Volume 5, Issue 1, January 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Implementation of Effective Third Party Auditing for Data Security in Cloud

Sukhvinder Kaur [1], Mandeep Kumar Kashyap [2], Ms. Jagdeep Kaur[3]
Research Scholar ,Department of CSE, PTU, INDIA
Assistant Professor & HOD(CSE), HPTU Hamirpur, KCIET, Pandoga ,Una (H.P.), INDIA
Assistant Professor & HOD(CSE\IT),KCCEIT SBS Nagar, INDIA

Abstract-Cloud Computing has been envisioned as the next-generation architecture of IT Enterprise. It moves the application software and databases to the centralized large data centres, where the management of the data and services may not be fully trustworthy. This unique paradigm brings about many new security challenges, which have not been well understood. This work studies the problem of ensuring the integrity of data storage in Cloud Computing. In particular, we consider the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. The introduction of effective TPA eliminates the involvement of the client through the auditing of whether his data stored in the cloud is indeed intact, which can be important in achieving economies of scale for Cloud Computing. By doing so, the burden on the authorization server is reduced, and the Denial-of-Service attacks on it during access control process are avoided. DDOS is a type of DOS attack where multiple compromised systems -- which are usually infected with a Trojan -- are used to target a single system causing a Denial of Service (DoS) attack. Victims of a DDoS attack consist of both the end targeted system and all systems maliciously used and controlled by the hacker in the distributed attack. The combinational RBAC & MAC Algorithm technique is used in this work. In third party auditing, roles can be easily created, changed, or discontinued as the needs of the enterprise evolve, without having to individually update the privileges for every user. This design is implemented in the ASP.NET environment.

KEYWORDS: DDOS Attack, Third party, Authentication, Authorisation, Assignment Roles

I. INTRODUCTION

Cloud computing is a rising area within the field of information technology (IT). Cloud computing is a model for enabling convenient, on-demand network to a shared pool of configurable computing resources (e.g., networks, servers, applications, and services) that can be instantly provisioned and released with minimum management effort or service provider interaction. [1]. Cloud computing security (sometimes referred as "cloud security") is a sub-domain of computer security, network security, and information security. [3] It refers to a broad set of policies, technologies, and controls deployed to provide protection to data, applications, and the associated infrastructure of cloud computing. Cloud security is not to be related with security software offerings that are "cloud-based‖. Access control services [4] should be flexible enough to capture dynamic, context or attribute/credential based access requirements, and ease enforcement of the principle of least privilege. Such access control services required to integrate privacy protection requirements derived from complex rules. It is important that the access control system deployed in clouds is easily managed and its access distribution is administered efficiently. It is also important to make sure that the cloud delivery models [5] provide access control interfaces for proper interoperability, which demands for a policy neutral access control design and enforcement structure that can be used to address cross-domain access control issue. There are some attacks like, DDDOS Distributed denial of service attacks which are launched by multiple zombies or compromised nodes to send large number of requests to a target node in the network at very short time intervals. As a consequence, the target node is flooded with more number of requests than its maximum processing capacity, thus incapacitating it from providing any further service to its clients. More specially, distributed denial of service attacks lead to exhaustion of the limited energy resources of a target node, owing to the large number of requests towards it. In this thesis, Third Party Auditing technique has been proposed to solve this issue. Third Party Auditor is kind of inspector. There are two categories: private auditability and public auditability. Although private auditability can achieve higher scheme efficiency, public auditability allows anyone, not just the client (data owner), to challenge the cloud server for the correctness of data storage while keeping no private information. To let off the burden of management of data of the data owner, TPA will audit the data of client. It eliminates the involvement of the client by auditing that whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for Cloud Computing. MAC algorithm is used in this technique. A MAC algorithm, sometimes called a keyed (cryptographic) hash function that accepts as input a secret key and an arbitrary-length message to be authenticated, and outputs a MAC (sometimes known as a *tag*).

