Review of Third Party Authentication Model for Securing User Space in Cloud Computing

Jahangir Ahmad Dar[1], Mandeep Singh Saini[2]
[1]*M.tech Scholar, Chandigarh Engineering College Landran*
[2]*Assistant Professor, Chandigarh Engineering College Landran*

Abstract - Cloud Computing that provide High Performance Computing services are being developed to address the need of pet scale and even exascale computing. It does so by providing necessary infrastructure for the formation of dynamic Virtual Organizations. Third Party Authentication is also an access control procedure which was proposed long back. According to this mechanism, the users of the cloud have a role in the cloud. An advantages of the cloud and hence most of the enterprises have their own clouds today. A cloud provides many services like Infrastructure as a Service, Software as a Provision and Platform as a Service. But there are many challenges associated with cloud computing. One of these challenges is security. Security in any field is very important and in cloud it is really important. Access control is one of the main issues which should be concentrated for a secure cloud.

Keywords - Cloud Computing, High Performance, Services, Third Party Authentication, Security and challenges**.**

I. INTRODUCTION

Cloud computing has developed as one of the innovative [1] technologies as it enables users to share their possessions and pay only for what they use [2]. This helps users to save time, money and it also helps users who have very little impression about the technologies. With the help of cloud, one can effortlessly use any resource from anywhere. The cloud decreases the complication of using resources. This also permits people to share their resources.

There are many types of cloud like;

- Public cloud
- Private cloud
- Hybrid cloud
- Inter cloud and
- Multi cloud.

Private cloud is a cloud related with a single organization and a public cloud is a common cloud which is intended for public use. Inter cloud is generally termed as "cloud of clouds". Security is also provided for the properties present in the cloud. A cloud has very high storage capacity, which allows the space of many resources, files. Performance, scalability, security, maintenance are some of the characteristics of a cloud.

Advantages of Cloud Computing

- **Achieve economies of scale** – increase volume output or productivity with fewer people. Your cost per unit, development or product falls [3].
- **Reduce spending on technology infrastructure.** Maintain easy contact to your information with negligible upfront spending. Pay as you go (weekly, quarterly or yearly), based on demand.
- **Globalize your personnel on the cheap.** Individuals worldwide can access the cloud, provided they have an Internet connection.
- **Reorganize processes.** Get extra work done in less time with less people.
- **Reduce capital costs.** There's no need to occupy big money on hardware, software or licensing fees.
- **Improve accessibility.** You have access anytime, anywhere, making your life so much easy.
- **Screen projects more effectually.** Stay within budget and ahead of completion rotation times.
- **Less workers training is needed.** It takes fewer people to do more work on a cloud, with a negligible learning curve on hardware and software problems.
- **Minimalize licensing new software.** Stretch and grow without the need to purchase exclusive software licenses or programs.
- **Recover flexibility.** You can change direction without serious "people" or "financial" issues at stake.

Disadvantages of Cloud Computing

- Security
- Lock-in
- Lack of Control
- Reliability

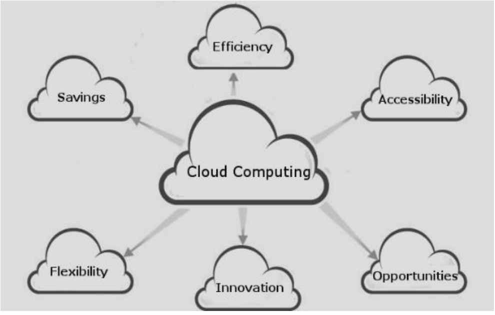

Fig.1: Cloud Computing Advantages/Needs

II. OVERVIEW OF TPA (THIRD PARTY AUTHENTICATION)

Third Party Authentication is also an access control procedure which was proposed long back. According to this mechanism, the users of the cloud have a role in the cloud [4]. The access is given to the user for a particular resource based on his role in the cloud. A user can have a single role or multiple roles. The third party based access policy is being used in many environments. This model has many advantages over other access control models. But there are many disadvantages like there is no detailed information about the role of a user. Many other access models like attribute based access control, cypher text attribute-based encryption were developed later.

