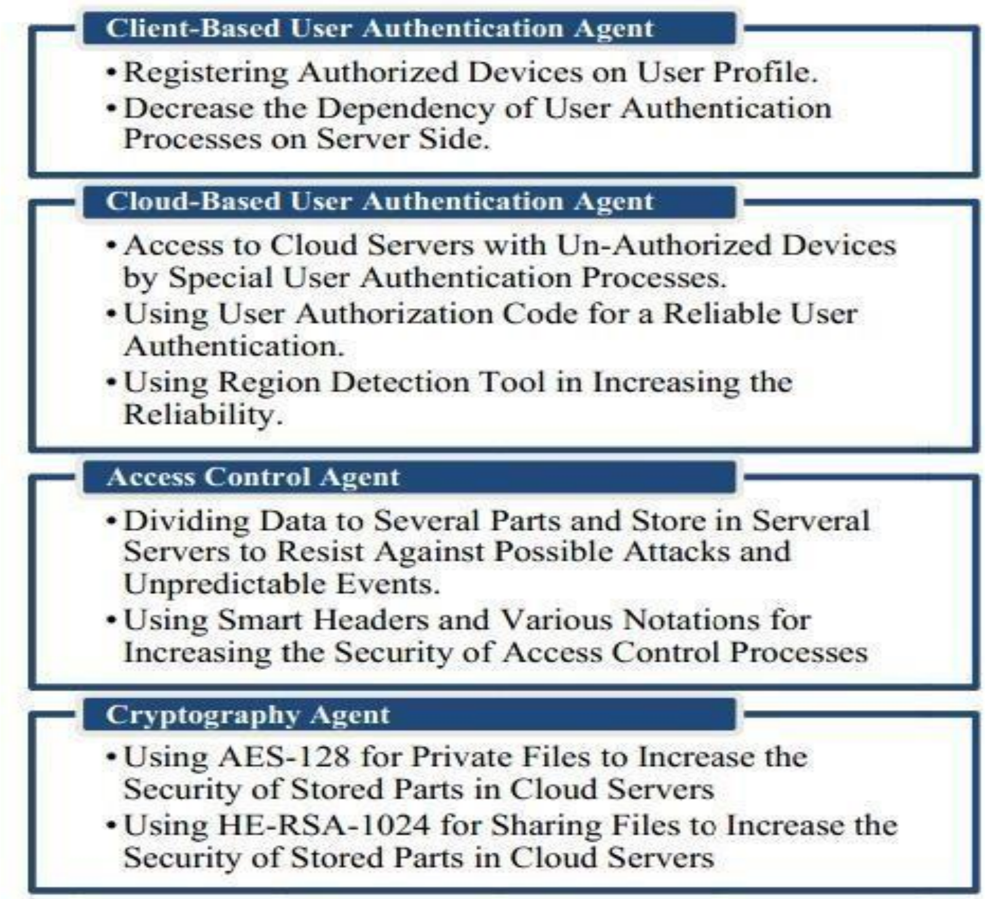
Air journal of Artificial Intelligence

Access Control	Cryptography Agent	Use Asymmetric key cryptography for sharing files. Use Symmetric key cryptography private files.
Access Control	Cloud Manager	Managing data from public cloud servers and private cloud servers.

Table 4.2 Brief Performance of Proposed Model Security

The proposed access control model and user authentication model increase the rate of security and reliability in cloud computing environment considerably. The following diagram shows the security evaluation of the proposed model.

Figure 4.7 Security Evaluation of Proposed Model



Client-Based User Authentication Agent

- Registering Authorized Devices on User Profile.
- Decrease the Dependency of User Authentication Processes on Server Side.

Cloud-Based User Authentication Agent

- Access to Cloud Servers with Un-Authorized Devices by Special User Authentication Processes.
- Using User Authorization Code for a Reliable User Authentication.
- Using Region Detection Tool in Increasing the Reliability.

Access Control Agent

- Dividing Data to Several Parts and Store in Serveral Servers to Resist Against Possible Attacks and Unpredictable Events.
- Using Smart Headers and Various Notations for Increasing the Security of Access Control Processes

Cryptography Agent

- Using AES-128 for Private Files to Increase the Security of Stored Parts in Cloud Servers
- Using HE-RSA-1024 for Sharing Files to Increase the Security of Stored Parts in Cloud Servers

As shown in the fig. 4.9 considered specifications of the proposed model will increase the rate of security in cloud computing environments during accesses, downloads, uploads, user authentications and transmissions. This increase will raise the reliability of cloud-based services Compatibility

There are two main parts of proposed model client based agents and cloud based agent.

