A Novel Cryptographic Framework For Cloud Computing

Neha Mittal[1], Charu Gupta[2], Dr. A.K. Mohapatra[3]

[1] *Student, Information Technology Department, Indira Gandhi Delhi Technical University For Women, Delhi, India*
[2] *Assistant Professor, Information Technology Department, Indira Gandhi Delhi Technical University For Women, Delhi, India*
[3] *Associate Professor, Information Technology Department, Indira Gandhi Delhi Technical University For Women, Delhi, India*

Abstract

At present , information is stored in the cloud directly by the client or third party with the help of a trusted third party .Since the cloud framework works on a sharing platform and as a result there are many security issues related to its authentication ,integrity and ownership. As a result, a cryptographic framework is required which encounters various cyber attacks like phishing ,man-in - the- middle attack , session-hijacking ,packet sniffing ,DNS attacks and cookie poisoning in a better way .In this paper ,we have proposed a security framework which encounters attacks and consists of three security layers. Layer 1 comprises the stakeholders involved in implementing the framework .Layer 2 provides the use of cryptography from user to cloud communication, security inside virtual machine and Layer 3 describes issues which are mitigated at each working layer level. According to the proposed framework ,bottommost section refers to the stakeholder and is input layer which is the cloud service provider ,cloud tenant or the combination of both cloud service provider and cloud tenant involved in the framework. The intermediate section of framework depicts the working layers ,encryption levels and basis and encryption ways .First sub section of intermediate section describes three working layers of cryptography which includes physical level dealing with hardware, virtual level dealing with middleware and application level dealing with application .Second sub section of intermediate section describes encryption levels and basis The topmost layer which is the output layer depicts the issues which are handled at each working layer level.

Key Words: *Cloud computing ,Cryptography , Encryption technique , Security issue and Virtualization*

----------***----------

1. INTRODUCTION

Cloud computing is an emerging trend in information technology for efficient use of IT assets .The emergence of cloud computing has offered various advantages like scalability,elasticity,easymanagement,costreduction,uninterrupted services ,green computing and disaster management. Cloud computing is used in a variety of applications like Customer resource management (CRM),video conferencing ,IT service management, Web content management, business intelligence, research ,sales ,social networks, database, file storage ,centralizing email communications ,new medical treatments and space [11]. As a flipping coin has two sides ,similar is with cloud computing .As discussed above ,its advantages but since cloud computing is a multiuser environment and has no geographical boundaries due to which data can reside anywhere across geographical boundaries. This made cloud prone to several threats.

Cloud computing is suffering from several attacks like man-in –the-middle attack ,packet sniffing ,cookie poisoning ,DNS attacks .phishing and session hijacking attack etc. [14] and following needs immediate attention .So, these issues will be addressed by proposed novel framework.

1.1 SECURITY ISSUES

1. Data Security :To ensure data security one can use encryption (which involves conversion of plaintext into cipher text) over cloud to be implemented in multiple deployment models.

2. Storage security [5] :To protect the data at rest is very important. For this also ,encryption can be used as a method for user to share data to a targeted user or device. For providing storage security, proxy-re encryption technique is to be used.

3. Data privacy and data confidentiality :As we know that the issues related to user data that is outsourced to cloud are solved using cryptographic techniques which includes privacy of data at rest or in transit. Confidentiality which ensures that only desired recipient has access to message is also ensured by encryption.

4.Data transfer :All data and traffic travels through the internet between cloud computing customers and cloud provider network [11].If data is transferred in plaintext it is prone to various attacks .Solution is to encrypt the data transferred by the cloud service provider.

5. Insecure Interfaces or APIs: Customers use various software interfaces to interact with cloud service providers .These application programming interfaces are also used in management ,monitoring ,orchestration and provisioning of cloud service [15].If the set of interfaces used are weak , organizations are very prone to various security threats such as clear text authentication ,improper authorization etc. Cryptography is viewed as one of the mitigation strategy

So, after study and analysis of cloud security challenges and attacks , an attempt is made to propose a novel cryptographic framework for cloud computing. The paper is organized as follows :In section 2, we summarized the related work. Section 3 discusses the attacks in cloud computing environment .Section 4 discusses the proposed framework .Section 5 discusses the conclusion and future work.