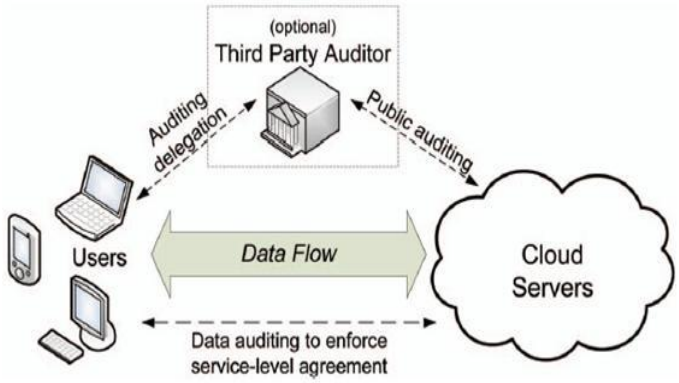

Figure 1. Third Party Model

Three primary rules are defined for Third Party:

1. Role Granted: A subject can exercise permission only if the subject has selected or been assigned a role.

2 .Role authorization: A subject's active role must be authorized for the subject. With rule 1 above, this rule ensures that users can take on only roles for which they are authorized.

3. Permission Granted: A subject can exercise permission only if the permission is authorized for the subject's active role. With rules 1 and 2, this rule ensures that users can exercise only [6] permissions for which they are permitted.

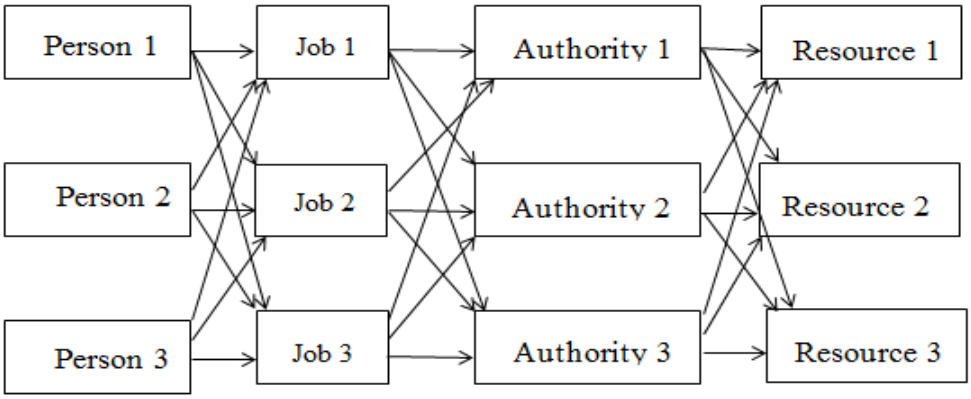

Figure 2. Represents Role Assignments and Permission

II. MOTIVATION

Cloud computing is becoming more and more popular nowadays, where data is outsourced into the cloud. Its advantages are obvious: relief of the burden of storage management on data owners, universal data access with independent geographical locations, and avoidance of capital spending on hardware, software, personnel maintenance, etc [1].

However, outsourcing data leads to new security issues as listed below.

- The first issue is data integrity and data loss. [2][3][4] Describes a wide range of both internal and external threats to data integrity. Data loss examples are mainly cloud service providers (CSP), for monetary reasons, reclaiming storage by discarding data that has not been or is rarely accessed [5], or even hiding data loss incidents to maintain a reputation [6].
- The second issue is data leak. To keep the data confidential against un-trusted CSPs, the main method is to store only the encrypted data in the cloud [7][8].
- The third issue is authorization and access control for data files. That is, operations on files must be authorized, and the cloud server (CS) must control operations on files according to the authorization information.

The first issue and the second issue are addressed by proof-of-storage schemes [9][10][11] and encryption schemes respectively [7][8], while the third issue is now under consideration by the NIST, who introduces a standard reference model, named role-based access control (RBAC) [12]. The basic idea of RBAC is establishing permissions for accessing data based on the functional roles, and then appropriately assigning data users to a role or a set of roles. Finally, access controls are based on the roles that individual data users have.

Distributed Denial of Service (DDOS) attack is a major problem for any kind of server. It not only affects the performance of the server but also it takes a lot of burden over the user using the server. A lot of different mechanisms have been already implemented to prevent the DDOS attack such as third party authentication (TPA) was integrated with access control mechanism but there was problem with that mechanism because TPA was outsourced to third party that was result in higher cost and the system was totally relay on third party that effects the reliability of the system .Our problem statement becomes the prevention of server [13] from unauthorized access so that the number of request to the server decreases. Our problem statement also includes one step further point in which if the DDOS attack happens then what are the chances of prevention of our data. For the same purpose, we have an integrated authentication mechanism

for which a MAC number would be associated with every data which would be helpful in the identification to check whether the data which has been uploaded before has been changed or not.

