International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 07, July-2015

Enhanced Framework for Authentication as a Service to Ensure Security in Public Cloud Environment

N. Veeraragavan
Research scholar
Dept. of Computer Science,
St. Joseph's College (Autonomous),
Tiruchirappalli.

Dr. L. Arockiam
Associate Professor in Computer Science, St. Joseph's College (Autonomous),
Tiruchirappalli.

S. Monikandan
Asst. Prof, Christhuraj Institute of Computer Application,
Christhu Raj College,
Panjappur, Trichy-12,

***Abstract* – Cloud computing is sprinkling widely the user and cloud service providers are enabled to use various resources or services inexpensively and simply without owning all the resources required. Cloud provides cost effective resource utilization and also it provides reliable and flexible usage of computing needs. IT companies are interested in migrating to cloud environment. Cloud computing provides various advantages such as lower computer costs, improved performance, data reliability, unlimited storage etc. Beyond the advantages of cloud computing, it has many issues in security, trust, scalability etc. Among these issues, security is the main issue in cloud environment. To solve this issues in cloud, this paper proposed a novel framework for Authentication as a Service (AaaS) in cloud computing. Authentication is provided as a Service to the cloud users. This paper also describes working components in the AaaS framework. It is an added advantage for Cloud Service Provider (CSP), when this framework is being adopted.**

Keywords - Authentication; Cloud Computing; Encryption; User Authentication System (UAS); Server Granting System (SGS);

I. INTRODUCTION

Cloud Computing can be defined as the utility or subscription based service since it uses "Pay as you go" principle [1]. It delivers various IT resources as services on demand. The Cloud user must have an internet connection to access the Cloud services [3]. Cloud computing is a computing environment center on clients and to access the programs or documents stored correspondingly in servers [4].

A. General Cloud Architecture

Cloud architecture allows users to access any type of services such as software as a service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) [5]. Cloud Service Provider (CSP) provides all the services to the users. Figure 1 shows the general architecture in which CSP provides computing resources to their users.

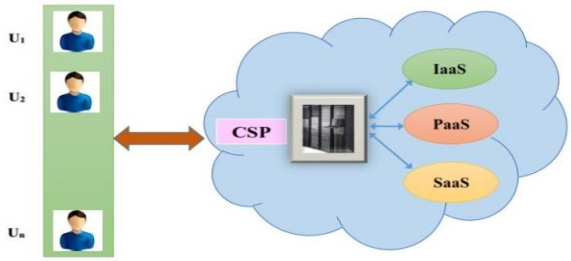


Figure 1. General Cloud Architecture

Nowadays, Cloud computing controls both the users and developers. Cloud computing is the best preferable platform for those who are involved in on-line businesses [2]. Cloud provides many advantages to the enterprises, but the same time it has different security issues [6]. As a result, data of files are stored in the cloud then open to all [7]. Therefore, all the data and files can be handled by other user of the cloud system. It leads that all files or data become more susceptible to attack [8]. As a result, it is easy for an intruder to access, misuse and abolish the original form of data [9]. Another problem with the cloud system is that an individual may not have control over the place where the data required being stored [10]. To address these entire problems in cloud environment, there is a need to have a secured and protected framework to ensure the security in the cloud. Thus, this paper proposes a secured authentication framework to ensure the security in cloud environment.

II. RELATED WORK

This section describes the several existing works carried out related to cloud security. Hongwei Li et al [11]. proposed an Identity-Based Hierarchical Model for cloud computing (IBHMCC) and its corresponding encryption and signature schemes, presented an Identity Based Encryption (IBE) and Identity Based Signature (IBS) schemes for IBHMCC for cloud computing and services. Using these IBE and IBS schemes, an Identity Based Authentication for Cloud Computing (IBACC) is proposed.

The author also concluded, SSL Authentication Protocol is of low efficiency for Cloud services and users.

Hyokyung et al [12]. discussed various technologies of access control and user authentication problems inside. The Access control is the technology that controls a process in the operating system not to approach the area of another process. There are DAC (Discretionary Access Control), MAC (Media Access Control), and RBAC (Role-Based Access Control). Weakness of User Authentication Technology in Cloud Computing such as Id/password, Public Key Infrastructure, multi-factor authentication, SSO (Single Sign On), MTM (Mobile Trusted Module), and i-Pin. We need a proper user authentication service model and protocol for Cloud Computing should be designed and developed.

