A New Method to Secure API in Cloud Computing Using HTTPS, MD5 and RSA

Neha Tiwari

Research Scholar, Dept of Computer Science & Engg
TIETECH, Jabalpur (M.P.)

Monali Sahoo

Prof., Dept of Computer Science & Engg
TIETECH, Jabalpur (M.P.)

***Abstract* - Cloud computing is surrounded by many security issues like securing data, and examining the utilization of cloud by the cloud computing vendors. The wide acceptance www has raised security risks along with the uncountable benefits, so is the case with cloud computing. They also provide authentication at certain specific level. Cloud computing offers an innovative business model for organizations to adopt IT services without upfront investment. Despite the potential gains achieved from the cloud computing, the organizations are slow in accepting it due to security issues and challenges associated with it. Security is one of the major issues which hamper the growth of cloud. This paper introduces a detailed analysis of the cloud computing security issues and challenges focusing on the cloud computing end user security based on browser or API/URL and SSL based security. This paper mainly proposes the core concept of secured cloud computing for end user. It suggests the cloud computing based on separate encryption using MD5 and SHA services based on transport layer security (TLS) for user data which will be transferred by user's API. Due to this increasing demand for more clouds there is an ever growing threat of security becoming a major issue.**

Keywords — SaaS, PaaS, IaaS, Security, threats, URL/API security, TLS

I. INTRODUCTION

The US National Institute of Standards and Technology (NIST) define cloud computing as "a model for user convenience, on- demand network access contribute the computing resources (e.g. networks, storage, applications, servers, and services) that can be rapidly implemented with minimal management effort or service provider interference" Cloud computing can also be defined as it is a new service, which are the collection of technologies and a means of supporting the use of large scale Internet services for the remote applications with good quality of service (QoS) levels [4]. Cloud computing is has many technologies such as Saas i.e. "Software as a Service", Paas i.e. "Platform as a Service", IaaS i.e. Infrastructure as a Service". Cloud Computing is a paradigm that focuses on sharing data and computations over a scalable network of nodes. Examples of such nodes include end user computers, data centres, and Cloud Services. We term such a network of nodes as a Cloud. Cloud service delivery is divided among three archetypal models and various derivative combinations. The infrastructure (as a Service), respectively defined.

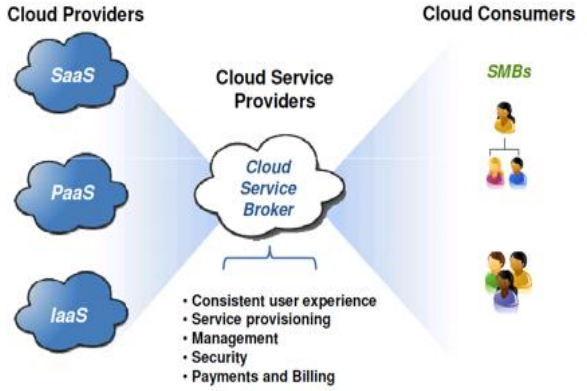

Fig1. Cloud Service Model

II. API SECURITY IN CLOUD ENVIRONMENT

Cloud computing and web services run on a network structure so they are open to network type attacks. One of these attacks is the distributed denial of service attacks. If a user could hijack a server then the hacker could stop the web services from functioning and demand a ransom to put the services back online. To stop these attacks the use of syn cookies and limiting users connected to a server all help stop a DDOS attack. Another such attack is the man in the middle attack. If the secure sockets layer (SSL) is incorrectly configured then client and server authentication may not behave as expected therefore leading to man in the middle attacks. It is clear that the security issue has played the most important role in hindering Cloud computing. Without doubt, putting your data, running your software at someone else's hard disk using someone else's CPU appears daunting to many. Well-known security issues such as data loss, phishing, and botnet (running remotely on a collection of machines) pose serious threats to organization's data and software. Moreover, the multi-tenancy model and the pooled computing resources in cloud computing has introduced new security challenges that require novel techniques to tackle with.

Identity and access management
Identity and Access Management (lAM)

(lAM) features are Authorization, Authentication, and Auditing (AAA) of users accessing cloud services. In any organization "trust boundary" is mostly static and is monitored and controlled for applications which are deployed within the organization's perimeter. In a private

data center, it managed the trust boundary encompasses the network, systems, and applications. And it is secured via network security controls including intrusion prevention systems (IPSs), intrusion detection systems (IDSs), virtual private networks (VPNs), and multifactor authentication.