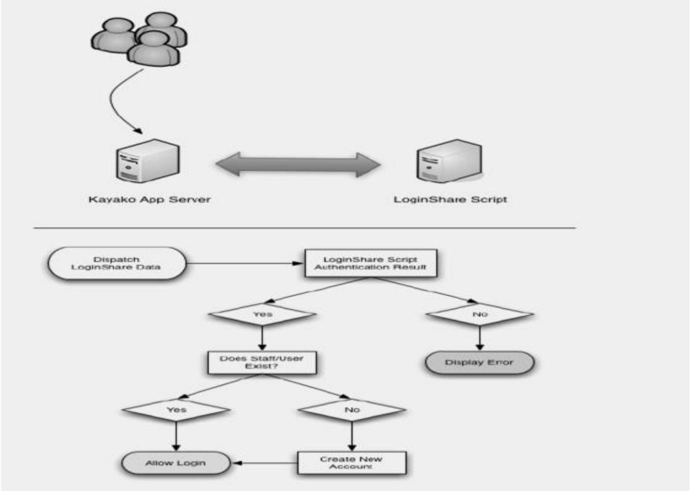

Fig.2: Third Party Authentciation Architecture

Access control is the progression of preventive the access to the system resources for authorized people, processes or other system mechanisms. Access controller is one of the essential issues of information security. Third party Authentication comes beneath access [5] control model which is a bendable and scalable access control model that governs accesses based on user roles and permissions. Role introduces a level of access control in mapping between users to privileges. Users can undertake a number of roles, and these characters are mapped to privileges.

III. CHARACTERISTICS OF THIRD PARTY AUTHENTICATION

1) In withdrawal mode, action a is suspended.
2) Third Party Authentication is transitory [6].
3) Third Party Authentication segregated and
4) Action a is restored when it gets authorized by a lower threat level (under rollback, restore mode) [7].

IV.RELATED WORK

Anil L. Pereira(et.al), 2011 In this paper shows how existing security standards can be [8] leveraged for the description and organization of TPA policies with the purpose to allow disparate applications, systems and refuge domains to interoperate. The extensible Access Control Mark-up Language can be used for policy specification and management across disparate establishments and the Retreat Assertion Mark-up Language can be used for authentication and agreement assertions across the same. Both principles can be leveraged to facilitate procedure Management and enforcement, and delegation of rights. **Wei Li (et.al), 2012** in this [9] paper discusses cloud calculating and its related safety risks, with a focus on access control. As a traditional access control mechanism, role-based access control model can be used to instrument several significant security principles such as least privilege, separation of duties, and data abstraction. This paper shows an on-going effort by sanitizing entities in TPA used for cloud computing, and additional discusses their security suggestions. **Wenkang Wu(et.al), 2013** In this paper, they study sequential restrictions and role-based constraints, and recommend Temporal [10] Constraint Consistency Problem. They study the computational difficulties of TCCP in different subcases and produce a valid assignment to satisfy all the constraints, and then reduce them into general P, NP and NP-Hard problems. **Zhu Tianyi(et.al), 2011** In this paper descried as , coTPA importantly improves the authorization process and user Knowledge [11] by reducing the redundant process of establishing secure connection and setting up multi-level cache, decreases the space complexity and time difficulty of access control system.

V. MODEL OF THIRD PARTY AUTHENTICATION

To be kept cloud as secure against attacker the TPA models support different authorization policies through the appropriate role configuration. The primary references models of TPA are TPA0, TPA1, TPA2 and TPA3 [3]. TPA0: The TPA 0 could be the simplest base model and it contains core concepts regarding the TPA architecture.

It's the minimum requirement for almost any system that maximum utilizes features of TPA. Users roles, and permissions would be the various important entity sets, hence the relations among these entities are defined by Permission Role and User-Role Assignment [2]. These relations and sets would end up being the main concepts associated with TPA. A cloud user might be member of several roles and each role can have several users. A cloud user can access numerous sessions within a session. So cloud user can access set of roles but each session applicable to only one user. Permission might be allocated to many roles and a task will surely have numerous permissions.

TPA1: This model includes the concept of Role hierarchies. These Role hierarchies are vital concept for formatting the roles to users to represent the authorize organization and responsibilities. TPA2: This model enhances the TPA 1 Model by adding constraints as well as restriction over the limit over the amount of users per role for all the safety purpose [6].

