IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 3, March 2016

Enhanced Authentication Mechanism for Securing the Cloud Services using AaaS

N. Veeraragavan[1], Dr. L. Arockiam[2]

Research Scholar, Dept. of Computer Science, St. Joseph's College (Autonomous), Trichy, Tamil Nadu, India[1]

Associate Professor, Dept. of Computer Science, St. Joseph's College (Autonomous), Trichy, Tamil Nadu, India[2]

Abstract: Cloud computing is an innovative concept that has carried a paradigm shift into the IT industries. Security is the most critical issue in cloud computing. In security, authentication is the one of the important parameters to be addressed. Authentication is a key mechanism to establish proof of identities to get the sources from any type of system. Traditional security system does not provide enough security for the data which is stored in the cloud computing environment. This paper proposes a mechanism to improve the security in cloud using Authentication as a Service (AaaS). The paper provides a brief survey of existing authentication mechanisms. The proposed novel AaaS is used to ensure security in public cloud environment. The proposed mechanism is provided as an authentication service from a Cloud Service Provider (CSP). The AaaS identifies the users verify different level of authentication.

Keywords: Cloud Computing; Authentication; User Authentication System (UAS), Key Generating System (KGS).

I. INTRODUCTION

Cloud computing is an internet based computing, whereby shared resources, software, and information are provided to computers and other devices on demand basis. According to the definition of (NIST), "cloud computing is a delivery model that enables convenient instant network access to a pool of shared configurable computing resources that can be quickly provisioned and released. Cloud computing has several characteristics such are resource pooling, rapid elasticity, measured services, on demand self-service and distributed network access" [1].

Cloud computing is a new technology, which is used presently in most of IT industries. It is one of the emerging technologies of modern computing because it has many advantages such as pay-per-usage, large storage capacity, scalability and so on. Figure 1 Represents, how the communication are interacted with cloud user and CSP. Cloud computing consists of three services such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) [2].

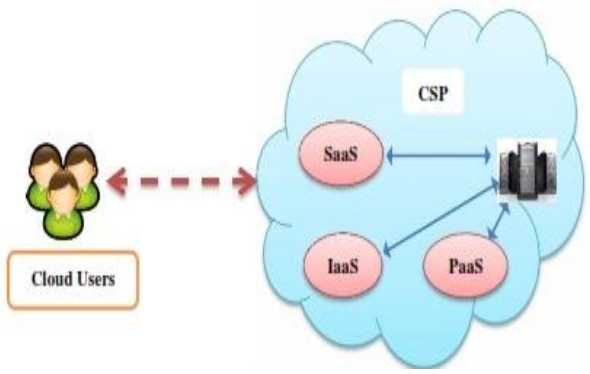

Fig. 1 Abstract view of Cloud Computing Environment

Cloud computing provides various IT resources as services on demand basis. The cloud user must have an internet connectivity to access the resources from the cloud environment [2]. In early research few authors discussed [3] [4] the security issues and challenges as data storage safety, application safety, data sharing safety concerns between CSPs and cloud user in distributed environment [5]. Cloud computing like a data centre, user information / resources moving to clouds, may involve numerous security issues and challenges such as authentication, integrity, confidentiality, virtualization, availability, auditing, reliability, trust of data and data loss or data theft [6].

User authentication and access control is representative security technologies for any type of application [7]. Security is a process to restrict, to protect against fraud, damage, theft, incursion of privacy, unlawful entry and other occurrences caused by premeditated action. In traditional security user needs to authenticate using the ID/password, Public Key Infrastructure, multi-factor authentication, Single Sign On, One time Pin etc. [8]. Traditional approaches addressing security is not enough for cloud environment. It is necessary to have a proper authentication mechanism to address the security issues in the cloud environment.

This paper is organized as follows section II discusses some of the existing literatures, section III and IV deal problem definition and motivation respectively. Section V and VI discuss methodology and objective of the paper respectively. Section VII is the proposed authentication service for cloud. Section VIII deals with the advantages of the AaaS and finally section IX is concludes the paper.