2. RELATED WORK

Bouyad and Blilat [1] provides a detailed analysis of cloud security problem for understanding to stakeholders.The problem is investigated from multidimensional perspective like cloud stakeholder perspective ,cloud service delivery models perspective etc .It also highlights the features that should be incorporated into proposed solution .However ,this paper fails to address every macro and micro level element and its appropriate solution design and deployment for tenants. Amanatullah et al [3] discusses an overview of cloud computing architecture which is simple and basic involving actors and various services management like architecture service, business support and operation support and the submodules involved in it. However this paper fails to conduct a research to combine different frameworks into one cloud . Jaber and Zolkipli [4] discusses cloud computing ,its features ,service models ,deployment models and use of encryption in cloud computing .This paper also sheds light on work done on cryptography for cloud computing .However this paper fails to deal with implementation of cryptography in cloud computing. Sadkan and Abdulraheem [5] describes various types of cryptographic systems and focus on those of available cryptosystems used in cloud networking environment which includes symmetric searchable encryption (SSE),asymmetric searchable encryption (ASE),elliptic curve cryptosystems(ECC) ,AES algorithm,homomorphic encryption etc .In this paper evaluation of parameters is used to compare cryptosystems .In this paper evaluation of parameters is used to compare cryptosystems .As we know cryptography ensures data privacy . Sashank [6] discusses various theoretical encryption techniques including fully homomorphic encryption ,Instance hiding etc .Also it discusses the challenges with current cryptographic techniques and depicts that they fail to cover some stated privacy requirements. However ,this paper concludes with a need for further generalization and formulation of all stated techniques and to focus on the formulation of theory behind computational privacy to achieve better solutions .Mohamed and Abdelkader et al [7] emphasis that single security architecture fails to satisfy the customers with different demands .Also ,different cloud providers solves data security problem by encryption of data by using encryption algorithms .This paper focuses on data security problem in cloud computing and presents the proposed data security model of cloud computing based on study of cloud architecture .The proposed data security model has three layers including strong authentication ,data encryption ,data integrity and fast data recovery. Different application areas and its suitable encryption techniques are also discussed .The paper also depicts the implementation of software which provides two factor authentication and compares between eight modern encryption algorithms using NIST statistical tests using Amazon EC2 ubuntu microinstance to find highest secure algorithm .Abuhussein, Bedi et al [9] presents an overview of cloud computing advantages ,applications and focus on attributes which ensures the cloud security and privacy .The paper states that attributes can also be used by consumers to compare various cloud computing services and by cloud service providers to offer better cloud solutions .However ,this paper fails to address new attributes for securing the different parts of cloud computing environment .Fawaz S. Al-Anzi ,Ayed A. Salman et al [10] discusses the concept of cloud computing ,advantages and problems in cloud computing along with description of proposed solutions .The paper focuses on data security in cloud at the service provider end ,explains data related vulnerabilities and threats and also proposes a network storage architecture of data which ensures availability ,scalability and security by depending upon multiple service providers for the better secure storage of outsourced data .Also ,analysis of security and performance of proposed architecture is being done. Nitin and Ashutosh [13] provides brief introduction to cloud computing and its applications in cryptography. Also ,the article discusses challenges in area of cloud storage ,communication and virtualization. Also ,an attempt is made to discuss how existing cryptographic mechanisms contribute to improve the security posture of cloud environment. Tripathy and Mishra [15] provides overview of cloud computing and the security issues that arise in cloud computing.It also highlights technical security issues arising from the usage of cloud services and key security issues related to cloud computing .The paper also proposes a secure cloud architecture focusing on single sign on ,increased availability ,single management console ,virtual machine protection and concludes with various lines of defense which includes firewall, ,integrity monitoring, intrusion detection and prevention ,log updation and malware implementation .However in future the proposed architecture may be modified when used for implementing this cloud security architecture.

3. ATTACKS IN CLOUD COMPUTING ENVIRONMENT

The description of attacks in cloud computing environment are as follows:-

1. Man in the Middle attack :This network based attack will occur when SSL is not used properly. ARP spoofing scheme is a man-in –middle attack .In this attack ,user 1's machine is in belief that it is communicating with user 2's workstation and vice-versa [14].

2. Packet Sniffing :This is a network attack which catches network movement at Ethernet frame level [14].After catch ,this information could be investigated and secured data might be removed.

3. DNS attack :This attack occur when server called client by name but the client has been traced to some malevolent cloud rather than the one originally requested[14].

4. Cookie Poisoning :This attack involves modification of cookie to have an unauthorized access to a site page .Cookies hold client personal identifiable information and once these cookies are receptive ,these cookies might be imitated to launch an attack [14].

5. Phishing attack :Phishing is an attack in which personal information of unsuspecting user is retrieved by sending emails ,webpage links or instant messages [14].These links appear to be authenticated but leads to fake access locations.

6.Metadata spoofing attack: In this attack ,an attacker modifies the Web Services Description Language (WSDL) service file which contain description of various services [15] .This attack is performed by intervention of service code from WSDL file at delivery time of service.

