A SURVEY PAPER ON CLOUD AUTHENTICATION ISSUES

[1] S.Hendry Leo Kanickam, [2] V. Jency Puela,
[1]Assistant Professor, [2]Student,
[1] Department of Information Technology,
[1] St.Joseph’s College, Trichy, Tamilnadu, India

Abstract: Cloud computing is a mechanical movement that revolves around the way in which we arrangement computing systems, make applications, and utilize existing organizations for building programming. It relies upon the possibility of dynamic provisioning, which is associated not only to organizations yet notwithstanding register capacity, accumulating, frameworks organization, and information technology (IT) system all around. Resources are made available through the Internet and offered on a pay for every use introduce from dispersed processing traders. The present condition of norms and interoperability in distributed computing takes after the early Internet period, when there was no normal concurrence on the conventions and innovations utilized and every association had its own system. Interoperability comes along with the concept of security measures and privacy of data. There are chances of unauthorized user access and loss of data. In this state virtual machines are doled out to the cloud customers. These devices are prone to open logins that can be effortlessly broken. This paper deals with customer authentication and authorization issues that leads to safe interoperability mechanisms.

Index Terms – Cloud computing, interoperability, user authentication, authorization, virtual machines.

I. INTRODUCTION

Cloud Computing is methodology for dispersed enlisting in which a particular application may tackle diverse interconnected PCs all the while. Distributed computing has conveyed with different stunning administrations like performing troublesome counts with solace, mass stockpiling, worldwide figuring, little stockpiling value, ease of section and so forth. An user access this facility with the help of a user password. But, cracking of these passwords is not difficult because they don’t provide problematical secret keys, or don't adjust their keys on and off, or may use practically identical watchword to utilize various applications. In this manner the security of data on circulated figuring is the need of the time.

According to the official NIST definition, "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1]." Associations, for instance, National Institute of Standards and Technology (NIST), Object Management Group (OMG), Distributed Management Task Force (DMTF) have offered their little hard work to build use cases . These use cases are categorized as into cloud management, cloud interoperability and cloud security. The interoperability use cases are as per the following:

1. Customer Authentication
2. Workload Migration
3. Data Migration
4. Workload Management

The use case for client confirmation identifies a customer or program that needs to be perceived in the cloud society. It is necessary to categorize end users and cloud-resource users. End users are customers of services rendered on cloud resources. The end users authenticate themselves only with application and are unaware that the application facility is rendered on the cloud environment. Whereas, cloud resource users are the owners of those cloud resource facilities. These users can grant approvals for the assets grounded on jobs, get to records, IP address, fields. The cloud resource user has bigger interest from an interoperability view. This paper examines the primary interoperability use case which is the authentication. The basic algorithms and protocols used for the above case are discussed in detail [2].

II. SECURITY ISSUES IN CLOUD COMPUTING

Cloud Computing isn't highly shielded usually. Cloud security isn't accurately substantial. There are concerns identified with the trustworthiness and protection of information. There ought to be suitable security activities for cloud clients to achieve their trust. Indeed, even though certain security activities were connected to cloud foundation still the clients are supposing extra security features on benefit of their information in mists. The cloud information is powerless to different sorts of assaults. The succeeding assaults can influence the cloud security:

1. Secret key Guessing Attack: This involves a few ambushes that help in finding the customer’s secret key.

2. Replay Attack: This issue involves tracing of the authorized details and giving them to unauthorized users.

3. Man-in-the-middle Attack: In this issue, the hacker acts as a user and attempts to fetch the keys from the server storage.

4. Disguise Attack: Similar to the man in the middle attack, the hacker acts as a verifier instead and fetches the secret keys.

5. Insider Attack: Here the hacker snips the personal information of the customer.

6. Phishing Attack: Social Engineering goals for instance, fake messages, sites request the client disclose to her secret keys.

7. Shoulder Surfing Attack: The hacker secretly watches the password that user enters [3].

The security can be applied to the applications by considering the following factors:

i. Cloud computing architecture
ii. Portability and interoperability
iii. Data center operations
iv. Notification and remediation
v. Application Security
vi. Encryption and Key management
vii. Identity and access management.

III. PROLOGUE TO USER AUTHENTICATION AND AUTHORIZATION

Cloud Computing offers flexible and on-demand resources to its customers. The three kind of service models include:

i. Softwares as a Service (SaaS),
ii. Platforms as a Service (PaaS), and
iii. Infrastructures as a Service (IaaS).

Every service model satisfies the different needs of a customer.

a. Softwares as a Service: It provides software or applications that the cloud provider approves and it is hosted in the cloud resource environment.
b. Platforms as a Service: It provides developing environment to build and host the application on the cloud service environment.
c. Infrastructures as a Service: It offers imagined registering assets, for example, virtual work area, virtual capacity, and so on.

