IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Issue-2, Feb 2019 E-ISSN: 2347-2693

SSL Based Cryptography Data Management in Private Cloud Computing

D. Meenakshi[1]*, V. Karthika Devi[2]

[1,2]Department of Computer Science,Shrimati Indira Gandhi Colloge,Tiruchippallai,India

*Corresponding Author: d.meenakshi2310@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7i2.439442 | Available online at: www.ijcseonline.org

Accepted: 13/Feb/2019, Published: 28/Feb/2019

Abstract— As a personal or business cloud computing user can processing their accumulated information on the '**cloud**', via an Internet connection. The main attitude following this form is for providing, processing, storing "as a service." Technologies such as cluster have all aimed at providing permission to accessing huge amount of information on entirely implicit way by combine the resources and recommending distinct sight of the structure. Network security is goings-on which were modelled for preventing our data while used on the network. It was included on both the technologies of hardware as well as software. Network security technology achieved variety of its targets such as coercions and prevents them from stabbing or extending on the network in this paper SSL handled the data in private cloud computing.

Keywords—SSL, Cryptography, Privatecloud computing

I. INTRODUCTION

Cloud computing has been make up as an umbrella term to describe a category of complicated on-need processing services from benignly provided by payments and providers are Amazon, Google, and Microsoft. Network security merged numerous levels of protections at the border in the network. [15] All the network security levels put in to its guidelines and powers. Certified consumers can achieve by accessing the network resources, but wicked actors are obstructed from hauling out abuse and coercion.

Now the world has digitized in all the ways. The way we survive, occupy ourselves, learning and earning everything was changed. The organization which are all wanted to delivers is services to the consumers and the workers insist must want to prevent the network. It also protects the confidential information from the attackers. Eventually it defends the clients' information from your reputation in computers and computer networks and molest is a challenge to description, alteration, immobilize, scoring through, thrash or achieve by an illegal process.

Network security takes vital role in all the business world and even people's day to day life. Most of the persons in the world have one or more wireless connections with wireless routers which was indeed to abuses the data for not secured properly. Perfect rigid network security system helps data loss from theft and reduces the risk of data loss, theft and damage. Section I contains the introduction of Network security in cloud computing. Section II contains the some secure socket layer implemented on web services. Section III contains related work for private cloud computing. Section VI conclusion

A) CLOUD COMPUTING SERVICE MODELS

Infrastructure-as-a-Service (IaaS): Infrastructure is most vital surrounded by the three service models because it is the basic need to launch the organization's forces over the internet in a cloud proposal, to make their services available to clients and applications to run them smoothly [9].

Software-as-a-Service (SaaS): It is a software allocation model anywhere a negotiator provider hosts applications and makes them offered to customers over the high-speed internet connection.

Platform-as-a-Service (PaaS): It is a centre layer which gives the organizations, institutions otherwise companies a freedom as well as framework for developers to develop their own applications along with deploy them and make customers within their company to access the resources [8].

B) TYPES OF CLOUD COMPUTING

Cloud computing type's public, private and hybrid cloud. Public cloud can be utilizes by all organizations are any companies sector, but private cloud can accessed by any one or particular organizations it needs some security control to access the data in cloud computing. Hybrid cloud is the combination for public and private cloud.

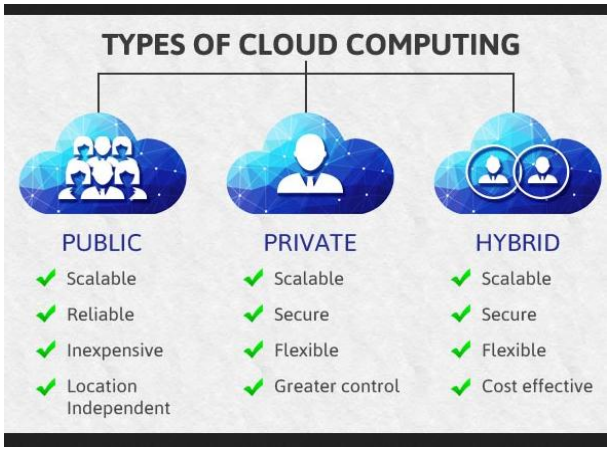

Fig 1.Types of cloud computing

BENEFITS OF CLOUD COMPUTING

1. Lower IT infrastructure and computer costs for users
2. Improved performance
3. Fewer Maintenance issues
4. Instant software updates
5. Improved compatibility between Operating systems
6. Backup and recovery
7. Performance and Scalability
8. Increased storage capacity
9. Increase data safety

C) CRYPTOGRAPHY

Transforming plain text to cipher text is known as cipher which is refers to algorithm. It has two methods encryption and decryption. The study of encryption principles and methods is known as cryptography. Cryptography is the combinational of cryptology and cryptanalysis .it has plain text and cipher text. Plain text is a original message. The original message is converted in to coded message called cipher text. The study of principles/ methods of deciphering ciphertext *without* knowing key are called as cryptanalysis[14].

