IJACT 19-12-24

ACCESS CONTROL MODEL FOR DATA STORED ON CLOUD COMPUTING

Ahmed Mateen[1,2], Qingsheng Zhu[1], Salman Afsar[2] , Akmal Rehan[2] , Imran Mumtaz[2] and Wasi Ahmad[3]

[1]Computer Science Department, Chongqing University, Chongqing China.
[2]Computer Science Department, University of Agriculture Faisalabad, Pakistan
[3]Department of Information Technology Resource Center and Data Bank (ITRCDB), University of Agriculture Faisalabad, Pakistan.
E-mail : Ahmedmatin@hotmail.com

Abstract

The inference for this research was concentrated on client's data protection in cloud computing i.e. data storages protection problems and how to limit unauthenticated access to info by developing access control model then accessible preparations were introduce after that an access control model was recommend. Cloud computing might refer as technology base on internet, having share, adaptable authority that might be utilized as organization by clients. Compositely cloud computing is software's and hardware's are conveying by internet as a service. It is a remarkable technology get well known because of minimal efforts, adaptability and versatility according to client's necessity. Regardless its prevalence large administration, propositions are reluctant to proceed onward cloud computing because of protection problems, particularly client's info protection. Management have communicated worries overs info protection as their classified and delicate info should be put away by specialist management at any areas all around. Several access models were accessible, yet those models do not satisfy the protection obligations as per services producers and cloud is always under assaults of hackers and data integrity, accessibility and protection were traded off. This research presented a model keep in aspect the requirement of services producers that upgrading the info protection in items of integrity, accessibility and security. The developed model helped the reluctant clients to effectively choosing to move on cloud while considerate the uncertainty related with cloud computing.

Keywords: access control model, cloud storage, public cloud architecture, network security

1. INTRODUCTION

Because of current development in computer science worked arrangements are changed and shift from individuals and associations. The current modernization in info and computer technology (ICT) has present the higher secured, brisk and less source consumed terminologies. Because of this current alteration and development cloud computing has gain outstanding consideration from analysts, individual and associations.

Manuscript received: October 22, 2019 / revised: November 07, 2019 / Accepted: November 16, 2019
Corresponding Author: Ahmedmatin@hotmail.com
Author's affiliation
Computer Science Department, Chongqing University, Chongqing, China

It has encouraged the whole ICT consumers this way it shifts computers archetypes from traditional to current term of cloud computing. Cloud computing facilitates virtualization and internet delivery of service, and public sources software (Alvaro & Beatritz, 2013).

The cloud computing designed of the cloud replies that infrastructure of framework which containing on prefacing and cloud estates, authorities, middle wares and coding piece, geo-location, the ostensibly apparent premises of these and along these lines the connections across them. The term conjointly possible pointing out document of the network cloud computing designing. Recorded encouraging corresponding b/w associate, reported early convictions around abnormal estate designing might use wherever need. Several management are see dominance of cloud computing since they accessible to expanding the environment while not containing to putting large allocation on directed servers and knowledge normal cost (Anderson, 2011).

Cloud needed a client get to structure whenever every client demands any legislation producers are wrapping through customers personality and title info. Client aspect may hold dependents and features about personality and outline client. The charter is fixed to the sites, whenever is moveable. Client approaches leaves client through final words authorities of the leading personalities. Client approaches more suggested which network keeping up the set of learning for each client, the searching out whenever perfect to responding to among an offer positions to gives client requested. For kinds of servicing a public communicate intermediate are utilized, like intranet where servicing offering are share amid all consumers grouping. The servicing offer in such cloud are available to everywhere (Avdhut, 2015). Finest example of servicing intranet base servers, here host provides are sharing amid clients. The compelling assistance of cloud computing, this is why more interested among the technology all over the world. It is low price, not needed for physical memories hardware's paid and might be worked (Bamiah & Brohi, 2102; Chuprat & Brohi, 2012).

Cloud computing are optimistic resolution of utilizing a get to assets to the intranet. Its stored, prepared or reliable compromises that are given on request. Cloud gives assistance to clients also have scoped among dependable and versatile (Beaston, Hong, Zhang and Feng, 2013). It scales plus enhancing the ability including much hardware' accordance to required, that concessions bargaining snarling needs of cloud stride beyond stride. Client accessing and facilitated info and approach from anyplace in world. Sources in cloud are distribute between clients. The sources give to organization on needed base and assets increases where client needs more and declines then require it's less (Beaty, Kundu, Naik & Acharya, 2013).