II. RELATED WORK

This section describes the various existing works carried out related to user authentication in cloud environment. Satish kumar et al. [9] proposed a multi-authentication framework for executing secure transaction in a cloud environment. In this proposed scheme, authentication process is carried out in two levels. This framework is

divided into two tier, first tier authentication uses the encryption decryption mechanism which is used normal authentication schemes. The second tier authentication requires the password which is received by user's personal device like mobile which have a unique id (IMEI - International Mobile Equipment Identity) which will be generated from cloud server and sent over to the user's personal device. They analysed that the proposed scheme uses the probability of success. Disadvantage of this scheme that in case user personal device is lost or maybe stolen by someone to illegally access the cloud data of that user.

S Leeet al. [10] proposed a mutual authentication that allowed cloud user and cloud remote server to authenticate each other as believed it is crucial to protect not only the server but also the legitimate users from security threats. like one way authentication, client must prove its identity to server and the server must prove its identity to client before any access have been granted or any application traffic is sent over the client-server connection. This proposed mutual authentication scheme is to minimize the cloud computing security risks such as man-in-the-middle attack, identity theft, side channel attack, and phishing attack. From the security analysis, its shown that this proposed scheme provides a robust and trustworthy mutual authentication between cloud user and CSP communicated over the internet. Performance analysis showed that this proposed framework has good efficiency and suitable for cloud computing.

Rui Jiang [11] pointed out the security vulnerabilities to the Choudhury et al's scheme, and presented the detailed attacks on the scheme. Then, based on some remote user authentication schemes such as Ku-Chen's scheme and Chen's scheme, then they applied the two-factor authentication technology to propose advanced secure user authentication framework which can overcome above security shortages. Without sending one time key through secure OOB (Out Of Band) channel, the new protocol is able to ensure that only legitimate users can access the cloud service based on smartcard. In addition, this advanced scheme can hold all the merits of the Choudhury et al's scheme. Formal security analysis, which is based on the strand space model and authentication test, proved that our proposed scheme is secure under standard cryptographic. Also, the simulation results illustrated that our advanced scheme is more efficient on the communication performance than other schemes.

Rohitash Kumar Banyalet al. [12], developed framework of Cloud Access Management (CAM) system which is authenticated the user based on multiple factors. Also using secret-splitting and encrypted value of arithmetic captcha is innovative factor for user authentication for cloud computing environment. The proposed framework shows the close agreement with the standard criteria for security

Jiangshan Yu et al. [13], introduced an efficient generic framework for three factor authentication. The proposed generic framework enhances the security of existing two-factor authentication schemes by upgrading them to three-factor authentication schemes, without exposing user privacy. In addition, they presented a case study by upgrading a secure two-factor authentication scheme to a secure three-factor authentication scheme. Furthermore, implementation analysis, formal proof and privacy discussion are provided to show that the derived scheme is practical, secure and privacy preserving.

Nan Chen et al. [14], first analyzed a user authentication framework for cloud computing proposed by Amlan Jyoti Choudhury et al and pointed out the security attacks existing in the protocol. Then this proposed an improved user authentication scheme. Our improved protocol ensures user legitimacy before entering into the cloud. The confidentiality and the mutual authentication of our protocol are formally proved by the strand space model theory and the authentication test method. The simulation illustrated that the communication performance of our scheme is efficient.

Prachi Soniet al.[15], proposed a new multi-factor authentication framework for cloud computing. In this paper the features of various access control mechanisms are discussed and a novel framework of access control is proposed for cloud computing, which provided a multi - step and multifactor authentication of a user. The model proposed is well-organized and provably secure solution of access control for externally hosted applications.

III. PROBLEM DEFINITION

Based on the above literature review, it is clear that authentication is the most important factor in the cloud security. Once the user enters into the cloud, then entire data have possibly to be hacked by the unauthorized users. It is needed to propose a new authentication mechanism to enhance the security in the cloud environment. The proposed IAaaS (Identity based Authentication as a Service)to comprises of three components, and are interrelated one another to protect from unauthorized users. This entire system is used to provide permission to access the cloud service for legitimate users.

