IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

A Novel Framework for Authentication as a Service (AaaS) in Public Cloud Environment

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 is the environment for elastic computing resources and provides reliable storage by maintaining the data in different datacentres. Main concern in the cloud is maintaining security by protecting the unauthorized access in the cloud environment. Authenticating the user access is the most important task in cloud. This paper proposes a novel framework, namely VEARAaaS, for authenticating the user for accessing the cloud services. This framework has different Authentication as a Service (AaaS) to protect the illegal users. The framework includes three major components such as Authenticator, Encryptor and Key generator. Authenticator is a cloud and it has two authentication mechanisms as a service to the cloud users. Encryptor is another cloud service for encrypting and decrypting the user credential in the cloud environment. Key Generator is also a cloud service which is used to generate for encryption and authentication service. The proposed framework protects the user by its functionality of verification. Hence, this framework provides better authentication system for the user to access their cloud service at anytime and anywhere.

Keywords: Cloud Computing; Security; Authenticator; Encryptor; Key Generator; Authentication Service.

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 NIST definition, "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 having several characteristics such as resource pooling, rapid elasticity, measured services, on demand self-service and distributed network access" [1].Cloud computing delivers various IT resources as services on demand. The Cloud user must have an internet connection to access the Cloud services [2]. Cloud computing is a computing environment center on clients and to access the programs or documents stored correspondingly in servers [3].

A. Cloud Architecture:

Cloud computing is a recent technology, which is used presently in many of IT industries. It is one of the emerging technology of modern computing because it has many advantages such as pay-per-usage, large storage capacity, scalability and so on. Fig 1 represents, how the communications are interacted with cloud user and Cloud Service Provider (CSP). Cloud computing consists three services such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) [4].

Cloud is deployed in four models public cloud, private cloud, Community Cloud and Hybrid Cloud. Cloud is mainly differ from existing computing paradigm by the following characteristics,

- On-Demand Access
- Broad Network Access
- Resource Pooling
- Elasticity
- Scalability
- Metering Service

Apart from this advantages and characteristic cloud has many issues, among that security is the most important concern in the cloud environment [5].

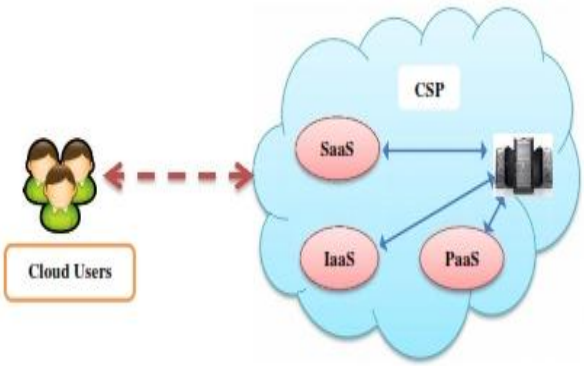

Fig. 1 Cloud computing Architecture

II. RELATED WORK

There are huge number of researches which are undergoing in the field of cloud computing security. Some of the related work on cloud authentication is listed in the section. Sunghyuck Hong et al. [6], said group communications are becoming popular by explosively increased Internet usage, and there are various group communications on Internet applications such as video conferences, on-line text chatting programs, online games and gambling. However, the conventional group key