Cloud
Computing

Figure 1. Cloud Computing Concept

In cloud computing we may obtain geologically increase the sources, instead the remotely accessible servers. Where aren't idol essence of cloud computing, wherever might state which is accumulation to geologically expand server called as ace personal computers, dedicate the request structure to end users and required of sponsor per utilizing strategies (Bell & Lapadula, 2013). There exist primarily 3 kinds of resources produced through cloud about SaaS, infrastructure as service and platform as services, amazon elastic compute cloud is brilliant example of cloud computing. Cloud changed their ideas of the software's evolution style and it turn out to further web directed. Several management is give cloud management, at instant some noticeable are Virtual Machines wares, Microsoft', Amazons lnc., lnternational Business Machines (lBM) and Google Corporations (Berman, 2013).

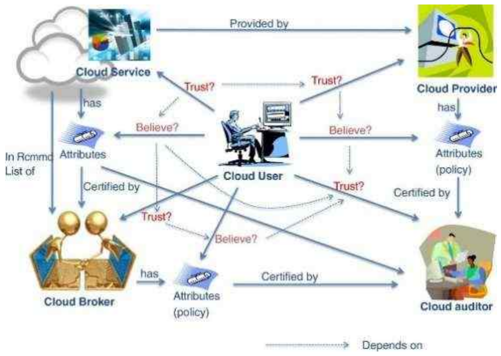


Figure 2. Cloud Insfrastructure

Cloud work as the part of protected which is private, public and hybrid' cloud. Private cloud contains private info of client and restrict to individual, grouping, institution, establishment are so on no one from extreme might get to private cloud (Boneh, Boyen & Goh, 2005). Its virtualized cloud inner info centers beyond the firewall, committing private spaces into info centers. Public cloud is accessible of public no one may utilize its through meaning of intranet can require. Generally, not safe as security in effect exceptionally complex task. For instances

Microsoft', Google Drives and Dr0p B0x and so on giving private and public cloud grouping. Half cloud has virtues of public and private cloud, it comprised of at least two public clouds (Springer, 2005).

2. COMPONENT OF CLOUD

Cloud comprised of 3 main types that are intranet, info centers and geographically distributing server. Everyone from these segments are diverse aspects too assumed crucial in cloud to given administrations to clients (Brucker, Bru, Kearney & Wolff, 2013).

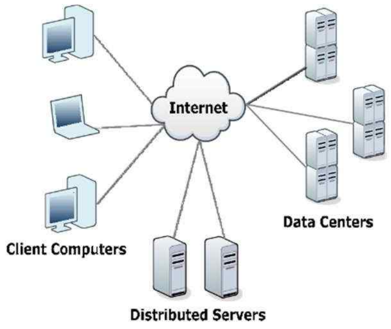


Figure 3. Cloud Components

2.1 Clients

The end users coinciding along clients to taken material relevant to cloud client are 3 levels.

2.2 Thick

This client is superior then thin' client while it has prepared abilities or quantity regions. Also, by utilizing extraordinary programmed thick client interfaces through intranet.

2.3 Thin

Thin clients are client which has no prepared ability. These utilized for to shown info on screening. Info centers scrap apart at sacked of thin consumers. This does not keep space for stored instruction and info.

2.4 Mobile

The particularly readily accessible source for clients get info is mobile client. Android phone, Window phones, Sony Ericson, Nokia Macro soft etc.

2.5 Distribute Server

The most important type of cloud is distribute/transmits server that are available by globe. That client gets the mandatory management for the server (Carroll, Merwe, & Kotze, 2011).

2.6 Data Center

This is an accumulation of large amount of server facilitating differ applications and information. A client by encouragement of internet data center appreciates diverse applications at place. This is topographically transmitted all around world.

3. PREVIOUS WORK

Berman (2013), told that the certain networks base get to control solution for public cloud benefits which are outlined, created also this is appropriate to the any different cloud stages are accessible. Arrangement are sent major aspect of the protection of the services demonstrate on lBM smarts cloud schemes, that are utilized for trades transformation of cloud structure. This application is provoked not only abnormal case of safety through no safety assaults by meaning of structure reception on management, still in extension altogether spared the amount for observance up safety of articles along structure in real procedure. These tests the networking addresses translator postures arrange construct get to control by respect to public cloud is greater test should resolve and have conceive replies for difficulties.

Chen & Zhao (2012), narrated that uncertainty still in inclusion terrible for undertake that utilizations these incidents to send cloud management, for the client's which utilization structure of the writing are on chances, and for cloud supplier which given the cloud infrastructure. ln this manner, a network level gets to control arrangement are required which helps of conveyance of cloud administrations while securing that system layouts.

Chong, Lai & Bonti (2011), narrated that these protection design which gives an adaptable security as an administration demonstrate which cloud supplier might offers the inhabitants also clients are essential elements. Protection like as a services model is offer as gauge safety to supplier to ensure his particular cloud framework; this likewise gives adaptability to occupants which might be extra safety functionalities which assembles to their safety necessities. To outline safety architectures were portrayed or talked about by means of extraordinary sorts of assaults might opposed through developed design.