IV. MOTIVATION

From the above readings and concerns, it is realized the importance of security in cloud computing. Security is maintained with various measures such as authentication, authorisation, integrity and confidentiality. Among them authentication is an essential security parameter, because once the authentication is fulfilled then other parameters are ensuring the security in the cloud. Following factors are the motivated concept to propose the authentication framework.

- Authentication protects the entry of malicious attacks.
- To improve the Cloud security by strengthening the authentication system.
- An efficient authentication system does not compromise the other security parameters, like confidentiality, integrity and etc...

V. OBJECTIVE

The objective of this paper is to propose an authentication mechanism to protect unauthorised access is cloud service.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 3, March 2016

VI. METHODOLOGY

The AaaS contains UAS and SGC. UAS generates UID, Password using key1 and also generates UAC and send to the user. The user decrypts the UAC and request the SGC from SGS. KGS generates the key1, key2 and key3. Fig. 2 and for 3 depict registration phase and user login and authentication phase.

A. Registration Phase:

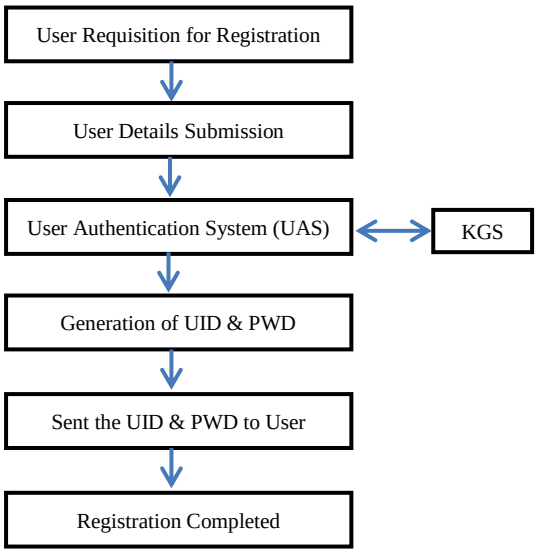

Fig. 2 Methodological diagram for Registration phase

B. Login and Authentication Phase:

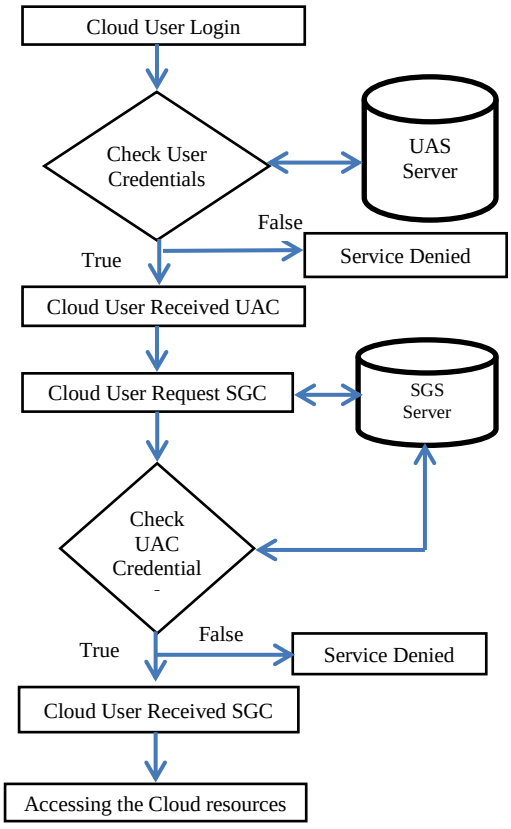

Fig.3 Methodological diagram for User login and Authentication

VII. PROPOSED AUTHENTICATION MECHANISM

Fig.1represents the abstract view of AaaS, as AaaS is one of the services in the CSP in cloud. Cloud user wants to access any type of resources from the cloud. CSP redirected to AaaS, and AaaS checks the user information. If the user information's are valid, CSP allows accessing the resources by the cloud user, otherwise user requests are repudiated.