III. WORK FLOWCHART

Here we are implement duel mechanism

1. User id: it shows that a request comes for process it detect by their id that helps to communicates with that client.
2. It is method that helps to detect the request on the basis of their behavior. It calculates all requests that sent from a client for process on server. The server works on the basis of roles [14] mechanism that implemented with the detection and prevention of DDOS attack.
3. Now a detection system that store all the request time and manage them during process.
4. Now at the server side a threshold set that checks the number of requests from the user and according to that a threshold set for prevent that attack.
5. If he requests are continually sent by client at a same time then after some request it checks the threshold that decided. If user crosses the limit that decided then the attack is detected and the client that request will discard from the server. Else it shows normal behaviour for the client that send request for processing.

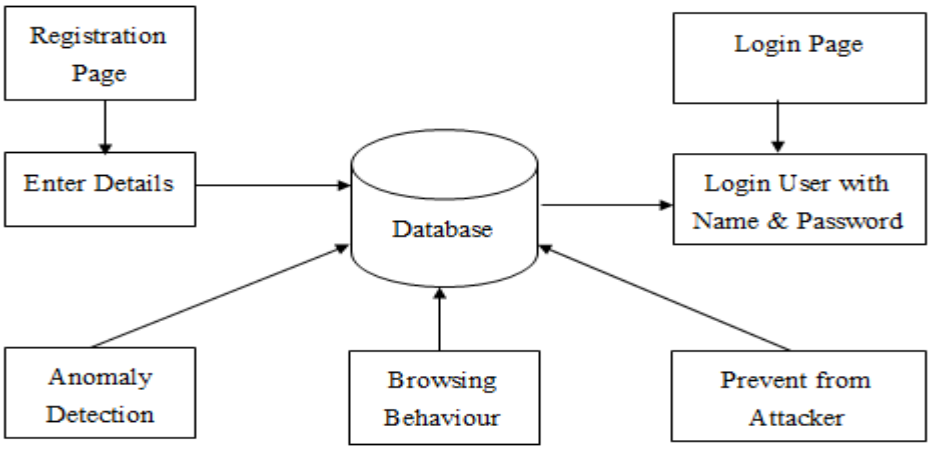

Figure 3. Proposed methodology

- **The main components of this model are:**

1 **User**: User can access their services according to their roles.

2 **Authentication and Role Set assignment**: In this step a login page appears to the user where user enters his/her user id and password. If this user's id and password is matched with the administrator database entries stored in the Knowledge Base, then the user is moved to next step of role assignment where the username and the corresponding Role Set is defined.

3 **Role assignment**: User can select one of the roles from the Role set. The role selected is assigned, if at that time, the same role is not associated with another user.

4 **Knowledge Base**: Knowledge Base is having the administrator's data which [15] can be used for authenticating the user and providing him with the Role Set.

- **Access control model based on ontology**

1. The user's role can be dynamically and partially delegated by changing permission.
2. Constraints on the authorized role can be defined for dynamic access control.
3. Objects, conditions, and obligations for data retrieval can be considered
4. Data access can be rejected whenever wanted.
5. Access control is based on location and equipment needs.
6. The key important factor is the prevention of any misuse of access rights.

In the ontology designed, there are two roles:
ADMIN: that can upload the data
USER: There are three types of users:

1) NORMAL-lowest priority
2) EXTENDED- high priority
3) PREMIUM- highest priority

- Upload the file
- Uploaded file can be text file.
- Normal user can only access or download the TEXT files.
- Extended user can update or download text file.

- Premium user can update, modify or download the entire file whether [16] it is text file.
- There is a limitation on the user.
- Change can be made from higher to lower level