Crago, Dunn, Eads, Hochstein & Kang (2011), explained that testing problems in shielding cloud administrations field. Creator was presented and developed another entrance control instrument called cloud services get to control. The cloud services get to control system thinks about installment position and administration level and two fundamental principles of cloud benefit. Only hypothetical establishment for this system. Indiscernible get to control arrangements was identified through arrangement of developed strategy covered by contention investigation rules. Inappropriate client entrances the reasonable by control approached concurred the developed getting to deny rules. Network construction were composing such might be bolster this system. Then a contextual analysis are gives to shown behavior. Finally, the appraisal was led gauge idea explosion problems in this model.

Ferraiolo, Barkley & Kuhn (2013), told that the control models for cloud computing are developed by creator. The developed model may satisfy get to control compulsions for various sort of cloud base clients those are shared the assets with potential entrust occupants. It has 3 unique levels of safety; every level may have utilized by level of belief. It bolsters different level of affect ability of data with a specific end goal to limit that might be view or compose data on cloud. The developed demonstrate are adaptability to manage diverse get to authorizations similar cloud client also enabled from utilize several structure identifications by time of confirmed and login.

Green, Hohenberger & Waters (2011), told that unique problems of used of get to control in cloud computing is necessary adaptability also versatility to help countless and sources in the dynamic and divergent quality, by collaborative effort and info shared demands. Producer are developed utilization of prospect base dynamics get to control for cloud computing. Proposition are displayed as get to control model in view of extension of the XACML standards alongside 3 current segments, concerned engines, the concerns evaluation policies. The concerned arrangements show technique of depict chance measurements its evaluation, utilizing nearby and remotely capacities. The concerns arrangements permit clients of cloud also cloud specialist provider to characterize whether to deal with chance base get to control for assets, utilizing diverse evaluation and conglomeration manner. The model achieved the get to adopt in aspect of a blend of XACML distinction and uncertainty examination.Designed of this model are actualized, indicating this keep sufficient expressiveness to portray that models of related works. ln exploratory outcomes, this model taking on proximity of 2 and 6 milliseconds to achieved entrance distinction utilizing a uncertain adjustment.

Habiba, Islam & Ali (2013), developed RBE base framework are executed also comes about and analyzed. lt represented which client simply needs to contain a solitary important for decoded, and infrastructure activity are sufficiently capable paid little need to complexity of kind ordering in network and client presence. Analyze in distinct get to control requisite analysis for cloud computing was led or vital gapes was distinguished, that is not satisfied the regular get to control models. The entrance control model to ace meeting through recognized cloud get to control necessities was developed. The developed model are not only guaranteed the save shared of sources amid potential in trust occupant, still in accession might bolster divergent get to authenticate to similar cloud client and enables then to utilize divergent assets.

4. METHODOLOGY

4.1 Access Control Model

An access control system is an accumulation of segments and strategy which determine the accurate entry to exercises by authenticate clients in aspect of pre-designing get to compliance and prosperity laid out in get to privacy preparation (Hansten, Pankaj & Rubal, 2012). The principal equitable of the get to control network is confined a client to precisely where they should have capacities to do his obligation and shield info from unauthenticated get to. There are vast combination of strategy, models, approaches and regulatory component utilized to developed and composition get to control network. Along every get to control network has the self-estate, strategy and capacity that are captured from a policy and set of policies.

Cloud computing are mutual public situation which is reasoning it exist particular qualities along appearances, for example, demands service or versatility. ln this manner, cloud services providers required a powerful get to control network for controlling entry to the belongings through the capacities to screening exactly who is get toing to authority. The network charged to be able to manage dynamic and irregular proceeding of cloud clients, heterogeneity and modest varieties of association. The examination around cloud protection association is

popularized in part of diagram that unmistakably shown the problem of this exploration and additionally privacy problems in cloud (Hashizume, Rosado & Fernandez, 2013).
Cloud computing is basically software's architecture and platform delivered service onto intranet. Its developing prevalent algorithm in aspect of this comfort, versatile in essence, inhabitant sources, adaptable, on request assistance, get to ability, extraordinary in surroundings. By all the benefits related through cloud it likewise has drawbacks and worried as it is in evolving moment. The significance danger is info protection in cloud computing, one time the client stored its info to cloud it could be in danger and several vulnerabilities client needed to encounter. information put around on cloud are not secured, potential programs could assault on cloud and utilize info for destructive sense, such that putt client's safety and info in danger. It would be certainty breaking for cloud clients and this would not have trusted on cloud.
Therefore, its imperative shield put away info from unapproved get to make cloud computing safe or reliable (Hocenski & Popovic, 2010).