Many cloud services and cloud service providers are much useful for customers who search for particular service resources; it leaves some security issues to the users who are in need of such application.

1. A cloud service provider wants their users to save their account information and access that information from that environment itself which leads to privacy issue.
2. Many SLAs have communicated the mystery of the tricky information. It is hard for customers to guarantee the appropriate guidelines are approved for the privacy of personal information.
3. When a customer uses various cloud services, duplication of customer information is created. .
4. Duplication of record will lead to multiple authentication procedures. As a result, the user exchanges their information for every service facility.
5. Cloud authority centers practice various confirmation mechanical assemblies for approving customers; this may have little impact on SaaS when compared to PaaS and IaaS, which has become a challenge to the user [4].

The main idea for user authentication is that a client who built up a character by association with distributed computing can rehearse a similar personality with different mists too.

As customers interconnect with the Cloud, identity suits a basic issue to take care of prosperity, obvious quality and control. In this environment, it is necessary for the applications to check the users identity and analyse the permissions granted for the user to build or refresh a record and examination their exercises. In this way check and approval are not kidding segments of a cloud personality stratagem and give portability and extensibility past creativity limitations.

Authentication

Validation is the advancement for checking the independence of the client. The cutting edge confirmation technique concurs the structure to order the client through a customer name and after that approve their personality through watchword. There are considerably solider gadgets of client check. region, for example, a Software-as-as-Service (SaaS) application, utilizing the verification that unfolded in additional area.

Authorization

Authentication is followed by the Authorization process. This limits what the customer is granted permission. The accessing application handles the authorization process. The authorization policy is centralized irrespective of the user's location or application's remote place. Authorization is purely decided based on the user's identity and sometimes along with designation or title.

IV. STRATEGIES UTILIZED IN CLIENT AUTHENTICATION AND AUTHORIZATION

Identity management and permissions to cloud resources for authorized units are provided by Identity and Access Control Service. Such units can be individuals, programming strategies or additional structures. So as to give an appropriate equivalent of access to a spare, the refinement of a thing should be affirmed principle, which is the affirmation strategy that drives the endorsement technique. Other than confirmation and approval forms, review logging device ought to be utilized to monitor all finished and fizzled activities about verification what's more, get to endeavors by the application. Grouping is practiced by various encryption frameworks, which is the way toward figuring information by methods for cryptographic procedures [5, 6]. Offering such service will assure delicate and personal data security and only the proposed unit can solve it.

Algorithms for Customer Authentication and Authorization

The security provisions focuses to stay away from the pointless interruption of unapproved clients and comfortable section spot. Whether a user is new or an existing one, he/she needs to prove his/her identity to the service provider to access the resources that he/she needs. The user's demand is coded and then transferred to the cloud environment in order to satisfy the customer needs. The encryption process algorithms are explained below. They are as follows:

a) RSA Algorithm: This algorithm helps in making a safe communication. The user's demands are coded and transferred to the service provider. In this algorithm, the encryption is based on the system's pubic key. Every time a user demands a file, the demand is encrypted by the system using RSA encryption calculation with the client's open key [7].

b) AES Algorithm and MD5 Hashing Algorithm: When a document is transferred by a client the structure server encodes the record utilizing AES encryption calculation. In this 128, 192, 256 piece key can be utilized. The key is produced coincidentally by the structure server. The produced key can be used only once which is used for both encoding and decoding a customer' file. This key cannot be used in any other instances afterwards. This key is stored along with the user account in the database [8].

c) OTP Password Algorithm: This algorithm uses OTP for validating the user. The OTP helps in preventing the account and data from hackers. One Time Password (OTP) has been created to overcome the chance of identifying the user defined secret keys [9].

d) Data Encryption Standard Algorithm: This algorithm belongs to similar key coding algorithms. Similar key encryption is a cryptosystem in which a single key is used to perform both encryption and decryption.

e) Rijndael encryption Algorithm: This is the most used encryption algorithm that is used to code delicate data. The iteration of a specific transformation accomplishes the data block encryption or decryption.

V. PROTOCOLS USED IN THE PROCESS OF CUSTOMER AUTHENTICATION AND AUTHORIZATION

Identity management and permissions to cloud resources for authorized units are provided by Identity and Access Control Service. Such units can be individuals, programming strategies or additional structures. To provide proper usage permission to services, the authentication process i.e., verification of user identity should be carried out. Also confirmation and approval forms, audit order gadget ought to be utilized to monitor all fruitful and unsuccessful activities about verification and induction endeavors by the application. Security is practiced by unprecedented encryption segments, which is the game plan of impact data by techniques for cryptographic computations. Offering such service will assure delicate and personal data security and only the proposed unit can solve it.