Fig. 4 represents the expansion of AaaS framework in cloud CSP. This section provides the detailed overall view of the AaaS framework. This AaaS consists of three major components such as, UAS, KGS and SGS. Cloud user can access the resources from the cloud environment. If user wants to access from any resources from cloud, first user identifies whether it is privileged user or not. This process will take over the AaaS. CSP redirects to AaaS service. AaaS has overall authentication process for entire cloud system. AaaS checks user credentials with various levels. If user's credentials are valid in all the levels, AaaS allows to access the resources through the any kind of CSP. Otherwise cloud user request is declined.

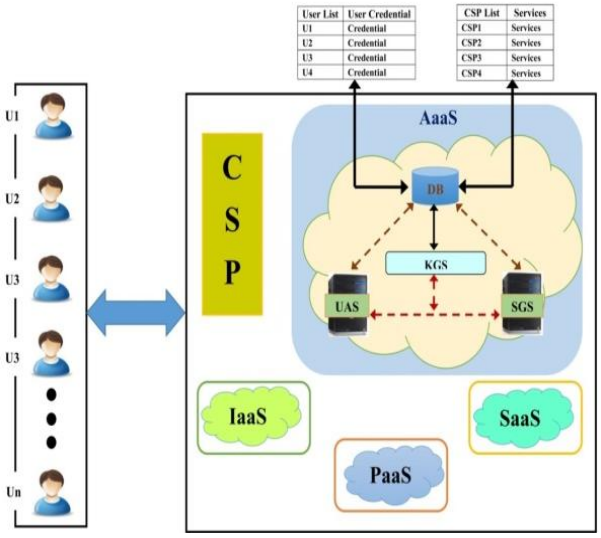

Fig.4 Overall view of Proposed AaaS in Cloud System [2]

A. Proposed AaaS Framework Components:

The following components are involved in the proposed AaaS framework:

AaaS – Authentication as a Service
UAS – User Authentication System
SGS – Service Granting System
KGS – Key Generating System
UAC – User Authentication Certificate
SGC – Service Granting Certificate
DB – Database
CSP – Cloud Service Provider

B. Procedures for Proposed AaaS:

Figure 5 explores the various processes involved in the proposed AaaS framework. This AaaS contains three major components such as UAS, SGS and KGS. In initial stage cloud users register their information to the UAS. UAS receives all the details of users and store in the

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 3, March 2016

database. UAS generates the UserID (User Identity) and password and sends to the users personal device or personal mail account. Using this UserID and password cloud user enters the login page. UAS receives UserID and Passwords, generates third authentication parameter of image captcha and sends to the user screen. Now cloud user enters the third authentication parameter and submits to the UAS. UAS checks all three information (UserID, password and image captcha) are valid, and then generate the UAC and sends to the cloud user. Using this UAC cloud user requests SGC to the SGS. SGS checks UAC, if the information are valid SGS generates SGC and sends to cloud user. At the same time AaaS sends the verification acknowledgement sent to the CSP, immediately CSP allows to access the services by the cloud user.