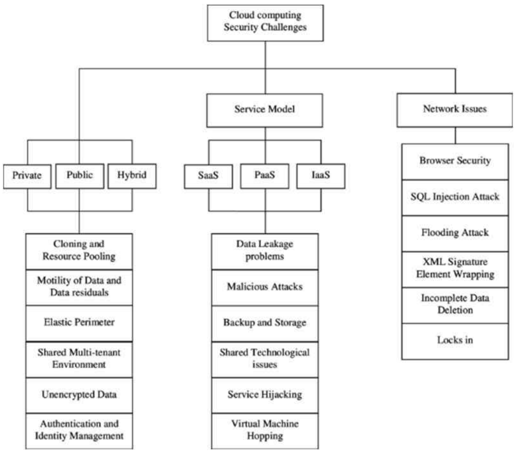


Figure 4. Classification of Cloud Computing Security

5. ARCHITECTURE OF DEVELOPED ACCESS CONTROL MODEL FOR CLOUD

Base on evaluation of analysis carries into areas, that framework for get to control model in cloud computing conditions are shown in figure 4.

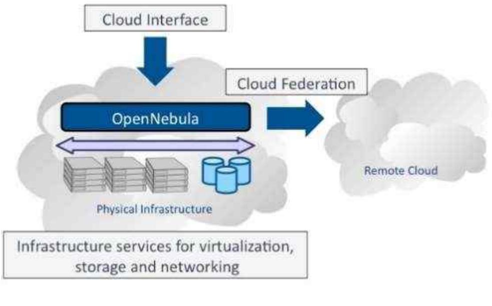


Figure 5. Architecture model of Cloud Computing

The developed model is named as access control and user authentication (ACUA) model that contain accurate tools for validating user legal identity.

- Protection Assertion Markup Language (SAML) is utilized. SAML is a regulation for logging clients into applications based on this discussion in other situations. SAML worked by transfer the client identification from identities producers to services producers.
- Process of device registration is used. The device should be enrolled at ACUA and by get to code we can get to the devices.
- Region detection tool is used which get to user location.

- Algorithm is also used.

6. WORKFLOW MODEL FOR ACCESS CONTROL IN CLOUD ENVIRONMENTS

This model of workflows for get to control in cloud computing situations are shown in figure 6. The distinctive step performs by the CSCs, CSPs and ldPs amid influence is given below:

- A cloud services consumer e.g. it needs to get to and utilize services hosting by cloud services providers or initiate the get to requests.

- ln initial steps dynamics trusted estimation of service providers are figured through CSC that depends on past actions performing and data gave as trusted third parties (TTP).
- Authentications requests were sent to cloud service consumer through the cloud service provider.
- CSC communicated alongside CSP to choose reasonable ldP in light of sort of services requested or protection predilections. lt is expected which cloud services providers chooses IdPs that are accessible in this trust areas depends on confess estimates of several IdPs, or in the old history of corresponding and trusted as well as character value given with another trust entity.
- The CSC at the points out speaking through selected ldP to take the protection expressions (e.g. SAMl affirmations).

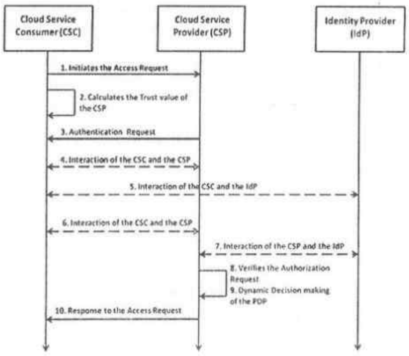

Cloud Service Consumer (CSC)
Cloud Service Provider (CSP)
Identity Provider (IdP)
1. Initiates the Access Request
2. Calculates the Trust value of the CSP
3. Authentication Request
4. Interaction of the CSC and the CSP
5. Interaction of the CSC and the IdP
6. Interaction of the CSC and the CSP
7. Interaction 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 6. Work Flow Model for Cloud

7. HYPOTHESIS

We will provide the access over the stored info and will handle cipher key utilized to encrypt the info by commutative encryption process. We will store this encryption key on third party provider so that cloud providers don't get access to it. Algorithm and our latest additions to it will help improve the performance even better by considering environment specific aspects.

8. ALGORITHM FOR DEVELOPED MODEL

1. ln process of sources requested, and services provides, later clients submitted get to requesting to ACUA, which checked that consumers have a valid authenticate tokens.
2. Presented the consumers identification, ACUA initiate to get to customer actions and obtaining the clients actions belief level. Compared the actions belief level through belief threshold, if greater about the threshold, turns to steps (3); else, refused to provide servicing to the consumer.
3. Reading the customers get to request and put all the cloud cell that could providing corresponded services into this customer queue.
4. Select the best servicing cell in customer cell queue and giving the client servicing get to rights.
5. The servicing cells providing servicing to client and updating clients trusted degrees.