Privacy - Privacy is the one of the Security issue in cloud computing. Personal information regulations vary across the world and number of restrictions placed by number of countries whether it stored outside of the country. For a cloud service provider, in every jurisdiction a single level of service that is acceptable. Based on contractual commitments data can store within specific countries for privacy regulations, but this is difficult to verify. In case of Private and confidential customer's data rising for the consequences and potential costs of mistakes for companies that handle. But professionals develop the security services and the cloud service privacy practices. An effective assessment strategy must cover data protection, compliance, privacy, identity management, secure operations, and other related security and legal Issues.

Securing Data in Transmission - Encryption techniques are used for data in transmission to provide the protection for data only goes where the customer wants it to go by using authentication and integrity and is not modified in transmission. SSL/TLS protocols are used here. In Cloud environment most of the data is not encrypted in the processing time, but to process data, for any application that data must be unencrypted. In a fully homomorphism encryption scheme advance in cryptography, which allows data to be processed without being decrypted. To provide the confidentiality and integrity of data-in-transmission to and from cloud provider by using access controls like authorization, authentication, auditing for using resources, and ensure the availability of the Internet-facing resources at cloud provider.

User Identity - In Organizations, only authorized users across their enterprise and access to the data and tools that they require, when they require them, and all unauthorized users are blocked for access. In Cloud environments support a large enterprise and various communities of users, so these controls are more critical. Clouds begin a new level of privileged users working for the cloud provider is administrators. And an important requirement is privileged user monitoring, including logging activities. This monitoring should include background checking and physical monitoring.

Audit and Compliance - An organization implements the Audit and compliance to the internal and external processes that may fallow the requirements Classification with which it must stand and the requirements are customer contracts, laws and regulations, driven by business objectives, internal corporate policies and check or monitor all such policies, procedures, and processes are without fail. In traditional out sourcing relationships plays an important role for audit and compliance. In Cloud dynamic nature, increase the importance of these functions in platform as-a service (PaaS), infrastructure-as-a-service (laaS), and software-as -a-service (SaaS) environments.

III. INFRASTRUCTURE SECURITY ISSUES [1]

Cloud suppliers provide security-related services to a good vary of client types; the security equipped to the foremost demanding clients is additionally created on the market to those with the smallest amount stringent necessities. Whereas Infrastructure Security Solutions and product are often simply deployed, they need to a part of an entire and secure design to be effective.

Securing Data-Storage- In Cloud computing environment data protection as the most important security issue. In this issue, it concerns include the way in which data is accessed and stored, audit requirements, compliance notification requirements , issues involving the cost of data breaches, and damage to brand value. In the cloud storage infrastructure, regulated and sensitive data needs to be properly segregated. In the service provider's data center, protecting data privacy and managing compliance are critical by using encrypting and managing encryption keys of data in transfer to the cloud. At the cloud provider, the best practice for securing data at rest is cryptographic encryption and shipping self encrypting is used by hard drive manufacturers. Self-encrypting provides automated encryption with performance or minimal cost impact. Software encryption is less secure and slower because the encryption key can be copied off the machine without detection.

Network and Server - Server-Side Protection: Virtual servers and applications, very like their non-virtual counterparts, have to be compelled to be secured in IaaS clouds, each physically and logically. Example, virtual firewalls are often used to isolate teams of virtual machines from different hosted teams, like production systems from development systems or development systems from different cloud-resident systems. Rigorously managing virtual machine pictures is additionally vital to avoid accidentally deploying pictures underneath development or containing vulnerabilities. Preventing holes or leaks between the composed infrastructures could be a major concern with hybrid clouds, as a result of will increase in complexity and diffusion of responsibilities. The supply of the hybrid cloud, computed because the product of the supply levels for the part clouds, also can be a concern; if the % availability of anyone part drops, the availability suffers proportionately. In cloud environment, purchasers want to form certain that every one tenant domains are properly isolated that no probability exists for data or transactions to leak from one tenant domain into successive.