Hyosik Ahn et al. [13] proposed the platform for user authentication using provisioning in Cloud computing environment. User authentication platform using provisioning first authenticates by using ID/Password, PKI, SSO, etc. which a user input. Second, it authenticates with Authentication Manager through the user profile and patterns and stores the changes of the state via Monitor. When using Cloud Computing services, to solve the inconvenience of user authentication, user's information is stored in the User Information. The proposed platform architecture analyses user information and authenticates a user through user profile.

M.S. Shashidhara et al. [14] proposed a multi-user authentication framework for cloud computing. In this framework, user identification is verified before logging into the cloud server. Proposed protocol can resist intruder attack and DOS (Denial of Service) attack.

Sultan Ullah et al. [15] proposed multistep, multifactor authentication approach is employed for the authentication and authorization of the client. This scheme increases the confidentiality and integrity of the data. This model proposed the combination of cryptography and access control to keep the data safe from vulnerabilities.

III. MOTIVATION

From the above readings and concerns, it is realized that the importance of security in cloud. Security is maintained with various measures such as Authentication, Authorization, Integrity and Confidentiality etc. Among them, authentication is an important security parameter, because once the authentication is done well then other parameters are ensuring the security in the cloud environment. Following factors are motivated me to propose the Authentication Framework.

- To protect unauthorized usage of cloud services
- To control the user by centralized AaaS
- To provide the better authentication mechanism to CSP

IV. PROPOSED FRAMEWORK

Figure 2 represents, the proposed framework of AaaS (Authentication as a Service) to the cloud environment.

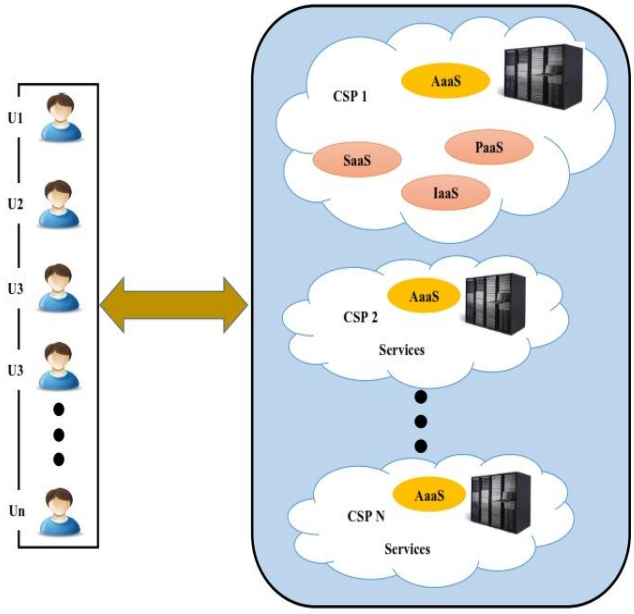


Figure 2. Proposed Framework for AaaS

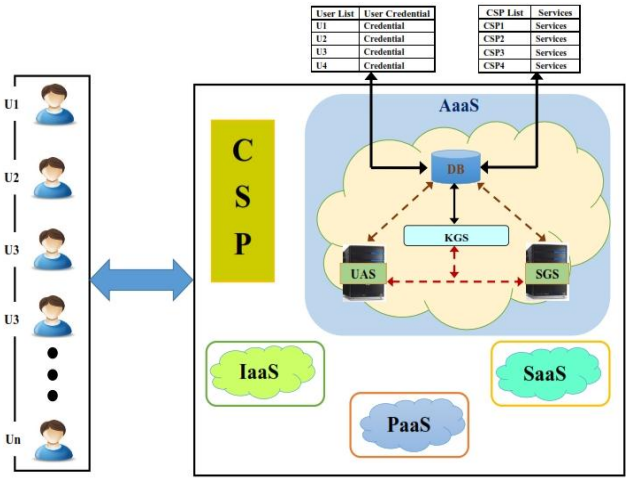
The AaaS include as a one of the service in CSP. Cloud users want to access any resources from the cloud. Before that, AaaS checks the user credential. If the user credentials are valid, CSP allows to access the resources by the cloud user. Otherwise requests are denied.