The get to control policy of model not only guaranteed that get to requested of consumers could get responses, but also ensured that all cloud services cell cannot attack or illegally occupy through malicious consumer. This model improves the achievements rate of cooperation, while ensured achievement of cloud services cell.

9. IMPLEMENTING PRIVATE CLOUD

The set trustable third parties in role of EaaS, should complete 3 phases: initially, implementing private cloud; 2nd, given encrypted algorithm; last, multi-threads indication in aspect of several virtual memories. The initial steps are implement this cloud. This cloud enables clients to keep further control about protection and safety due to further detention on the network and clients get to. Likewise, in private-base cloud, the preparing info under the management are achieved under lawful problems and not influenced by organized into repression among processed time. This doesn't get prosperity with the large numbers of belongings, as public cloud

might have offered; which is still sufficiently large suitable to acknowledge the asides of cloud computing. ln private cloud that are conceivable to distributing clients' workloads on several sources relying on enterprising amount.

The divergent aspect, into private cloud, existent group of clients which offered virtual places, while that are checking always in correlation through homogeneous clients in public cloud. Likewise, get to ability of servicing may establish in the private cloud that have intend for particular reasoning for undertaking. For actualizing this cloud, they required utilizing the network for outlining and execute laaS (Infrastructure as services). The most prominent network for discriminant extant are OpenNebula and Eucalyptus.

Actually, the accurate network relies client and application necessary. OpenNebula is easily introduced; more, divergent network like Eucalyptus appreciate in last type. Thus, OpenNebula keep no stored network for images, this is very slow to deploy. Eucalyptus and OpenStack acted relatively consummated that server is handful, still for all systems and virtual memories, time and failure increment.

This is not capable network association, and this is not bolster. Furthermore, like OpenStack are regularly discharging in 4 month which may considering as disadvantage. Amazon services are accepting standards and among another recent public cloud. Consequently, similarity about amazingly fundamental to have the accepted and cloud that is needed.

Still exceptionally solid to learn by defective documentation. This might direct to disagreeability, unless that will be explained in comes rendering maker led the correlation among and Eucalyptus. That quantification along opportunities to achieving the sources that places was propelled and called virtual expedition time. ln serial expedition of virtual memories, the Stack carried on speedy still in parallel expedition of virtual memories, Eucalyptus acted quickly.

The partly Eucalyptus send the image for some opening due to virtual machines capsules propelling separately. At last, by respected to alliances correlation, that asserting which perspective in stack aren't as solid as right scale in Eucalyptus. For example, incorporating a private onto general population cloud are permit by meaning of interfaces.

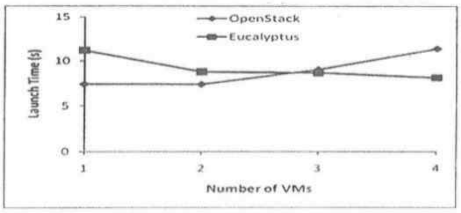


Figure 7. Parallel launch Times

Eucalyptus utilizes 6 coins subject including cells controller which the similar machines by virtual memories is compact that are given fundamental sources, VI3 sector it should be occurred of utilizing supervise, grouping and capacities controller are bunched level of Eucalyptus lastly walrus along cloud controller for seeing and questions divergent details. For reliability amid corresponding among them Walrus also ClC also in adding disentangling association, additionally superfluous requisite of large volume into work, we actualize all details, side for NC, under a solitary physical machine. Cell controller piece combined through vital supervisor are situation. Finally, it utilizes computers for dealing by cloud sectors by meaning of EUCA20OlS and dashboards.

10. CLOUD SECURITY FRAMEWORK

The protection layer are base overs the OpenNebula network, an open-source cloud computing toolbox for heterogeneity distributing info infrastructures. The structure coordinates the adjustment and association of Virtual Memories, and it overseen by means of a ClI, a web service and language 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 developed security layer utilizes the Open Nebula Cloud API (OCA) and verifiably the XMl-RPC API to get to the usefulness of the cloud system over the Open Nebula Cloud API.

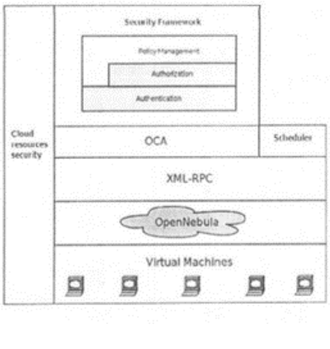


Figure 8. Architecture of Cloud Security Framework

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 approaches to tracked malicious requesting. Later all steps is validated, demands is decapsulated and relevent information is separated. Utilizing OpenNebula Cloud APl, the recent invocation is problems, the time coordination to OpenNebula. That developed privacy network into this path go which is additional layer OpenNebula, where all request should be passed. The whole agreement structure module legitimizes the network naturally takings measured across privacy assaults and to take downward helplessness level of cloud situations. The developed network depending on 2 types that retain functioning front end. The logger along analyzer. That collaboration amid them are outlined in fig 8.