Client Based Agent

There is one client based application that should be given in different versions according to different platforms to be compatible in all circumstances. As indicated by the nature of this client-based agent, there isn't any issue to create distinctive versions of this application.

Cloud Based Agents

As we described there are four cloud based agents in the software-as-a-se service application. These agents are totally compatible with different devices and platforms as a result of the structure of applications that depend on cloud computing concepts.

Power of Intelligence

The proposed model uses several intelligence tools to increase the efficiency and the rate of trust in cloud computing environments.

Region Detection

This tool can measure the distance between location of user and location of unauthorized device to have a more reliable authentication process.

Access Control Agent

Using smart data header during access control processes will help to handle expected errors better and more significant. The notations of data headers will save log data for the efficiency of error identification and error handling during access control processes.

Limitations

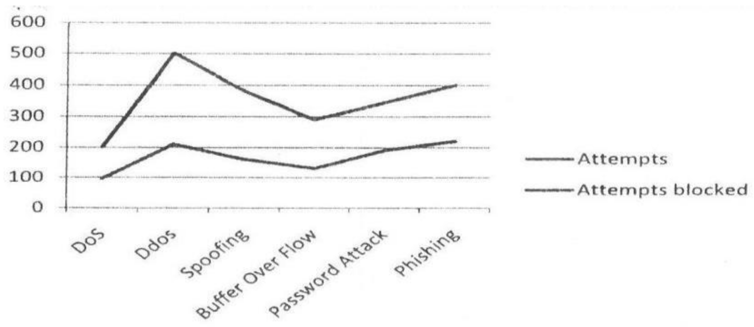
As each model, the presented model has few limitations during development, execution, usage, maintenance etc. The primary limitation of the proposed model is the similarity of cloud manager agent with different public and private cloud servers. This implies communication between various cloud servers with different structures is a challenging issue during the advancement of the proposed model. However, the time consuming during data in several parts and joining them to the fundamental parts in access control agent is another limitation for the proposed model. Likewise, changing the cryptography algorithm after changing the type of file is a challenging issue in cryptography agent. For example, when a private data that was encrypted by AES-128 is changed to a shared data the data should be decrypted and re-encrypted by HE- RSA 1024.

Air journal of Artificial Intelligence

Results after Implementation of Proposed Security Model

Numerous attempts were made after the proposed security model was implemented however among them number of attempts were blocked as shown in figure 4.10.

Figure 4.8 Attacks Attempted and Blocked



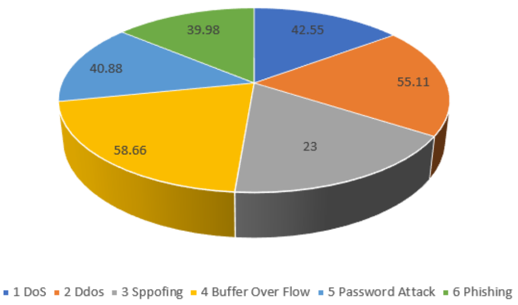


Figure 4.9 Percentage of Blocked Attacks

After the implementation of proposed model, the percentage of attacks blocked is specified as above. So, on the average the execution of this model is 47.75% is superior to existing models.

Conclusion

The purpose behind this research was to focus on user's data security in cloud computing i.e. data storage security issues and how to minimize unauthorized access to data by proposing access control model, at that point available solutions will be presented and access control model will be recommended. Cloud computing can be referred as technology based on internet, having shared scalable infrastructure that can be used as service by users. Compositely cloud computing is software and hardware delivered over internet as a service. Confirmation of the identity and the access privileges of the service consumers is most extreme imperative in cloud computing or services computing, before they are allowed to access the various resources or services hosted by the Service Providers. With the tremendous increase in the number of distributed applications, the issue of distributed access control has become an important research topic for both the academic and the industry.

Numerous access models are available those models do not fulfill the security requirements according to service providers and cloud is always under attacks of hackers and data's integrity, accessibility and privacy is compromised. This research will present a model keeping in view the requirements of service providers and will enhance the data security in terms of integrity, accessibility and privacy. It will help the reluctant users to easily decide to shift on cloud while understanding the risks associated with cloud computing. According to the identified limitations of the proposed model, it has been recommended to provide appropriate e-learn media files to teach users how to handle their privacy and access control processes more efficient and more secure. Moreover, it has been recommended to design an automatic re-encryption algorithm for encrypting data that their type has been changed in cryptography agent.