A. User Authentication Mechanism

Figure 3 represents the proposed framework for User Authentication Mechanism (UAM) of AaaS. This section provides the detailed overall process of proposed framework. This consists of two major components. First component denotes User and other component is AaaS. User is a kind of person who can access the resources from the cloud environment. AaaS has overall authentication process of entire cloud system AaaS in one of the cloud services. It's mainly used to validate the cloud user identities. Only authorized persons can access cloud services. AaaS consists of the following components:

- *UAS (User Authentication System):* It receives the user registration details and stores all the information in the database. Based on the user profile along with the key, it generates the password. Then the password is sent to the cloud user through his mail id and also stored in the database. It checks the user login details which are provided by the cloud user. If the user information are valid, UAS sends the User Authentication Certificate (UAC) to the cloud user.
- *KGS (Key Generation System):* KGS generates the key and send along with User Authentication Certificate (UAC) and Service Granting Certificate (SGC). The key generation is based on the encryption techniques.
- SGS *(Service Granting System):* Service Granting System (SGS) checks the User Authentication Certificate, if the certificate are valid then generates new certificate of Service Granting Certificate (SGC) along with the session key and type of service.

- *DB (Database):* Database contains user profile details, all the keys which are generated by KGS and list of services



which are provided by the CSP.

Figure 3. Proposed User Authentication as a Service in Public Cloud

B. Working Procedure of Proposed Mechanism

Step 1. Cloud user enters all the information like firstname, lastname, date of birth, mailId, mobile number, and address through Registration Phase.

Step 2. UAS sends password through the user mail id, which is generated using the encryption technique.

Step 3. Cloud user enters the information of user name and password in the login page and requests the User Authentication certificate.

Step 4. User Authentication System (UAS) sends the User Authentication Certificate (UAC) along with the key to the cloud user.

Step 5. Cloud User requests Service Granting Certificate (SGC) using the User Authentication Certificate (UAC) to Service Granting System (SGS).

Step 6. Service Granting System (SGS) check the user certificate. If the information is valid then SGS sends the Service Granting Certificate (SGC) along with session key + type of service, otherwise access is denied.

Step 7. Using Service Granting Certificate cloud user requests service from any CSP.

Step 8. If the SGC is valid CSP provides service to the cloud user.

Figure 4 represents the proposed User Authentication Mechanism (UAM). The users provide their information like FName, LName, DOB, EmailID, Mobile Number and Address in the registration phase. The User Authentication System (UAS) sends the password through the user mail account by using encryption technique. The cloud user requests User Authentication Certificate (UAC) through login phase with multi-factor authentication. The User Authentication System (UAS) checks the user credential. If it is valid then User Authentication System (UAS) sends User Authentication Certificate (UAC) to the user along with the key. Cloud user requests the Service Granting Certificate (SGC) to the Service Granting System (SGS). The Service Granting System (SGS) checks the UAC and user credential. If the information is valid then Service Granting System (SGS) sends the Service Granting Certificate (SGC) to the cloud user. Then the cloud user requests the service with the help of Service Granting Certificate (SGC) to the cloud service provider. Finally, Cloud Service Provider (CSP) checks the user information and service details. User is able to access the resources from the Cloud, if UAC and SGC are valid otherwise, access is denied.

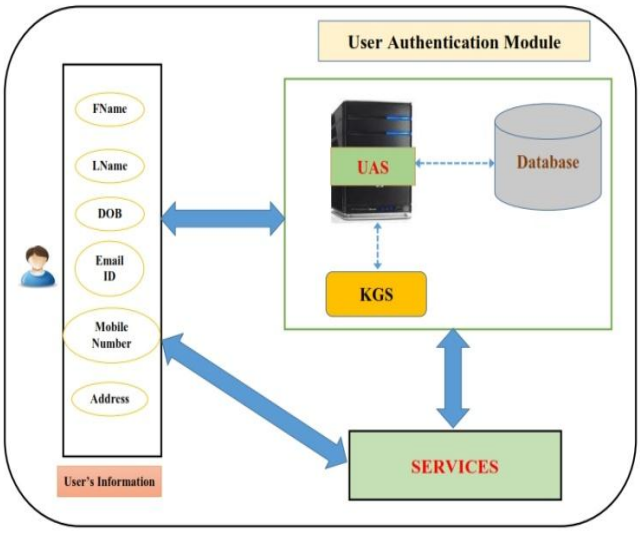


Figure 4. Proposed User Authentication Mechanism

C. Working Procedure of User Authentication Mechanism

Registration Phase:

Step 1. Users enter their details such as FName, LName, DOB (Date Of Birth), Email ID, Mobile Number and Address during registration.

Step 2. Taken only three information from the database such as DOB (number only), mail id, and mobile number. Example: 01011982ragavan@gmail.com 9894915046

Step 3. Key Generating System (KGS) generates key of random number system and sends to the UAS.

Step 4. UAS generates password using user information + random number with the following processes:

a) Convert the user information into binary format
b) Convert the random number into the binary format
c) Take left rotate of binary format of user information values
d) Take right rotate of binary format of random number values
e) Add these two binary values using the XOR operation
f) Covert the binary format into ASCII values

Step 5. ASCII (Password) values sends to the user through the user mail id.