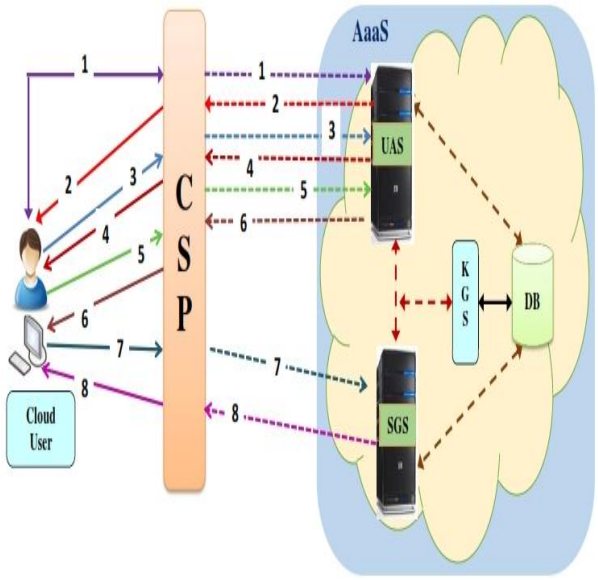

Fig.5 Procedures for AaaS

Figures 6 describes that Cloud User submits their details for registration such as First Name, Middle Name, Last Name, DOB, Gender, MobileNo, MailID, and stored in the Database. CSP directs the AaaS. AaaS has its three components such as UAS, KGS and SGS. UAS generates the UserID and Password based on the user profile along with a Key_1, which is generated from KGS. UserID and Password are encrypted by a Key_2 which is also generated from KGS and they are forwarded to the user. (Key_1, Key_2 are stored in Database). From login page, user submits that encrypted data as their UserID and Password (Sent to UAS). UAS takes any two images from the Databases and makes the image captcha and sends to the cloud user. Then, image captcha (pop-up window) will appear on user screen, and then user enters the name of the images and submits to UAS. Now, UAS decrypts user credentials such are UserID, Password and captcha using Key_1 and Key_2 taking from UAS Database, and checks the decrypted UserID, Password and captcha with original information's which are stored in Database in UAS. If UserID, Password and captcha are valid then UAS generates UAC and forwards to user. Using with UAC, user requests SGC to SGS. Now, SGS checks the UAC with the help of UAS Database, if the information is valid, SGS generates SGC and forwards to the user. Suppose, SGC is not valid, then SGS declined the user service request. Fig.6 represents the Sequential Diagram of Proposed AaaS.

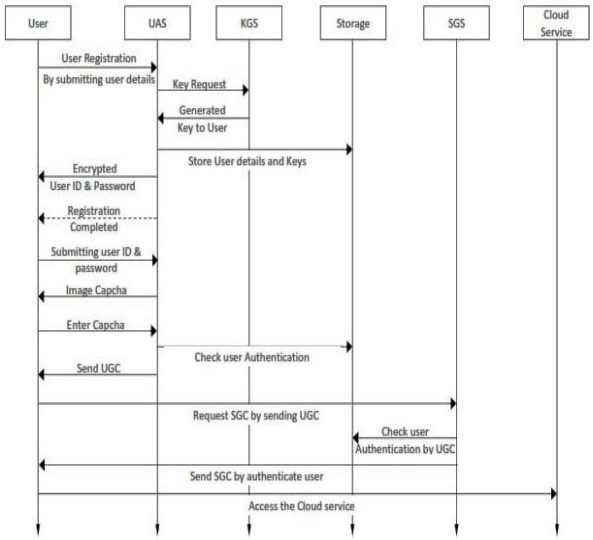

Fig. 6Sequential Diagram of Proposed AaaS

VIII. ADVANTAGES OF PROPOSED AAAS

The proposed framework satisfies the security concern in cloud environment

- ✓ AaaS framework is used for User Authentication in Cloud environment.
- ✓ The proposed framework satisfies the security concern in cloud environment.
- ✓ Users are verified with their credential.
- ✓ Authentication is provided as a service to users.

IX. CONCLUSION

Cloud computing is a recent mode of delivering computing resources which introduces a lot of benefits to the cloud users. Despite advantages, it also brings in new security uncertainties such as data security, confidentiality, and integrity. The proposed Authentication as a Service (AaaS) is minimized in security attacks such as man-in-middle attack, identity theft etc. UAC and SGS are the two important components contributed in the entire authentication procedure. Different security analysis is conducted in the proposed framework. From the security analysis, it's shown that proposed AaaS provides a strong and trustworthy authentication between cloud user and CSPs. Hence Authentication as a service is provided by a separate cloud service provider. From performance analysis its shown their our proposed authentication service has good efficiency and suitable for public cloud environment.

REFERENCES

[1] Mell P and Grance T, "The NIST definition of cloud computing", September 2011.
[2] N. Veeraragavan, Dr. L. Arockiam and S. Monikandan, "Enhanced Framework for Authentication as a Service to Ensure Security in Public Cloud", International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 4 Issue 07, July-2015, pp 442-445.