IV. PROPOSED ALGORITHM TO IMPLEMENT METHODOLOGY

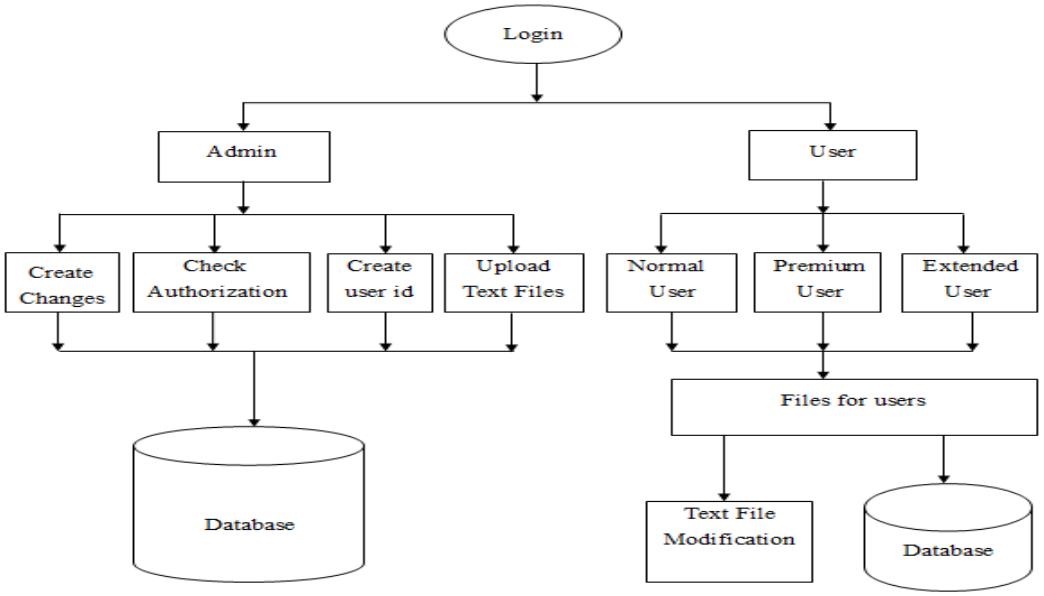

Figure 4. Single User Model

V. RESULTS AND IMPLEMENTATION

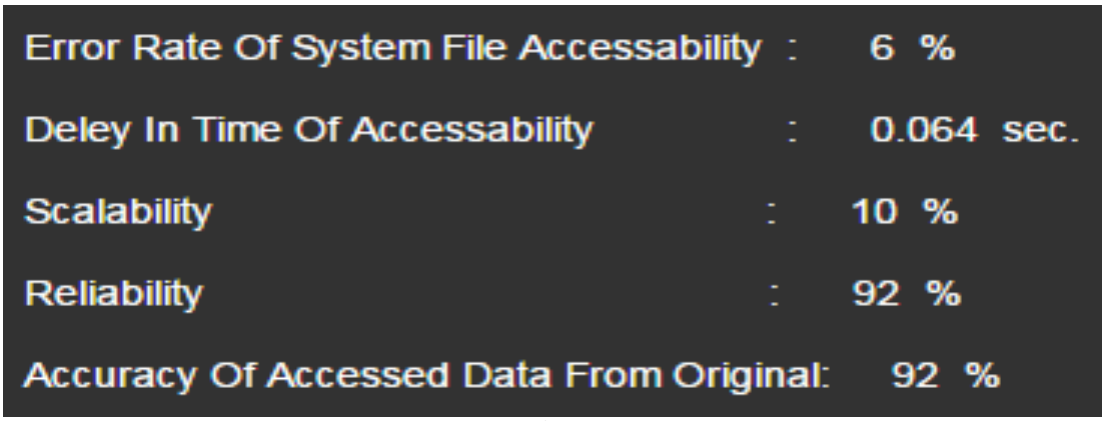

Figure. 5 Performance parameters

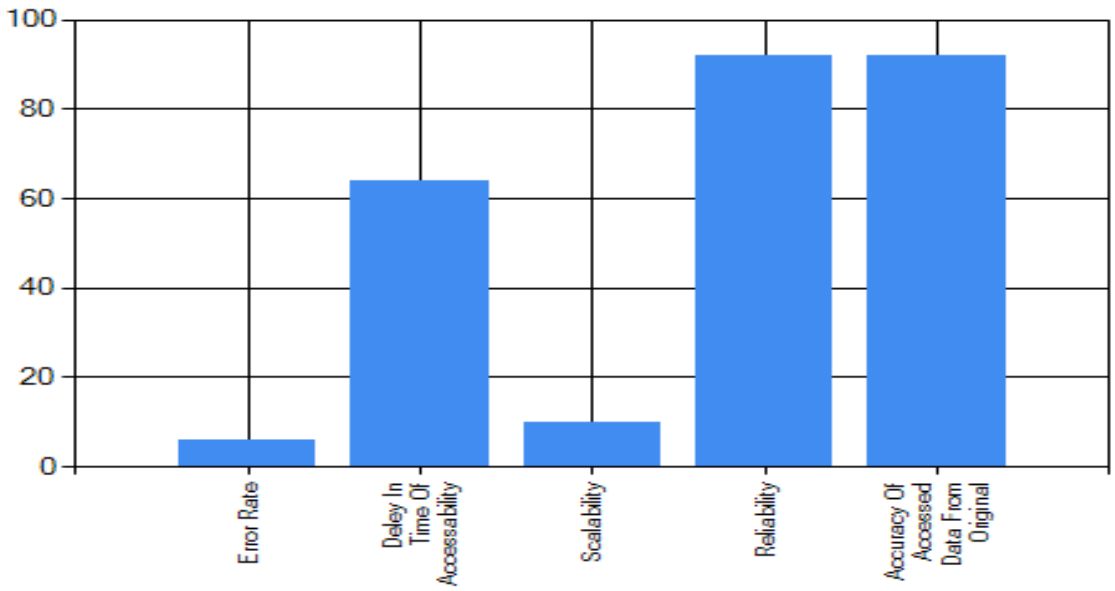

Figure. 6 Performance graph

The whole simulation has been taken place in .NET environment, in which various parameters like error rate, delay time, scalability, reliability and accuracy has been taken. Above mentioned figure and graph shows that how much value has been obtained using propose model.

VI. CONCLUSION AND FUTURE SCOPE

We have seen how delegation of responsibility trusted 3rd party which provides security services secures user data. It reliefs the client from maintaining any kind of key information and allowing the client for using any browser enabled device to access the cloud services. It allows the client to verify the integrity of the data stored on download or retrieval of its own stored data in cloud. The client can share the data securely with specific band of people without any overhead of key distribution. The results show that our scheme is quite improved, because it can reduce the burden on the authorization server by separating the authorization process from the access control process, and releasing the authorization server from the access control process. Therefore, the Denial-of-Service attacks on the authorization server during access control process are avoided.

1. To enhance the security more, a mechanism to secure the keys in security cloud can be an area of research.
2. To reduce the overhead of network traffic can be another area of research.

REFERENCES

[1] Chandramouli R., (2000), "Application of XML Tools for Enterprise-Wide RBAC Implementation Tasks", *5th ACM workshop on Role-based access control*.

[2] T. Finin et. Al (2008), "ROWLBAC – Representing Role Based Access Control in OWL", *ACM SACMAT'08*, Vol.11.

[3] M.M.R. Chowdhury et. Al (2008), "Enabling Access Control and Privacy through Ontology", *4th International Conference on Innovations in Information Technology, IEEE.*