Air journal of Artificial Intelligence

REFERENCES

[1] A. Albugmi, M. O. Alassafi, R. Walters, and G. Wills, "Data security in cloud computing," in *Proc. Fifth Int. Conf. Future Generation Commun. Technol. (FGCT)*, Aug. 2016, pp. 55–59.

[2] H. F. Atlam, A. Alenezi, R. J. Walters, G. B. Wills, and J. Daniel, "Developing an adaptive risk-based access control model for the Internet of Things," in *Proc. IEEE Int. Conf. Internet of Things (iThings), IEEE Green Computing and Communications (GreenCom), IEEE Cyber, Physical and Social Computing (CPSCom), and IEEE Smart Data (SmartData)*, Jun. 2017, pp. 655–661.

[3] S. Bhardwaj, L. Jain, and S. Jain, "An approach for investigating perspective of cloud software-as-a-service (SaaS)," *Int. J. Comput. Appl.*, vol. 10, no. 2, pp. 40–43, 2010.

[4] E. Celikel, M. Kantarcioglu, B. Thuraisingham, and E. Bertino, “A risk management approach to RBAC,” *Risk Decision Anal.*, vol. 1, no. 1, pp. 21–33, 2009.

[5] S. Oh and S. Park, “Task-role-based access control model,” *Inf. Syst.*, vol. 28, no. 6, pp. 533–562, 2003.

[6] A. Pappas and S. A. Hailes, “A comparison of traditional access control models and digital rights management,” Tech. Rep., Univ. College London, U.K., year unknown.

[7] L. Qian, Z. Luo, Y. Du, and L. Guo, “Cloud computing: An overview,” in *Cloud Computing–Proc. First Int. Conf. (CloudCom 2009)*, Beijing, China, Dec. 2009, pp. 626–631.

[8] I. Ray and M. Kumar, “Towards a location-based mandatory access control model,” *Comput. Secur.*, vol. 25, no. 1, pp. 36–44, 2006.

[9] N. Serrano, G. Gallardo, and J. Hernantes, “Infrastructure as a service and cloud technologies,” *IEEE Softw.*, vol. 32, no. 2, pp. 30–36, Mar./Apr. 2015.

[10] H. B. Shen and F. Hong, “An attribute-based access control model for web services,” in *Proc. 7th Int. Conf. Parallel Distrib. Comput., Appl. Technol. (PDCAT)*, Dec. 2006, pp. 74–79.

[11] A. A. Soofi, M. I. Khan, and F. E. Amin, “A review on data security in cloud computing,” *Int. J. Comput. Appl.*, vol. 96, no. 2, pp. 95–96, 2017.

[12] H. Takabi, J. B. Joshi, and G. J. Ahn, “Security and privacy challenges in cloud computing environments,” *IEEE Secur. Privacy*, vol. 8, no. 6, pp. 24–31, Nov./Dec. 2010.

[13] W. Tsai, X. Bai, and Y. Huang, “Software-as-a-service (SaaS): Perspectives and challenges,” *Sci. China Inf. Sci.*, vol. 57, pp. 1–15, 2014.

[14] W. Wang, S. Wang, X. Ma, and J. Gong, “Recent advances in catalytic hydrogenation of carbon dioxide,” *Chem. Soc. Rev.*, vol. 40, no. 7, pp. 3703–3727, 2011.

[15] N. Yang, H. Barringer, and N. Zhang, “A purpose-based access control model,” in *Proc. 3rd Int. Symp. Inf. Assurance Security*, Aug. 2007, pp. 143–148.

[16] R. Yasrab, “Platform-as-a-service (PaaS): The next hype of cloud computing,” *arXiv preprint*, arXiv:1804.10811, 2018.

[17] Y. A. Younis, K. Kifayat, and M. Merabti, “An access control model for cloud computing,” *J. Inf. Secur. Appl.*, vol. 19, no. 1, pp. 45–60, 2014.

[18] E. Yuan and J. Tong, “Attribute-based access control (ABAC) for web services,” in *Proc. IEEE Int. Conf. Web Services (ICWS)*, Jul. 2005.

[19] Q. Zhang, L. Cheng, and R. Boutaba, “Cloud computing: State-of-the-art and research challenges,” *J. Internet Serv. Appl.*, vol. 1, pp. 7–18, 2010.

[20] H. Zhu, K. Lü, and R. Jin, “A practical mandatory access control model for XML databases,” *Inf. Sci.*, vol. 179, no. 8, pp. 1116–1133, 2009.

Air journal of Artificial Intelligence