agreement protocols are only focused on how to minimize the computational overhead by concentrating on generating the common group key efficiently. As a result, the common group key is generated efficiently. However, a failure in user authentication permits unknown attackers to obtain valuableinformation during the group communication. This paper proposes a Media Access Control (MAC)-based authentication in the group key agreement in order to secure the user authentication process in group communications. Without a preliminary agreement, participants in a group communication cannot trust each other in the beginning of the group setup. Therefore, the group controller, who is randomly selected from the group members, needs a security deposit from all members in case an illegitimate user tries to join the group. The user MAC address proposed in this paper can act as a security deposit to provide a secure communication channel while preventing the MAC spoofing problem. Praful S. Kadam et al. [7] provided a Cloud system environment which ensures that user can use highly extensive drivable services resource over the network as and when required. The main aim of the cloud services is the dealing out of users' information is carried out remotely. The user does not own or operate these remote machines. However users always worried about their confidential data, it might be compromised when they use this new environment. This limitation can turn into hindrance to the extensive use of cloud services resource. Praful et al. presented to attend this problem, by using a new highly distributed information accountability cloud bundle. This cloud bundle lets user monitoring to the real usage of the user information inside cloud. This proposed cloud bundle has an object-and domain centered steps which we can use to club the logging method with users' information and policies. This proposed cloud bundle uses the jar programmable capabilities for creating active and roaming object. It also ensures that when anyone accesses the users' data, authentication and automated logging is carried out locally to the jars. In order to make the user's control strong, we can give distributed auditing methods. This proposed cloud bundle also ensures extensive experimental studies to demonstrate that the proposed steps are efficient and effective. Manjusha S et al. [8] describes Cloud computing that helps in transforming the traditional internet computing paradigm and IT industry. Since many Cloud Service Providers (CSPs) are untrusted, the confidentiality, integrity, and privacy of the enterprise information must be protected by some mechanisms. In this paper, we proposed a new framework to enhance secure data storage, fine grained access and preserve data from unknown users or intruders in enterprise cloud. Manjusha et al. proposed mechanism data is encrypted under the set of user attributes and privilege access rights. The Associated Digital Certificate (ADC) is generated for secure, authenticated and Fine grained access from cloud. The proposed framework extended the research towards user revocation and integrity check by data owner. Thus, the analysis of our newly approached scheme is provably secure and efficient in enterprise cloud than other existing scheme. Fahan Ul Arifeen et al. [9], over the recent years of research in cloud computing, different approaches are adopted for Inter- Cloud Authentication. These approaches give successful results in identifying the authentic request. Defense organization communicates with each other's through legitimate requests. For establishing a security and privacy, a PKI based authentication model is needed. This paper signifies a new approach in implementing cloud based PKI authentication inside the existing infrastructure of defense organization. As security is the prime concern for any organization and its implementation requirement varies from organization to organization, each and every organization embrace their own policies to implement it. The problem of understanding each other's security policies is a huge barrier and challenge for existing IT infrastructure for implementation purposes. Requirement to establish Inter-Cloud Authentication is made possible through this PKI based model which ensures all five security services i.e. confidentiality, integrity, authentication, digital signature and non-repudiation. This PKI model is a multi-domain atmosphere between various defense organization and their Data Centers (DC) for the facilitation and resource provisioning inside the cloud platform. This model utilizes the existing network infrastructure composed of high intercommunication traffic between various Data Centers of defense organization. In this model, a nationwide Certification Authority (CA) is implemented in the Inter-Cloud infrastructure and all other Data Centers are inter-communicated through this mechanism having different authentication approaches for legitimate access through the X.S09 Certificates. Rachna Jain et al. [10], Cloud computing is the key powerhouse in numerous organizations due to shifting of their data to the cloud environment. According to IDC survey, Security was ranked and observed first utmost issue of cloud computing. As a result, protection required to secure data is directly proportional to the value of the data. The major handicap of first level of security where cryptography can help cloud computing i.e. secure storage is that we cannot outsource the processing of the data without decryption. A novel framework to secure data access in cloud environment is implemented. Here security is addressed for securing transaction in such a way that transaction should be encrypted and decrypted by data owners only. Server performs equality, addition and subtraction on encrypted data without decryption. Moreover, access should be provided to the users as per their access rights. Security is enhanced by utilizing the concept of multicloud. Venkatesh D et al. [11] Software-as-a service (SaaS) makes utilization of a distributed computing base to convey their applications to numerous clients paying little respect to their area. Due to this offering nature SaaS mists are powerless and give more chances to aggressors to endeavor the framework helplessness and perform vital assaults. In this paper, we exhibit IntTest, a successful administration trustworthiness verification system for SaaS mists. IntTest gives an incorporated diagram authentication examination system that can pinpoint

noxious administration suppliers than existing routines. Additionally IntTest will consequently right the debased result that are delivered by the pernicious administration suppliers and supplant it with great results created by considerate administration suppliers. Our exploratory results demonstrate that our plan is powerful and can attain to higher exactness in pinpointing the aggressors than the current methodologies.

Sanket Salvi et al. [12] said that Cloud Computing is the recent technology that is based on shared pool of resources and provides features like Ubiquitous access, multi-tenancy, flexibility, scalability and pay as you use, which makes it more resource efficient and cost effective. But Cloud-based systems open unfamiliar threats in authentication and authorization. Explicit authorization accordance must be defined at smallest level, especially in multitenant environments. The liaison between Cloud Service Provider & customer must also be clearly mentioned in relation like who holds administrative rights and indirect access to privileged customer information. Moreover the scenario of cloud in educational and research community is still developing and has some security concerns. Sanket et al. provides a brief review about Cloud Security concerns for adoption of cloud computing in data sensitive research and technology aided education. Also this paper proposes, ECK based framework for securing end-user data in Community Cloud. Implications and considerations for additional research are provided as well.