IV. END USER SECURITY ISSUES [1]

End Users need to access resources within the cloud and may bear in mind of access agreements like acceptable use or conflict of interest. The client organization have some mechanism to find vulnerable code or protocols at entry points like servers, firewalls, or mobile devices and upload patches on the native systems as soon as they are found.

Browser Security - In a Cloud environment, remote servers are used for computation. The client nodes are used for input/output operations only, and for authorization and authentication of information to the Cloud. A standard Web browser is platform in-dependent client software useful for all users throughout the world. This can be categorized into different types: Software as-a-Service (SaaS), Web applications, or Web 2.0. TLS is used for data encryption and host authentication.

Authentication - In the cloud environment, the primary basis for access control is user authentication and access control are more important than ever since the cloud and all of its data are accessible to all over the Internet. Trusted Platform Module (TPM) is a widely available and stronger authentication than username and passwords. Trusted Computing Groups (TCG's) is IF-MAP standard about authorized users and other security issue in real-time communication between the cloud provider and the customer. Other such risks which are marked as high risk in cloud security are

Loss of Governance: in using cloud infrastructures, the client necessarily cedes control to the Cloud Provider (CP) on a number of issues which may affect security. At the same time, SLAs may not offer a commitment to provide such services on the part of the cloud provider, thus leaving a gap in security defences.

Data Protection: cloud computing poses several data protection risks for cloud customers and providers. In some cases, it may be difficult for the cloud customer (in its role as data controller) to effectively check the data handling practices of the cloud provider and thus to be sure that the data is handled in a lawful way. This problem is exacerbated in cases of multiple transfers of data, e.g. between federated clouds. On the other hand, some cloud providers do provide information on their data handling practices. Some also offer certification summaries on their data processing and data security activities and the data controls they have in place, e.g.,SAS70 certification. Data flowing from the Internet is filled with mal ware and packets intended to lure users into unknowing participation in criminal activities.

V. SECURE WEB ACCESS

Secure web access provides the following services to the users:

i. Authentication service: The web server is configured to present a notarized credential called "certificates" to address identity concerns.

ii. Encryption service: The web server and web client negotiate a session key for encrypting the packet data exchanged among them, ensuring the confidentiality of the information.

iii. Option: mutual authentication service: The web server is configured to ask browsers to prompt the user to select a personal certificate, and then check on the authenticity of the signed personal certificate and against an access control ("password") list.

The mutual authentication service enables the web server to verify users without them presenting the login/password. Secure access to a web server can be enhanced by requiring a client to present its digital certificate. Certificate is signed by a CA: The CA takes all the fields of the certificate except the last field and generates the message digest (hash) typically using MD5 and SHA. CA then encrypts (also called signs) the message digest (256 bits if MD5 is used) using CA's private key. The resulting encrypted/signed message digest is called signature. The signature was filled in the last field of the certificate.

TLS/SSL Architecture

The TLS/SSL security protocol is layered between the application protocol layer and the TCP/IP layer, where it can secure and send application data to the transport layer. Because it works between the application layer and the transport layer, TLS/SSL can support multiple application layer protocols.