11. RESULTS

11.1 Evaluation of Developed Access Control Model

The developed model was named as ACUA model which accommodate accurate tools for validating client legal identity and procuring the get to control benefits for sources following to role information's. ln the developed model, idea of agent, multi-clouds and SaaS are considering setting up a reliable algorithm amid client confirmation and get to control process. The detailed intro of developed model in figure 4, given model used the ideas of multi-clouds for planning a cloud base SaaS and manage get to and user authentication procedure to increase the reliability of public or private cloud computing conditions.

The developed model one client base agent and four cloud base agents to set up a reliable algorithm throughout procedure, service and communication. The primary objective of given operators is expanding the amount of intelligence and reliability throughout cloud computing communication. Accordingly, every agent is isolate execution and associated with different agents through ACUA application. The responsibilities of every agent and ACUA portrayed in following functions.

Get to control manages figuring out which client acquire what kind of get to authorities against an article. The objective of get to control networks are given assurance to network resource amid unapproved and illegal get to through malevolent client. The secured or impressive get to control network encourages resources shared also. The problems of get to control in area of cloud system, in collaborative, conveyed, concerted atmosphere like distributed system, there are numerous clients keeping distinctive put of necessities get to the resourced and servicing, through various get to rights, is known as the distributing get to control. Different clients have distinctive get to integrity the get to accessible available resourced into network that should be briefly determined and implemented accurately. Get to control includes determination and requirement of client's get to authorization and get to reductions with respect to sources of the structure.

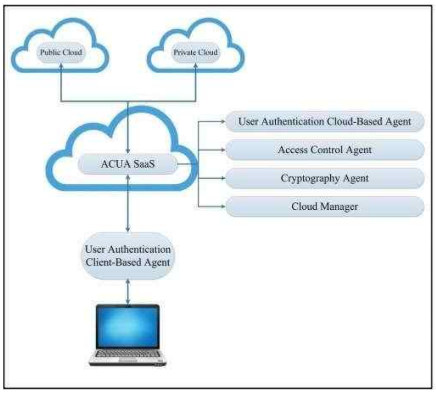


Figure 9. Proposed Access Control Model in a View

12. CLIENT-BASED USER AUTHENTICATION (CBUA)

In present user's authentication models reliance of procedure on cloud server's structure are one of the most difficult issue. As needs be, client base users authentication agent are application which deals with the character of clients before get toing to cloud condition. Because of this intention, client's registering device should be registering by installing CBUA. The accompanying fig demonstrates the procedure of devices registered in ACUA.

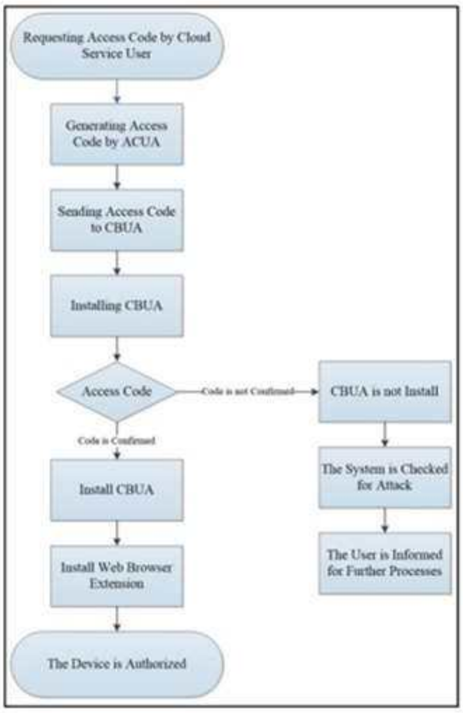

Requesting Access Code by Cloud Service User
Generating Access Code by ACUA
Sending Access Code to CBUA
Installing CBUA
Access Code
Code is not Confirmed
CBUA is not Install
Code is Confirmed
Install CBUA
The System is Checked for Attack
Install Web Browser Extension
The User is Informed for Further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

Figure 10. Process of Device Registration

The device should be enrolled at ACUA and enlisting and get to code which will send to devices. The get to code will be enter throughout installation processing will be examined through ACUA database. After confirming, device will be enlisted by MAC lD and applications will be installed. Besides, the customer base application should be should install an expansion on web browsers of registering devices for more process. After registered a device by installing CBUA and affirming it, clients might get to the cloud servers all further safely. The accompanying algorithm demonstrates execution of CBUA agents in details.