Login (Multi-factor Authentication) Phase:

Step 1. Users enter their username and password through the Login page.

Step 2. In, Login page, three authentication parameters are displayed, the user provides the following information, such as (Multi-factor authentication) Username, Password and Image captcha.

Step 3. UAS checks these three information. If the user information are valid, then UAS sends the UAC to cloud user otherwise user request is denied

V. ADVANTAGES OF PROPOSED FRAMEWORK

The proposed framework satisfies the security concern in cloud environment.

- Users are verified with their credential.
- Authentication is provided as a service to users.
- Users can trustworthy use the cloud environment.
- Unauthorized access is prevented in the framework.
- This framework helps the providers to improve their business

VI. CONCLUSION

This paper discussed about basic concepts of cloud computing and security. Security concerns such as Authentication, Authorization, and Integrity etc. This paper discussed several existing authentication frameworks. Authentication is the important parameters among other security aspects. This paper proposed a new Authentication as a Service (AaaS) framework to entire cloud computing environment. If the user wants to access any resources from the cloud, they must get proper User Authentication Certificate (UAC) and Service Granting Certificate from AaaS in a CSP. Later, this work will be extended to implement in mathematical model.

REFERENCES

[1] Wayne Jansen, Timothy Grance, "Guidelines on Security and Privacy in Public Cloud Computing", *NIST Special Publication*, (2011).

[2] Peter Mell and Tim Grance, The NIST Definition of Cloud Computing, Technical Report-800-145, Version 15, National Institute of Standards & Technology, Gaithersburg, MD, United States, 2011.

[3] *Yashpal Kadam*, "Security Issues in Cloud Computing A Transparent View", *International Journal of Computer Science Emerging Technology*, Vol. 2, No. 5, pp. 316-322, (2011).

[4] Arockiam, L., Monikandan, S., Parthasarathy, G., (2011), 'Cloud Computing: A Survey', *International Journal of Internet Computing*, Volume 1, Issue 2, ISSN: 2231 – 6965, pp 26-33.

[5] Longji Tang, Jing Dong, Yajing Zhao, Liang-Jie Zhang, Enterprise Cloud Service Architecture, IEEE 3rd International Conference on Cloud Computing, pp. 27-34.

[6] Arockiam, L., Monikandan S., (2013), 'Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm', *International Journal of Advanced Research in Computer and Communication Engineering*, Volume 2, Issue 8**,** ISSN: 2278-1021, August, pp 3064-3070.

[7] N. Veeraragavan and Edel Josephine Rajakumari, "Security Issues and Solutions in Cloud Computing- A Survey", *National Conference on Advanced Computing*, (2013)

[8] Arockiam, L., Monikandan, S., (2014), 'Efficient Cloud Storage Confidentiality to Ensure Data Security', *IEEE International Conference on Computer Communication and Informatics*, ISBN: 978-1-4799-2352-6, January, pp 355-359.

[9] N. Veeraragavan, S. Monikandan, Dr. L. Arockiam, "A Novel Framework for an Authentication as a Service in Public Cloud Environment", *Proceedings of National Conference on Data Science and Engineering (NCDS 2014), Elsevier*, (2014).

[10] Ramgovind S, Eloff MM and Smith E, The Management of Security in Cloud Computing, Proceedings of IEEE International Conference Information Security for South Africa, 2010, pp. 1-7.

[11] Hongwei Li, Yuanshun Dai, Ling Tian and Haomiao Yang, "Identity-Based Authentication for Cloud Computing", *Springer*, pp. 157–166, (2009).

[12] Hyokyung Chang and Euiin Choi, "User Authentication in Cloud Computing", *Springer-Verlag Berlin Heidelberg*, pp. 338–342, (2011).

[13] Hyosik Ahn, Hyokyung Chang, Changbok Jang, and Euiin Choi, "User Authentication Platform Using Provisioning in Cloud Computing Environment", *Springer*, 2011.

[14] M.S. Shashidhara, Jaini.C.P,K.Dayana Devi, "A Study on Multi-User Authentication Framework and Security problems for Cloud Computing", *Journal of NanoScience and NanoTechnology*, Vol. 2, Issue 3, pp.347-352, (2014).

[15] Sultan Ullah, Zheng Xuefeng and Zhou Feng, "TCLOUD: A Multi – Factor Access Control Framework for Cloud Computing", *International Journal of Security and Its Applications*, Vol. 7, No. 2, pp.15-26, (2013).