[4] Rodolfo Ferrini et. Al (2009), "Supporting RBAC with XACML+OWL", *14th ACM Symposium on Access Control Models and Technologies (SACMAT '09)*.

[5] Avari Sirisha et. Al (2010) "API, Access Control in Cloud Using the Role Based Access Control Model", *International Conference on Trendz in Information Sciences & Computing (TISC), IEEE*

[6] L. Fuchs et. Al (2011), "Roles in information security - A survey and classification of the research area", *Elsevier Journal of Computers & Security*, Volume 30, Issue 8.

[7] Lingfeng Chen et. Al (2011), "Novel data protection model in health care cloud", *International Conference on High Performance Computing and Communications, IEEE.*

[8] Lili Sun et. Al (2010), "Semantic access control for cloud computing based on e-Healthcare", *16th International Conference on Computer Supported Cooperative Work in Design, IEEE.*

[9] Sukhoon Lee et. Al (2012), "Two-step Role-Based Access Control method for Ontology Storage", *The 2012 World Congress in Computer Science, Computer Engineering and Applied Computing (WORLD COMP'12).*

[10] Blake S et. Al (2009), "An architecture for differentiated services, in: *IETF*", RFC 2475.

[11] Zhao W. et. Al (2001), "Internet Quality of Service: An Overview", *Columbia Technical Report CUCS-003-00.*

[12] Kargl F., et. Al (2003), "Protecting web servers from Distributed Denial of Service attacks", *In Proceedings of the Tenth International Conference on World Wide Web*, Hong Kong, pp. 514–524.

[13] Ferguson P., et. Al (2001),"Network ingress filtering: defeating Denial of Service attacks which employ IP source address spoofing", In *RFC* 2827.

[14] Global Incident analysis Center—Special Notice—Egress filtering, Available from <http://www.sans.org/y2k/egress.html>.

[15] Park K., et.al (2001) ,"On the effectiveness of route-based packet filtering for Distributed DoS attack prevention in power law Internets", *In Proceedings of the ASIGCOMM_01 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, ACM Press, New York, pp. 15–26.