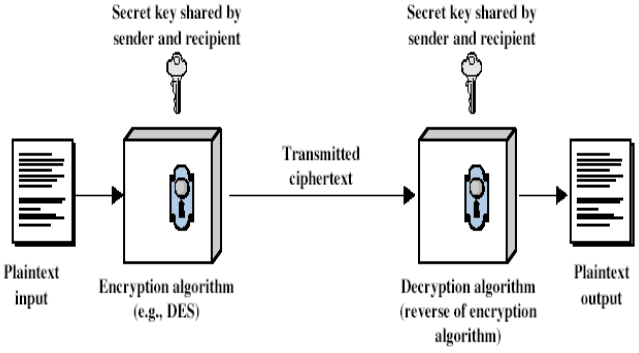

Fig 2. Cryptography model

It represents as two key algorithms. First one is symmetric it means that same key is used for encryption and decryption. Second one is asymmetric it means that mathematically related key pairs for encryption and decryption. Public and private keys. Cryptography has four objectives. **Confidentiality** the information cannot be understood by anyone for whom it was unintended **Integrity** the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected **on-repudiation** the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information **Authentication** the sender and receiver can confirm each other's identity and the origin/destination of the information[14]. Cryptography has many algorithm techniques. In this paper discuss about the private cloud the solidus (/), the exp function, or appropriate exponents. Italicize Roman symbols for quantities techniques authentication specified in SSL (Server Socket Layer)

II. SSL (Secure Sockets Layer)

Secure Sockets Layer (SSL) is a standard protection tools for encrypted link between a server as well as a client. It allows susceptible in sequence such as credit card numbers, social security numbers, in addition to login credentials to be transmitted securely .it have a variety of threats so we need added security mechanisms. SSL was first developed by Netscape in 1994 and became an internet standard in 1996 (RFC 2246 – TLS V1.0) SSL is a cryptographic protocol to secure network across a connection-oriented layer. Any program using TCP can be modified to use SSL connection [1].

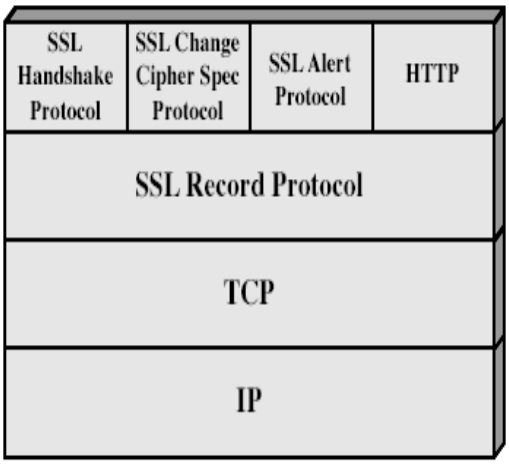

FIG 3. SSL Architecture

SSL session is association between client & server. It has created by the Handshake Protocol and also defines as set of cryptographic parameters with shared by multiple SSL

connections. SSL connection is peer-to-peer communications link. In figure4 shows the data management in web services and secures the data for authentication purpose [5]. SSL protocol provides two services for SSL connections (i) Confidentiality using conventional encryption. (ii) Message Authentication using a Message Authentication Code (MAC).SSL provides security for web based applications. The Handshake Protocol, Change Cipher Spec Protocol, Alert Protocol are used in data management for SSL exchanges it has not a single protocol but it has two layer protocols[14] Authenticate the server to the client. Allow the client and server to select cryptographic algorithms, or ciphers, which they both support optionally, authenticate the client to the server. Use public key encryption techniques to generate shared secret. Establish an encrypted SSL connection assured.

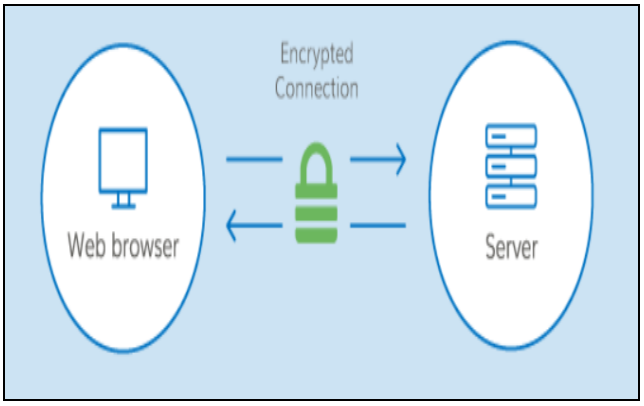

Fig 4.Data Management in SSL

In cloud data storage system, users store their data in the cloud and no longer possess the data locally; this involves the use of strong network traffic encryption techniques such as Secure Socket Layer (SSL).