The following authentication protocols are used

a) Extensible Authentication Protocol-CHAP: Cloud environment implements EAP(Extensible Authentication Protocol) for authenticating the user's identity. For transporting and using keying texture and parameters created by EAP methods, this protocol is used. Challenge-Handshake Authentication Protocol (CHAP) can also be used for authentication [10].

b) Lightweight Directory Access Protocol: Predominantly organizations are putting away their key in grouping in some method server. SaaS suppliers can give the check technique to the customer's inside LDAP/AD server, which helps organizations in monitoring the users.

c) Single Sign-on (SSO) Protocol: SSO Protocol is depicted as a portion of the cloud environment's distributed security system. An SAML server gives SSO administrations to application examination suppliers: SAML server issues SAML name which contains a statement on the customer's self-confirmation, along these lines affirming that it has been properly verified or not. Once the client is verified, the person can apply for entrée to various approved pay at various application supplier locales without the need to re-confirm for every zone.

VI. CONCLUSION

In the current state of Networking, cloud computing plays a vital role for developers and users. However, security is the most vital testing issue in distributed computing. Without right security and withdraw occasions planned for mists, this possibly upsetting processing model could form into a gigantic breakdown. Information wellbeing has turned into the key issue of distributed computing security. Interoperability implies just contacting the outstanding tasks at hand from single cloud to any more. The interoperability use case has the vital and first principle necessity of bolted and more secure client confirmation and approval. The key thought in the back this exercises was to venture out cloud security. The opening or the most fundamental assault danger of client get to is checked driving by utilizing uncommon calculations. Every calculation utilizes uncommon conventions in perspective of giving most amazing likely check to client confirmation and approval.

In this paper we managed unique calculations utilized for client check and approval in distributed computing. Various algorithms, for example, RSA, AES, MD5, OTP generation calculation, DES, Rijndael encryption Algorithm were determined. RSA Algorithm is deterministic and henceforth turns out to be effectively broken in long run. Be that as it may, alternate calculations examined make the model very anchored. Every one of this calculations examined were produced to give most ideal ever answer for the client validation and approval issues. Distinctive conventions, for example, LDAP, EAP, and SSO conventions were likewise contemplated. Regardless of whether some interloper gets access of the information inadvertently or purposefully, he won't have the capacity to unscramble it.

References

[1]. Wayne A Jansen, NIST, "Cloud Hooks: Security and Privacy Issues in Cloud Computing**"** Proceedings of the 44th Hawaii International Conference on System Sciences – 2011.

[2]. Grace A.Lewis, "The Role of Standards in Cloud Computing Interoperability", Technical note, Software Engieering Institute, October 2012.

[3]. Shikha Choksi, "Comparative Study on Authentication Schemes for Cloud Computing", IJEDR, Volume 2, Issue 2, ISSN 2321-9939.

[4]. Abdel Majid Hassan, Mansoor emam, "Additional Authetication and Authorization using registered E-mail id for cloud computing", International Journal of Soft Computing and Engineering(IJSCE), ISSN 2231-2307,Volume-3, Issue-2,May 2013.

[5]. Dawei Sun, Guiran Chang, Lina Sun, and Xingwei Wang, "Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments", Scienceverse Science Direct , Elsevier, Volume-15, 2011

[6]. Davit Hakobyan, "Authentication And Authorization Systems In Cloud Environment", Master Of Science Thesis, Stockholm, Sweden, 2012.

[7]. "Cloud Data Security Using Authentication And Encryption technique, Sanjoli single, Jasmeet Singh, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 2, Issue 7, July 2013.

[8]. Burt Kaliski, "The Mathematics of the RSA Public-Key Cryptosystem", RSA Laboratories.

[9]. Ronald Rivest, "MD5 Message-Digest Algorithm", rfc 1321, MIT Laboratory for Computer Science and RSA Data Security, Inc., April 1992 .

[10]. Sadia Marium et al, "Implementation of EAP with RSA for Enhancing the Security of cloud Computing", International Journal of Basic And Applied Sciences, Volume-1, Issue-3, 2012.

Mr. S. Hendry Leo Kanickam working as a Assistant Professor in Department of Information Technology , St. Joseph's College (Autonomous) Trichy, India. He received his M.Phil. Degree in Bharathidasan University in 2008 and also He is pursuing Ph.D (Computer Science) in Bharathidasan University.

Ms. V. Jency Puela is studying II M.Sc. Information Technology in the Department of Information Technology, St. Joseph's College (autonomous) Trichy, India.