International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER SSRN

IJIEMR Transactions, online available on 15th Nov 2021. Link
:http://www.ijiemr.org/downloads.php?vol=Volume-10&issue=ISSUE-11

DOI: 10.48047/IJIEMR/V10/I11/17

Title: **Flexible password-authenticated key agreement scheme for multiple servers to server architecture**

Volume 10, Issue 11, Pages: 121-123

Paper Authors
Ms. Anjali Mamidi, Ms. Ritwika Das

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Flexible password-authenticated key agreement scheme for multiple servers to server architecture

[1]Ms. Anjali Mamidi, [2] Ms. Ritwika Das
[1]Student, BTech in Computer Science, Gitam deemed to be University, Hyderabad, Telangana
[2]Student, BTech in Computer Science, Gitam deemed to be University, Hyderabad, Telangana

Abstract:

Protection is one of the key factors to be considered in application development. Every application should follow some security mechanisms to be free from fraudulent users. One of the important criteria to ensure security is Access control. [4]The reliability and security of the cloud and user are assured and effectively guaranteed during its interaction in the cloud computing environment. But these traditional models were unable to determine the vulnerability and ambiguity created by these open conditions. So the main focus throughout the evolution of new access control methods is on creating a mutual trust relationship between both interaction parties. The paper proposes a mutual access control model which is trust-based (MTBAC). Trust relationships between both interaction bodies are secured by mutual trust mechanisms. This model takes both the cloud service node's trustworthiness and user's action trust into consideration.

Key Words: Access control, Cloud, Trust

Introduction

Cloud computing provides services to people via the Internet. People use these services most often in their personal and professional lives. It helps users by providing the resources only when required through the internet. These being scalable helps the users from maintenance fees and up-front costs. [2]Security is an essential concern of the scalable computing environment that cannot be neglected. This environment is a common shared environment; therefore the frequency and anonymity of learning sources and services remain exceptional characteristics of these environments.
The researcher's main focus is to implement these policies in unique ways. Hence, the conventional standard access control model seemingly cannot meet the security demands of cloud-based. It is likely to encounter a set of challenges during its implementation in on-demand computing environments. Among the many methods to ensure its security, Access control is the most crucial measure. [2]Early access control technology also solves the security difficulties made by legitimate users' misoperation besides ensuring the standard access requirements of actual users and preventing attacks from unapproved users. In this paper, the access control models are developed using trust computation mechanisms.[3]Shared trust between both interaction parties users and cloud service nodes is guaranteed using trust mechanisms.

Trusted users alone have cloud access, and simultaneous users can choose those with the most trustworthy cloud service connections. Several professors have developed access control patterns that are fit for cloud environments. [1]Chaotic Maps, another and efficient way to the key agreement between communicating nodes. It is based on Chebyshevpolynomials(Chaos theory). Our proposed work is based on Chebyshev polynomials (Chaos theory) which is the field of study in mathematics that deals with the behavior of Dynamical systems that are highly sensitive to initial conditions, where Dynamical system is a system in which a function describes the time dependence of a point in a geometrical space

Proposed :

Our main objective is to study fraud user perception when entering the website.
Combining Trusted Computing into cloud-based environments and doing that a reliable process to render this service is an exciting subject in cloud protection. [1]Santos et al suggested entrusted cloud systems TCCP upon which IaaS service providers could present a restricted box-type execution situation to their users and assure the secrecy of customer virtual devices. Before commencing the virtual device, the user is permitted to verify whether the service rendered is safe or not. [1] Jong P. Yoon et al recommended a reliable design for cloud sources depending on the authori-zation series. These designs utilized specific metadata of cloud support and access control system to set authorization organizations.

Trust Degree - It describes the inclination with which entity the user would prefer to communicate with. It is formed of recommended trust and direct trust. The trust degree of cloud-based service node c is displayed as Tc(t), at time t. [1]If Tc(t)= I, it

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

describes that node c has been completely trusted by user u. If Tc(t)=0, it implies that node c is not at all trusted by the user u.

Direct Trust - These relationships are developed through firsthand engagement in communications among every user and object.

Trust pheromone - It is expressed as Tp. It is a primary perception of direct trust degree between both interaction bodies. [1]The user u's Tp towards cloud service node c is represented by $Tp_j(t)$, at time t. In the beginning, the value of Tp is usually assigned to '0', that is $Dt_c(0)=c$, where c is constant. If the direct trust degree is initially set to '0', then the rate of Tp also needs to be '0'.

System Methodology-

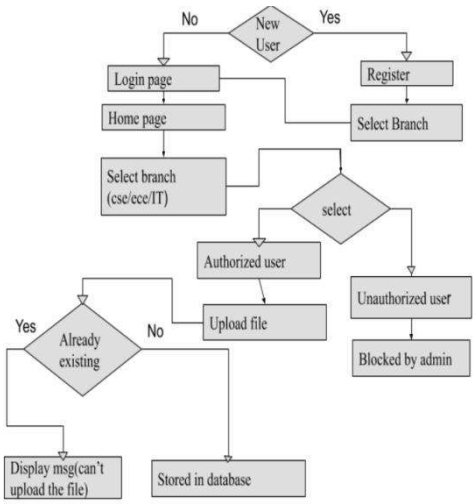

Figure 1: workflow of the user

Results & Discussions:

Figure 2: registration and login page of the website

Figure 3: Showing the screen of the home page where the user can select the branch

Figure 4: If the user is considered as good user then they are allowed for further access that is file uploading.

Conclusion:

This paper examines access control and recommends a mutual trust-based access control design. [1]Unlike these conventional mecha-nism, MTBAC takes the trust of both the interaction parties into consider-ation. It adjusts to the features of dynamism, risk, and sharing in cloud computing. In the users' trust model, the behavior of the user is classified into 3 types and each of these types holds a specific weight. The trust level of the user will be obtained by trust quantization of the user's performance. Finally, implement ac-cess control in cloud computing environments based upon this mutual trust between both the cloud service nodes and the user, and guard user's and cloud server's safety efficiently.

References:

[1] Guoyuan Lin, Shan He, Hao Huang. *Access Con-trol Security Model Based on Behavior in Cloud Computing Environment[J]. Journal of China In-stitute of Communications*, **2012, 33(3): 59-66**.

[2] Guoyuan Lin, YuyuBie, Min Lei. *Trust Based Access Control Policy in Multi-Domain of Cloud Computing. Journal of Computers*.**2013, 8(5): 1357-1365**.

[3] ijitet.com

[4] www.ijcttjournal.org