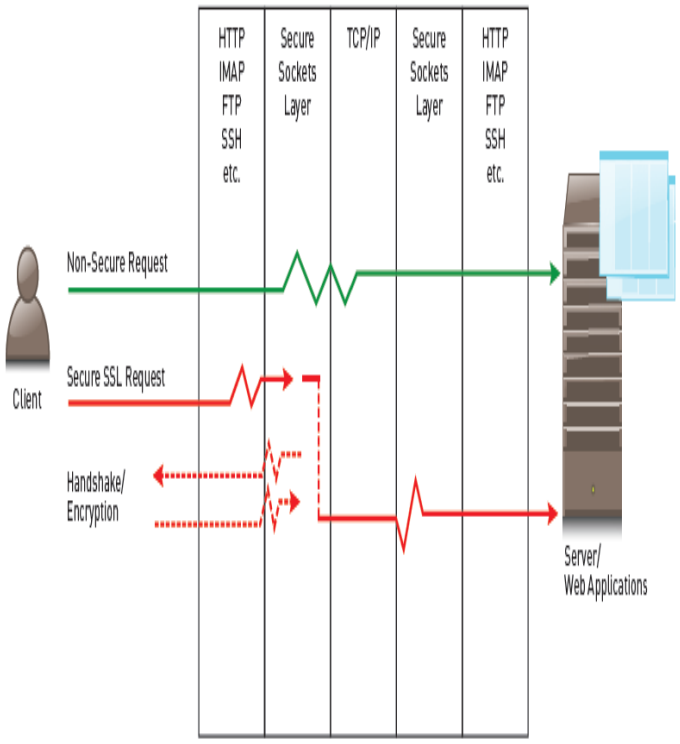

Fig2. Non-Secure Transmission Request vs. Secure SSL Transmission Request

TLS/SSL assumes that a connection-oriented transport, typically TCP, is in use. The protocol allows client/server applications to detect the following security risks:

- Message tampering
- Message interception
- Message forgery

The TLS/SSL protocol can be divided into two layers. The first layer consists of the application protocol and the three Handshake sub-protocols: the Handshake Protocol, the Change Cipher Spec Protocol, and the Alert Protocol.

The second layer is the Record Protocol. The following figure illustrates the various layers and their components.

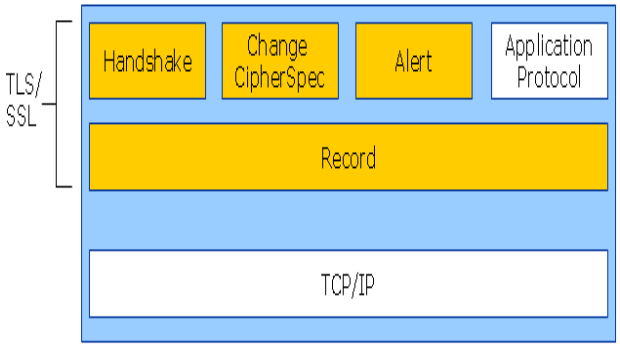

Fig3. TLS/SSL Protocol Layers

VI. PROPOSED SCHEME

The proposed solution calls upon cryptography, specifically Public Key Infrastructure, to ensure the authentication, integrity and confidentiality of involved data and communications. The solution, presents a horizontal level of service, available to all implicated entities, that realizes a security mesh, within which essential trust is maintained. This approach cloud computing end user security based on browser or API/URL and SSL based security. This paper mainly proposes the core concept of secured cloud computing for end user. It suggests the cloud computing based on separate encryption using MD5 and SHA services based on transport layer security (TLS) for user data which will be transferred by user's API.

Public key Infrastructure is able to effectively transform security problems into key management issues. Ultimately, the success of the proposed solution, as any cryptographic system, is dependent on controlling access to private keys. An additional important factor as in every centralized system is system and network performance. As additional encryption processes could deter efficiency. The constant encryption and decryption of data could have a heavy toll on speed, inducing additional processing consumption. Using the cloud infrastructures flexibility within the context of demand on cpu, could leverage the system from this overhead and accelerate encryption/decryption. Currently encryption schemes are being researched that allows data to ''searched'' without the need of it being decrypted.

A Trusted Third Party is able to provide the required trust by guaranteeing that communicating parties are who they claim to be and have been scrutinized to adhere to strict requirements. This process is performed through the certification process, during which an entity requiring certification is required to conform with a set of policies and requirements. TTP is an ideal security facilitator in a distributed cloud environment where entities belonging to separate administrative domains, with no prior knowledge of each other, require establishing secure interactions

Trusted Third Party Sever Installation

Fig4. User Authentication Process in Cloud using Trusted Third Party

RSA RSA Implementation

After successfully implementation of RSA algorithm digital certificate will be appear on web browser.