[3] Michael E.Whitman In defense of the realm: Understanding the threats to information security International Journal of Information Management, 24, 2004, pp.43-57.
[4] Dimitrios Zissis , Dimitrios Lekkas, Addressing cloud com-putting security issues Future Generation Computer Systems, 28, 2012, pp.583-592.
[5] Arockiam L. and Monikandan S., Data security and privacy in cloud storage using hybrid symmetric encryption algorithm. International Journal of Advanced Research in Computer and Communication Engineering, 2(8), pp.3064-3070, 2013.
[6] G. Kumaresan, N. Veeraragavan, Dr. L. Arockiam, "A Study of User Authentication Techniques in Cloud Computing", Journal of Emerging Technologies and Innovative Research (JETIR) (ISSN-2349-5162), Volume 2, Issue 8, August 2015, pp. 3309-3314.
[7] HyosikAhn, Hyokyung Chang, Changbok Jang, and Euiin Choi, "User Authentication Platform Using Provisioning in Cloud Computing Environment", Springer-Verlag Berlin Heidelberg 2011, ACN 2011, CCIS 199, pp. 132–138.
[8] Hyokyung Chang and Euiin Choi, "User Authentication in Cloud Computing", Springer-Verlag Berlin Heidelberg 2011, UCMA 2011, Part II, CCIS 151, pp. 338–342.
[9] Satish kumar, Anita Ganapati, "Multi-Authentication for Cloud Security: A Framework", International Jouranl of Compuer Science & Engineering Technology (IJCSET), ISSN: 2229-3345, Vol. 5, No. 4, April 2014.
[10] Shirly Lee, Tae Yong Kim and Hoon-Jae Lee, "Mutual Authentication Scheme for Cloud Computing", Future Information Communication Technology and Applications, Springer, chapter 17, 2013, pp 149-157.
[11] Rui Jiang, "Advanced Secure User Authentication Framework For Cloud Computing", International Journal Of Smart Sensing And Intelligent Systems Vol. 6, No. 4, September 2013.
[12] Rohitash Kumar Banyal, Pragya Jain and Vijendra Kumar Jain, "Multi-factor Authentication Framework for Cloud Computing", IEEE Computer Society, Fifth International Conference on Computational Intelligence, Modelling and Simulation, pp 105-110.
[13] Jiangshan Yu, Guilin Wang, Yi Mu, and Wei Gao, "An Efficient Generic Framework for Three-Factor Authentication with Provably Secure Instantiation", IEEE, 2013.
[14] Nan Chen and Rui Jiang, "Security Analysis and Improvement of User Authentication Framework for Cloud Computing", Journal of Networks, Vol. 9, No. 1, January 2014, Pp 198-203.
[15] PrachiSoni and MonaliSahoo, "Multi-factor Authentication Security Framework in Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 1, ISSN: 2277 128X, January 2015.

BIOGRAPHIES

N. Veeraragavan received his Master's degree in Computer Science from Bharathidasasn University, Tiruchirappalli, India. Currently, he is a Ph.D. research scholar in the Department of Computer Science at St. Joseph's College (Autonomous), Tiruchirappalli affiliated to Bharathidasan University, India. He has skilled himself with 8 years of experience in teaching and 3 years of experience in research. He has published six Research Papers in International Journals with Impact Factor. His main area of research is Cloud Computing Security. He has attended several National and International Conferences and workshops.

Dr. L. Arockiam is working as Associate Professor in the Department of Computer Science, St. Joseph's College, Tiruchirappalli, Tamil Nadu, India. He has 26 years of experience in teaching and 18 years of experience in research. He has published more than 235 research articles in the International & National Conferences and Journals. He has also presented 3 research articles in the Software Measurement European Forum in Rome, Bali and Malaysia. He is also the Member of IEEE, Madras Section. He has chaired many technical sessions and delivered invited talks in National and International Conferences. He has Co-authored 5 books. His research interests are: Cloud Computing, Big Data, Cognitive Aspects in Programming, Data Mining and Mobile Networks. He has been awarded "Best Research Publications in Science" for 2009, 2010, 2011 & 2015 and ASDF Global "Best Academic Researcher" Award from ASDF, Pondicherry for the academic year 2012-13 and also the "Best Teacher in College" award for the year 2013 & 2014