TPA2 introduces the idea of constraints. TPA adds static (not pertaining to sessions) and dynamic (pertaining to sessions constraints between core concepts [2]. Constraints are considered to achieve the primary motivation for TPA, because constraints are mechanism to set up higher-level organizational mechanism. Constraints may be added to Permission-Role Assignment, User-Role Assignment and Session [4].

TPA3: It includes all features of TPA0, TPA1 and TPA2, so it is called a basic model of TPA. TPA3 integrate TPA1 and TPA2 to merge both constraints and role hierarchy In this model constraints may be applied to the role hierarchy apart from the constraints in TPA2. The below figure shows base model of TPA.

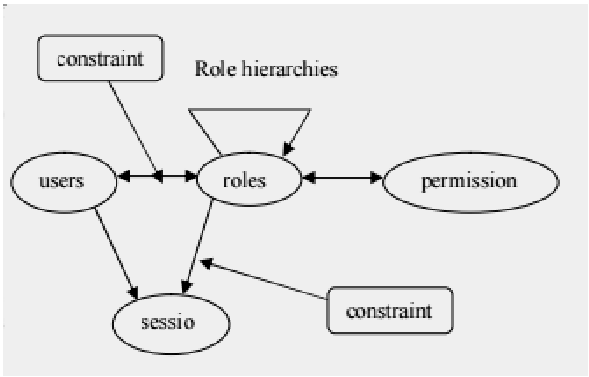

Fig.3 TPA model

VI. CONCLUSION

Third party Authentication in cloud is leading research area which will improve the security on user's information that is saved in cloud environment. Ensuring role access control in cloud platform improves security. In this paper we have studied TPA method that is used in past and current. A comprehensive and description of analysis of TPA provide the importance of role based access control in cloud to guarantee the protection of user's information.

VII. REFERENCES

[1] 1. Ranganathan, Vidya, and Guha P. Venkataraman. "Object Isolation for Cloud with DOMAIN RBAC." Cloud Computing in Emerging Markets (CCEM), 2012 IEEE International Conference on. IEEE, 2012.

[2] Wang, Wenhui, et al. "The design of a trust and role based access control model in cloud computing." Pervasive Computing and Applications (ICPCA), 2011 6th International Conference on. IEEE, 2011.

[3] Subashini, Subashini, and Veeraruna Kavitha. "A survey on security issues in service delivery models of cloud computing." Journal of network and computer applications 34.1 (2011): 1-11.

[4] Balamurugan, B., E. Durga Chowdary, and S. Linkesh. "A Combined Architecture for RBAC and DAC for Inter-cloud Communication." Eco-friendly Computing and Communication Systems (ICECCS), 2014 3rd International Conference on. IEEE, 2014.

[5] Rajesh, K., and Amiya Nayak. "Modified BTG-RBAC model for SaaS." Cloud Computing Technologies, Applications and Management (ICCCTAM), 2012 International Conference on. IEEE, 2012.

[6] Sirisha, Avvari, and G. Geetha Kumari. "API access control in cloud using the Role Based Access Control Model." Trendz in Information Sciences & Computing (TISC), 2010. IEEE, 2010.

[7] Lindqvist, Hakan. "Mandatory access control." Master's Thesis in Computing Science, Umea University, Department of Computing Science, SE-901 87 (2006).

[8] Karaboga, Dervis, and Bahriye Basturk. "A powerful and efficient algorithm for numerical function optimization: artificial bee colony (ABC) algorithm."Journal of global optimization 39.3 (2007): 459-471.

[9] Pereira, Anil L. "RBAC for high performance computing systems integration in grid computing and cloud computing." Parallel and Distributed Processing Workshops and Phd Forum (IPDPSW), 2011 IEEE International Symposium on. IEEE, 2011.

[10] Li, Wei, et al. "A refined RBAC model for cloud computing." Computer and Information Science (ICIS), 2012 IEEE/ACIS 11th International Conference on. IEEE, 2012.

[11] Wu, Wenkang, Zhuo Tang, and Renfa Li. "On the complexity of authorization of temporal rbac in cloud computing service." Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on. IEEE, 2013.