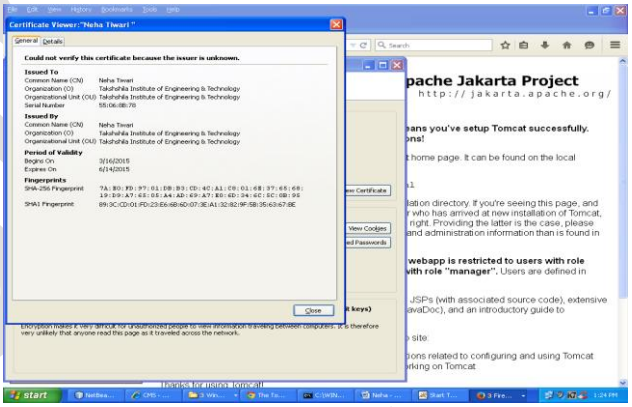

Fig5. Implementation of RSA

Information of Digital Certificate- Detailed information of the generated digital certificate

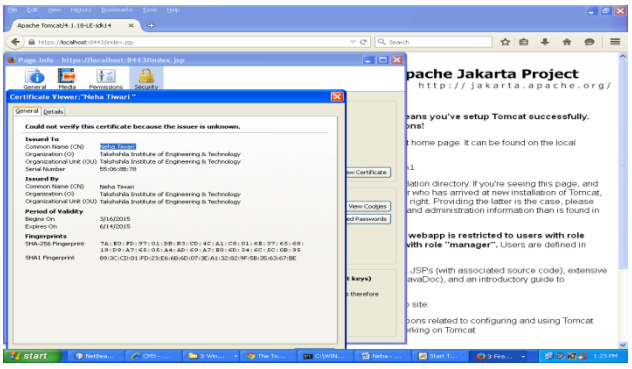

Fig6. Information about Digital Certificate

VII. CONCLUSION

Cloud computing systems challenge is assessing and managing risk. In the system lifecycle, risks that are identified should be rigorously balanced against the

protection and privacy controls out there and therefore the expected edges from their utilization. In this paper, we explored the security issues at various levels of cloud computing service architecture. Security of customer information is a major requirement for any services offered by any cloud computing. So the main focus of security is the user API security in this paper. However, one must be very careful to understand the security risks and challenges posed in utilizing these technologies. We use many secure methods to secure the end user's data in API. The HTTPS is used for Validate server certificates, including CA checking and revocation checks using Certificate Revocation Lists (CRLs), check and optionally enforce various SSL parameters such as cipher and version. To achieve this implementation along with Digital signature we have used RSA and MD5 Encryption algorithm to improve security one step ahead. This model ensures authentication and security for end user's API system.

REFERENCES

[1]. "Security Architecture of Cloud Computing", V.KRISHNA REDDY 1, Dr. L.S.S.REDDY, International Journal of Engineering Science and Technology (IJEST), Vol. 3 No. 9 September.

[2]. "Security Architecture of Cloud Computing", V.KRISHNA REDDY 1, Dr. L.S.S.REDDY,

[3]. International Journal of Engineering Science and Technology (IJEST), Vol. 3 No. 9 September 2011.

[4]. 'The Effective and Efficient Security Services for Cloud Computing ",Sambhaji Sarode, Deepali Giri, Khushbu Chopde, International lournal of Computer Applications (0975 - 8887) Volume 34- No.9, November 2011.

[5]. "Cloud Computing Security" Danish Jamil Hassan Zaki, International Journal of Engineering Science and Technology (IJEST), Vol. 3 No. 4 April 2011

[6]. Peter Mell, and Tim Grance, "Draft NIST Working Definition of Cloud Computing," 2009

[7]. http://csrc.nist.gov/ groups/SNS/cloud-computing

[8]. "Cloud Computing Security Issues and Challenges", Kuyoro S. 0.Ibikunle F., Awodele O.

[9]. Catteddu D. 2010 Cloud Computing. [Online] Available from: http://w. enisa. europa. eu/ act/rm/files/deliverables /c1oud-computing risk- assessment [Accessed 26th April 2010] http://adventuresinsecurity.comlblognp=67.

[10]. P. Mell and T. Grance, "The NIST Definiton of Cloud Computing", NIST Special publication 800-145

[11]. T. Prabhakar and B. Sodhi, "Introduction to Cloud Computing," http://cse.iitk.ac.in/users/sodhi/cloud_lect.html

[12]. C. Wang, S. Chow, Q. Wang, K. Ren, W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Trans. Computers, vol. 62, No. 2, February 2013.

[13]. F. Shaikh and S. Haider, "Security Threats in Cloud Computing," Dec 2011 Abu Dhabi, United Arab Emirates.

[14]. E. Mohamed and H. Abdekar, "Data Security Model for Cloud Computing," ICN 2013.