III. RELATED WORK

Cloud computing is one of the largely significant secure way to giving out information to the business background Based on the highly developed services in the technology of IT many kinds of network services are accessible in the protected along with unprotected ways[8].. Different security measurements are discussed deeply in various papers and some trusted third parties they can assure some security (Data confidentiality, integrity and availability) in cloud environment. It is noted that not any of them converse obviously about a universal standard, SLA (Service Level Agreement) policies such that: what does consumer need to know and what does service provider need to provide and some other security measurements and quality of services. But the main goal is to provide adequate security for cloud services.

IV. CONCLUSION

The paper describes the convention of SSL in securing the data transmitted throughout data centre in private cloud computing for data managements protocol provides total fortification to data which is sent over the communication scheme. The paper shows that it provides the fortification against eavesdropping and other submissive attacks. It also momentarily key swap over protocol through handshake protocol authenticates parties who have certificates signed by a trusted certificate authority. It has also exposed a number of ways in which the robustness of the SSL protocol can be improved.

REFERENCES

[1]. O. Freier P. Karlton and P. C. Kocher. *The SSL Protocol,Version 3.0. NetscapeCommunications*, 1996, http://wp.netscape.com/eng/ssl3/draft302.txt (2003).
[2]. National Institute of Standards and Technologies. *DataEncryption Standard*. U.S.Dpt. of Commerce, December 1993.
[3]. *ANSI*. American National Standard for Financial InstitutionKey Management (wholesale). ANSI, 1985
[4]. R. Rivest. *A Description of the RC2(r) EncryptionAlgorithm*, RFC 2268. Network
[5]. *Working Group*, 1998, ftp://ftp.rfc-editor.org/innotes/rfc2268.txt (2003).
[6]. *Schneier. Applied Cryptography*, 2ed. John Wiley andSons, 1996.
[7]. R. Rivest. *TheMD-5 Message-Digest Algorithm*, RFC1321. John Wiley andSons,1996, ftp://ftp.rfc-editor.org/innotes/rfc1321.txt (2003)
[8]. Chetan M Bulla , Satish S Bhojannavar and Vishal M Danawade, "Cloud Computing: Research Activities and Challenges", International Journal of Emerging Trends & Technology in Computer Science, Vol 2, No. 5, 2013, pp.206-214
[9]. Palvinder Singh, Er. Anurag Jain, "Survey Paper on Cloud Computing", International Journal of Innovations in Engineering and Technology, Vol 3 No. 4, 2014, pp.84-89
[10]. *.D2RQ*. http://sites.wiwiss.fu-berlin.de/suhl/bizer/D2RQ/
[11]. *Virtuoso*.http://virtuoso.openlinksw.com/wiki/main/Main/VOSSQL
[12]. P. Mell and T. Grance, The NIST definition of cloud computing
[13]. S. Jha et al., Programming Abstractions for Large-scale Distributed Applications, submitted to ACM Computing Surveys;draftathttp://www.cct.lsu.edu/Bsjha/publications/dpa_surveypaper.pdf.
[14]. Semantic web technologies in SSLbased cryptography data management D.Meenakshi,T.Malathi,V.Karthika Devi ijesird , Vol. II Issue IX March 2016/596-599

Authors Profile

Ms. D.Meenakshi pursed Bachelor of Science from University of Bharthidasan, Trichy in 2000 and Master of Science from Bharthidasan, University in year 2002. She is currently working as Assistant Professor in Department of Computer Sciences, Shrimathi Indira Gandhi College, Trichy,India.. She has published more than 10 research papers in reputed international journals and conferences including IEEE and it's also available online. Her main research work focuses on Cryptography Algorithms, Network Security, Cloud Security and Privacy, Wireless communication.,Image Processing.She has 9 years of teaching experience .

Ms. V.Karthikadevi pursed Bachelor of Science From University of Bharthidasan, Trichy in 1995 and Master of Computer Applications from Bharthidasan, University in year 1999. She is currently working as Assistant Professor in Department of Computer Sciences, Shrimathi Indira Gandhi College, Trichy,India.. She has published more than 5 research papers in reputed international journals and conferences including IEEE and it's also available online.. Her main research work focuses on Cryptography Algorithms, Network Security, Cloud Security and Privacy, Big Data Analytics, Data Mining, IoT and Computational Intelligence based education. She has 16 years of teaching experience .