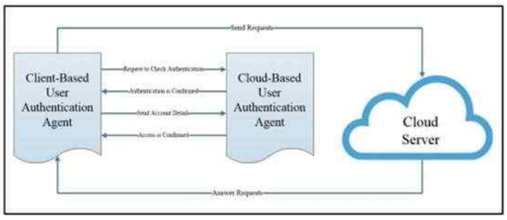

Send Requests
Client-Based User Authentication Agent
Request to Check Authentication
Authentication is Confirmed
Send Account Details
Access is Confirmed
Cloud-Based User Authentication Agent
Cloud Server
Answer Requests

Figure 11. Performance of CBUA Agent

According to above figure performance of CBUA are as follows:

- Client base agents sent the request for checking authorization to cloud base agents.
- Cloud base agents gets requesting and confirm it if customer based get to code is acceptable.
- Client base agents sent accounts details, like the users' name and password for cloud base users confirmation.
- After affirmation client might get to the cloud servers.

Users and cloud servers' will convey to one another and suitable information will be transmitting.

12. EVALUATION OF DEVELOPED MODEL

The developed model is evaluated through four parameters e.g. performances, compatibility, safety and power of intelligence.

13. PERFORMANCES

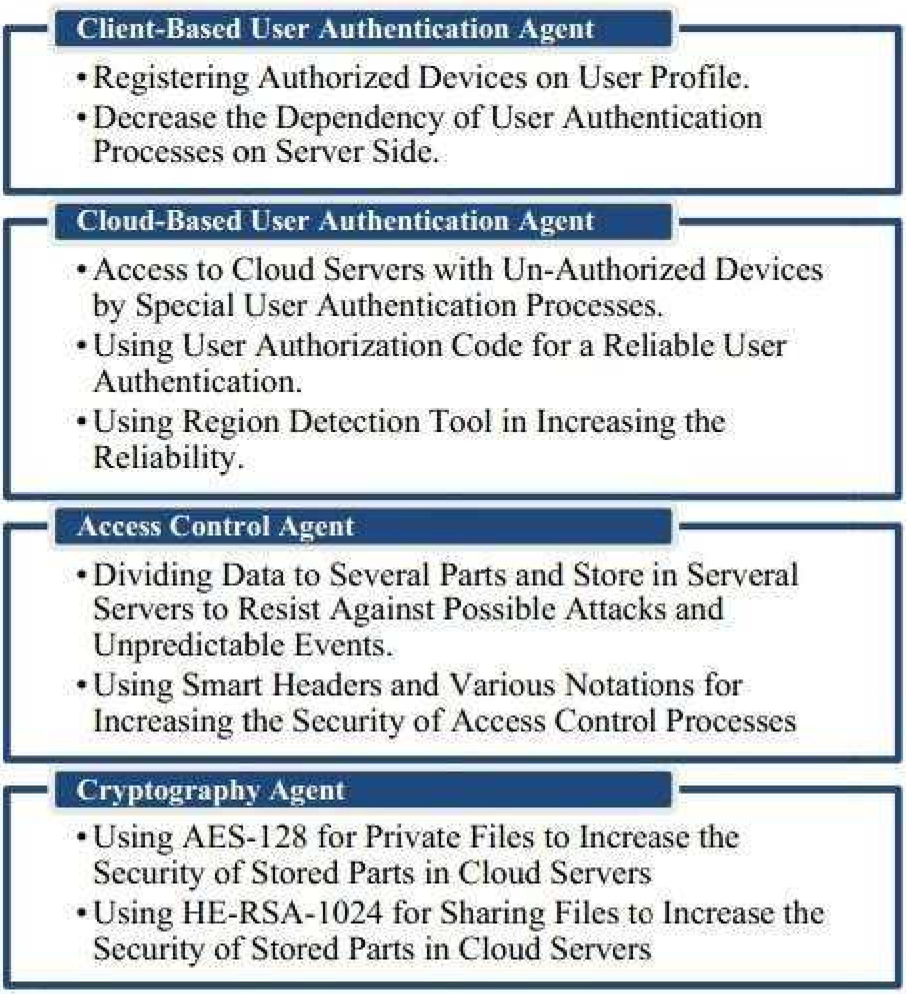
The brief performance of developed model is show in following table.