Ashish Singh et al. [13] Day by day users has been adopting remote storage system due to its secure service. But some time it may possible that people comes to know what security policy has been applied in server side. As the result, new security risks and attacks are coming in cloud. So, it is necessary to provide more secured and updated authentication scheme. For any cloud application, in which personal or private information are exchanged, single-tier authentication is not sufficient for authentication. In such situation, multi-tier authentication scheme is much more secured than single-tier authentication scheme. In computing environment, there are various multitier authentication schemes, but they do not provide security against insider attacks and virtualization attacks. In cloud environment, whole authentication control lies in the server side. So, it is hard to trust the third party server in cloud system. Ashish et al. proposed a secured and more advanced multi-tier authentication scheme for accessing cloud services.

Nan Chen et al. [14] Cloud Computing faces many secure challenges, one of which is authentication. Nan et al. analysed a user authentication framework for cloud computing proposed by Amlan Jyoti Choudhury et al and point out the security attacks existing in the protocol. The proposed an improved user authentication scheme. The 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 illustrates that the communication performance of our scheme is efficient.

Satish Kumar et al. [15], Cloud computing is a multi-tenant computational paradigm that offers an efficient, elastic and scalable business model for organizations to adopt various information technology (IT) resources i.e. software, hardware, network, storage, bandwidth etc. There are various aspects of security problem in cloud computing field which include data security, privacy and users' authenticity. The purpose of this research paper is to construct a framework for secure and more advanced authentication scheme for executing secure transactions in a cloud environment. For any cloud service which deals with personal and private information exchange, single tier authentication is not adequate. Authentication schemes that imply more than one tier for authentication are comparatively safer than single tier authentication scheme. Ganesh kumarK et al.[16] analysed the computer security of systems and importance of the digital signature and hashing message algorithm. The proposed digital signature algorithm gives a new technology for producing effective output of digital signature as a result the signing 1 and verifying of signatures are very fast compared to earlier ones. To improve the security and authentication of sending data, this method uses "Message Digest", "IDEA" and "GOST"2 algorithms. The new message digest algorithm is to provide high security, to transfer data by combination of digital signature algorithm and symmetric key cryptography algorithm. The new hashing algorithm proposed creates a unique digital fingerprint along with symmetric key encryption generated IDEA and GOST algorithms. The receiver used the symmetric key and hashing algorithm to form a signature. Ziyad S et al. [17] Cloud computing is a technology, which provides low cost, scalable computation capacity and a stack of services to enterprises on demand for expansion. The complications caused by data security and privacy are the main hindrances in its acceptance. Threats in Cloud computing can be faced by adopting various security measures. One such security measure is authentication. In recent years a lot of research has been carried out throughout the world and several schemes have been proposed to improve authentication in the Cloud. Keeping in view the importance of authentication in cloud security, a survey of current cloud computing authentication trends has been conducted. On the basis of this critical review, we identify the areas of cloud computing authentication that indeed warrant further investigation. Jen-Ho Yang et al. [18] In cloud computing environments, the user authentication scheme is an important security tool because it provides the authentication, authorization, and accounting for cloud users. Therefore, many user authentication schemes for cloud computing have been proposed in recent years. However, the most of the previous authentication schemes have some security problems. Besides, it cannot be implemented in cloud computing. To solve the above problems, Jen et al. proposed a new ID-based user authentication scheme for cloud computing in this paper. Compared with the related works, the proposed scheme has higher security levels and lower computation costs. In addition, it can be easily

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

applied to cloud computing environments. Therefore, the proposed scheme is more efficient and practical than the related works.

Rohitash Kumar et al. [19] Authentication is a key technology for information security, which is a mechanism to establish proof of identities to get access of information in the system. Traditional password authentication does not provide enough security for information in cloud computing environment to the most modern means of attacks. Rohitash et al. proposed a new multi-factor authentication framework for cloud computing. The proposed framework provides a feasible and a most efficient mechanism which can closely integrate with the traditional authentication system. The proposed framework is verified by developing Cloud Access Management (CAM) system which authenticates 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. Prototype model for cloud computing own cloud server is implemented using open sources technology. The proposed framework shows the close agreement with the standard criteria for security.

III. PROPOSED VEARAAAS SECURED AUTHENTICATION FRAMEWORK

The proposed framework namely VEAR AaaS mainly is used for authenticating user access to protect the unwanted entry. Fig.2 shows the proposed a novel authentication as service framework with its components in public cloud computing.

The framework comprises of three major components such as Authenticator, Encryptor and Key generator. Authenticator has two authentication services to the cloud users. Based on the users' needs, they have to select the any one type of authentication service.

A. Authenticator

Authenticator is one of the cloud components in the framework. It consists of two authentication services namely UIDaaS and DIUaaS. UIDaaS is based on user identity based authentication. DIUaaS depends on image based authentication. UIDaaS is used for all types of users in the cloud. DIUAaaS is used for those who need high-end security to their data. Users can choose any one service from the authenticator to protect their data in the cloud. Once the user chooses an authentication service then cloud asks the user registration details such as UserID, Name and etc. The users' registration details and their credential are maintained by the AaaS framework.

B. Encryptor

This component is used to encrypt the data of users. Users submit their details for registration, at the completion of registration users details are encrypted and stored in the cloud. This is an symmetric encryption. It uses a key for encryption and decryption.

C. Key Generator

Key generator is used to generate key for encryption. Encryptor request key for encryption then Key generator generates a key and forwards to the encryptor. Key generator maintains a log file for generating the keys.

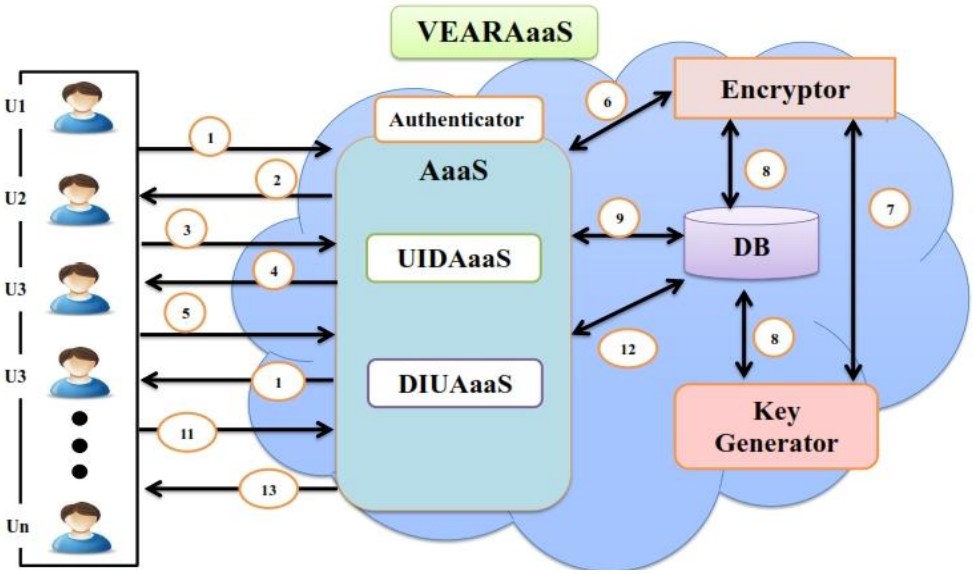

Fig2. Proposed VEAR AaaS Secured Authentication Framework

IV. PROCEDURES FOR VEARAAAS SECURED AUTHENTICATION AAAS FRAMEWORK

Step1: Cloud User request for Cloud services

a. Redirect Authentication as a Service

Step 2: Details about AaaS and Select any one type of Authentication Service

b. Shows information Regarding Cloud Authentication Service

Step 3: Cloud user choose any one type authentication service

Step 4: Shows Registration instruction

Step 5: Cloud user enters Registration Details

Step 6: Encrypt the user registration details
Step 7: Key Request and Response for encrypt the user details
Step 8: Encrypt message and key are stored in the DB
Step 9: AaaS User Authentication details are stored in DB
Step10: AaaS sent Registration success message cloud user
Step 10: Cloud user login with user credential
Step 11: AaaS check the user credential verification
Step 12: Login Success Completed

V. CONCLUSION

Cloud is an open environment to host the data of users. It has many benefits at the same time it also has some security problems. It is necessary to have the proper security framework to address the authentication issues in cloud environment. This paper proposes a framework namely VEAR AaaS which strongly protects the cloud services from the unauthorized users. The users canchoose their authentication service based on their wish. Once the user selects the specific authentication service then the user is authenticated bythat service only. Users' details are encrypted by the symmetric encryption algorithms which is specifically designed and adopted in the cloud authentication service. The proposed framework protects the cloud environment using its components Authenticator, Encryptor and Key Generator.