Table 1. Briefed Performance of Proposed Model

Mani Task	Sub Task	Expectations
User Authentication	Client-based user authentication	Reliable Authorization in client side. Manage client-based user authentication process
User Authentication	Client-based user authentication	User conformation code for accessing from unauthorized device. Manage cloud-based user authentication process
User Authentication	Region Detection	User location service for user authentication process
Access Control	Access control Agent	Dividing the data and stored in several multiple locations. Adding header for access management
Access Control	Cryptographic Agent	Cryptography process management
Access Control	Cloud Manager	Managing private and public cloud data

13.1 Security

The developed get to control model and client authorization model increasing the chance of protection and reliability in cloud computing conditions considerably. The following diagram are shown protection evaluation of developed 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

Figure 12. Security Evaluation of Proposed Model

As shown in the fig. 12 considering conditions of developed model will increasing chance of protection in cloud computing conditions during access, downloads, uploads, client authorizations and transportation. This increased will accession the reliability of cloud base servicing.

REFERENCES

[1] Alvaro, J., & Beatritz, B. (2013). A New Cloud Computing Architecture. Journal of Computer and Applications. 2(2): 40-45.

[2] Anderson, R. (2011). Security Engineering: A Guide to Building Dependable Distributed Systems. Journal of Security Engineering. 2(1): 640-645.

[3] Avdhut, S. B. (2015). A Review of Role Based Encryption System for Secure Cloud Storage.

[4] International Journal of Computer Applications. 10(9): 975-980.

[5] Bamiah, M., Brohi, S., Chuprat S., & Brohi, N. (2012). Cloud Implementation Security Challenges. Journal of Security Engineering. 3(1): 174-178.

[6] Beaston, D., Hong, C., Zhang, M., & Feng, D.G. (2013). Cryptographic Access Control Scheme

for Cloud Storage. Journal of Computer Research and Development. 4(7): 259-265.

[7] Beaty, K., Kundu, A., Naik V., & Acharya. A. (2013). Network Level Access Control Management for Cloud. IEEE International Conference on Cloud Engineering (IC2E). 98-107.

[8] Bell, D. & Lapadula. L. (2013). Secure Computer Systems: Mathematical Foundations.

[9] International Journal of Computer Applications. 6(9): 7-10.

[10] Berman, S. (2013). Data Severe Dynamic Access Control Model. IEEE Transactions on Dependable and Secure Computing. 3(4): 221-229.

[11] Boneh, D., Boyen X., & Goh, E.J. (2005). Hierarchical Identity Based Encryption with Constant Size Cipher Text, in EUROCRYPT. New York, NY, USA: Springer Verlag. 3494: 440- 556.

[12] Brucker, A., Bru, L., Kearney P., & Wolff. B. (2013). An Approach to Modular and Testable Security Models of Real World Health Care Applications. IEEE 16th ACM Symposium on Access Control Model and Technologies. 2(2): 133-142.

[13] Carroll, M., Merwe, V.D., & Kotze, P. (2011). Secure Cloud Computing Benefits, Risks and Controls. Journal of Information and Security. 6(5): 1-9.

[14] Chen, L., & Hoang, D.B., (2011). Novel Data Protection Model in Healthcare Cloud. IEEE 13th International Conference on High Performance Computing and Communications (HPCC). 550-555.

[15] Chen, D., & Zhao, H. (2012). Data Security and Privacy Protection in Cloud Computing.

[16] Computer Science and Electronic Engineering. 1(5): 647-651.

[17] Chong, A., Lai, H., & Bonti, A. (2011). Cloud Security Defense to Protect Cloud Computing.

[18] Journal of Network and Computer Applications. 34(4): 1097-1107.

[19] Crago, S. and Dunn, K., Eads, P., Hochstein, L., & Kang, M. (2011). Heterogeneous Cloud Computing. IEEE International Conference on Cluster Computing. 378-385.

[20] Ferraiolo, D., Barkley, J., & Kuhn, D. (2013). A Role Based Access Control Model. ACM Transactions on Information and System Security. 2(1): 34-64.

[21] Green, M., Hohenberger, S., & Waters, B. (2011). Outsourcing the Decryption of ABE Cipher Texts. USENIX Security Symposium, USA. 78-83.

[22] Habiba, M., Islam, M., & Ali, A. (2013). Access Control Management for Cloud. IEEE 12th International Conference on Security and Privacy in Computing and Communications (TrustCom). 485-792.

[23] Hansten, A., Pankaj, P., & Rubal, C. W. (2012). Cloud Computing Security Issues. International Journal of Advanced Research in Computer Science and Software Engineering. 55 (21): 81-82.

[24] Hashizume, K., Rosado, D.G., & Fernandez, E. (2013). An Analysis of Security Issues for Cloud Computing. Journal of Internet Services and Applications. 4(1): 1-13.

[25] Hocenski, Z. and Popovic, K. (2010). Cloud Security Alliance. 33rd MIPRO International Convention. 8(6): 344-349.

[26] Al-Ani, M.S. and Haddad, R. (2012). IPv4/IPv6 Transition. International Journal of Engineering Science. 4(12): 4815-4822.