REFERENCES

[1] Mell P and Grance T, "The NIST definition of cloud computing", (2011).
[2] 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).
[3] Arockiam, L., Monikandan, S., Parthasarathy, G, 'Cloud Computing: A Survey', International Journal of Internet Computing, Volume 1, Issue 2, ISSN: 2231 – 6965, pp 26-33 (2011).
[4] 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 (2015).
[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] Sunghyuck Hong, "Multi-factor User Authentication on Group Communication", Indian Journal of Science and Technology, Vol 8, No. 15, ISSN 0974-5645, pp. 1-6 (2015).
[7] Praful S. Kadam and Pramod A. Jadhav, "Pattern Based User Authentication for Secure Cloud Access and Storage", International Journal of Recent Scientific Research, Vol. 6, Issue 4, ISSN, pp. 3739-3743 (2015).
[8] Manjusha S and Ramachandran R, "Secure Authentication and Access System for Cloud Computing Auditing Services Using Associated Digital Certificate", Indian Journal of Science and Technology, Vol 8, Issue 7, ISSN 0974-5645, pp. 220-227 (2015).
[9] FahanUlArifeen, Raees A. Siddiqui, Sajjad Ashraf and Salman Waheed, "Inter-Cloud Authentication through X.509 for Defence Organization", In proceedings of the 12th International Bhurban Conference on Applied Science & Technology (IBCAST), IEEE, ISBN 978-1-4799-6369-0, pp. 299-306 (2015).
[10] Rachna Jain, Sushila Madan and Bindu Garg, "Framework to Secure Data Access in Cloud Environment", ICSI-CCI 2015, Springer, DOI: 10.1007/978-3-319-20472-7, pp. 127-135 (2015).
[11] Venkatesh D, Dr. P. Venkateshwarlu and B.V. Srikanth, "Flexible Data-Driven Reliable Service Authentication for Multi-tenant Cloud Systems", International Journal of Research, Vol 2, Issue 4, ISSN 2348-6848, pp. 502-509 (2014).
[12] Sanket Salvi, Sanjay H.A, Deepika K.M and Rangavittala S.R, "An Encryption, Compression and Key (ECK) Management Based Data Security Framework for Infrastructure as a Service in Cloud", IEEE, ISBN 978-1-4799-8047-5, pp. 872-876 (2015).
[13] Ashish Singh and Kakali Chatterjee, "A Secure Multi-tier Authentication Scheme in Cloud Computing Environment", International Conference on Circuit, Power and Computing Technologies (ICCPCT), IEEE, ISBN 978-1-4799-7075-9 (2015).
[14] Nan Chen and Rui Jiang, "Security Analysis and Improvement of User Authentication Framework for Cloud Computing", Journal of Networks, DOI 10.4304/jnw.9.1.198-203, pp. 198-203 (2014)
[15] Satish Kumar and Anita Ganapati, "Multi-Authentication for Cloud Security: A Framework", International Journal of Computer Science & Engineering Technology (IJCSET), Vol 5, Issue 4, ISSN 2229-3345, pp. 295-303 (2014).
[16] Ganeshkumar K and Arivazhan D, "Generating a Digital Signature Based on New Cryptographic Scheme for user authentication and Security", Indian Journal of Science and Technology, Vol 7, Issue 6, ISSN 0974-5645, pp. 1-5 (2014).
[17] Ziyad S and Rehman S, "Critical Review of Authentication Mechanisms in Cloud Computing", International Journal of Computer Science, Vol 11, Issue 3, ISSN 1694-0784, pp. 145-149 (2014).
[18] Jen-Ho Yang and Pei-Yu Lin, "An ID-Based User Authentication Scheme for Cloud Computing", 10th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IEEE, ISBN 978-1-4799-5390-5, pp. 98-101 (2014).
[19] Rohitash Kumar Banyal, Pragya Jain and Vijendra Kumar Jain, "Multi-factor Authentication Framework for Cloud Computing", Fifth International Conference on Computational Intelligence, Modelling and Simulation, IEEE, ISSN 2166-8531, pp. 105-110 (2013).

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 year2013 & 2014.