7. Side Channel Attack: Firstly, an attacker places a malicious cloud machine in close proximity to a target cloud server and then initiate a side channel attack which involves using side channels to gather information about co-resident virtual machine instances .This attack targets cryptographic implementations of algorithms.

The attacks in cloud computing environment with possible solution are listed in table below:

Table 1: Possible attacks and their solutions in Cloud Environment

Attack Name	Solution
1. Man in the Middle attack	(a) Use SSL. (b) Use encrypted session negotiation and encrypted communication channels. [14]
2. Packet Sniffing	(a) Encryption of sensitive information and passwords. [14] (b) Encoded SSL or TLS associations with mail servers.
3. DNS attacks	(a) Use cryptographic electronic marks with public key certificates for secure DNS. [14]
4. Cookie Poisoning	(a) Implementing an encryption scheme for the cookie data.[14]
5. Phishing attack and Session Hijacking	(a) Use of encryption [14]
6. Metadata spoofing attack	(a) Information about services and applications should be kept in encrypted form. [15]
7. Side Channel attack	(a) Random Encryption and decryption [15]

4. PROPOSED FRAMEWORK

In this Section a brief discussion is made on the proposed framework.. .In this paper, a layered approach for security through cryptographic framework has been proposed which handles attacks and consists of three security layers. Layer 1 comprises the stakeholders involved in implementing the framework. Layer 2 provides the use of cryptography from user to cloud communication and security inside virtual machine and Layer 3 describes issues which are mitigated at each working layer level.

According to the proposed framework, bottommost section refers to the stakeholder and is input layer which is the cloud service provider ,cloud tenant or the combination of both cloud service provider and cloud tenant involved in the framework.

The intermediate section of framework depicts the working layers , encryption levels and basis and encryption ways .First

sub section of intermediate section describes three working layers of cryptography which includes physical level dealing with hardware ,virtual level dealing with middleware and application level dealing with applications.

Second sub section of intermediate section describes encryption levels and basis .Encryption levels are Full disk ,Full directory ,File level and Application level .In encryption of data at the disk level: the operating system ,the applications in it and the data and applications use are all encrypted simply by existing on a disk that is encrypted .Ex :I-scsi encryption .In directory level entire data directories are encrypted or decrypted as a standalone unit .In file level ,individual files are encrypted .In application level ,the applications are responsible for encryption and decryption of application-managed data .Encryption basis discusses three types :stream basis ,Block basis and File basis .Stream basis is used to encrypt or decrypt individual data units .Block basis forms group of individual data units of fixed size and then encrypt or decrypt these blocks. Cryptographic hash function takes an arbitrary long stream of input data and outputs a short , fixed length hash and hash is used to verify integrity of data .The last subsection of intermediate section describes encryption ways. Encryption is done of data at rest or data in transit/motion .Data at rest refers to the data in computer storage, including files stored on computer, corporate files on server or files stored as an off-site backup[11].Data in motion refers to data as it moved from a stored state as a file or database to another form in the same or to a different location. Data at rest is encrypted using encryption schemes which may be symmetric scheme, asymmetric scheme ,homomorphic scheme ,identity based encryption and attribute encryption etc and encryption of data in motion is done with use of protocols like SSL, TLS and SSH. Symmetric Cryptography involves encryption and decryption of data using common or shared key between sender and receiver. Example of such schemes are: Advanced Encryption Standard(AES),Data Encryption Standard (DES),Triple-DES and Blowfish scheme etc.Asymmetric cryptography involves two keys:one for encryption of plaintext into ciphertext and other for decryption of cipher text into plaintext. Example of such schemes are: RSA, Diffie Hellman Key Exchange etc. Homomorphic encryption ensures data confidentiality and privacy by processing of encrypted data and obtain an encrypted result which when decrypted matches the result of the operations performed on plaintext. Identity Based Encryption is a form of asymmetric cryptography in which some server of third party uses identifier like email address to generate keys for encryption and decryption of electronic messages .Attribute Based encryption is used to protect to protect data at rest and the encryption is done using a set of attributes and only the authorized person possessing the attributes can decrypt the data .Attribute Based encryption can be Key Policy attribute based encryption, cipher text policy attribute based encryption or Multi Authority attribute based encryption .This layer also outlines the various usage areas of proposed cryptographic architecture which includes storage ,communication ,virtualization,processing,software(O.S,D.B.M.S),transmission ,services,authentication and identity management.

The topmost layer which is the output layer depicts the issues which are handled at each working layer level..At Physical level, issues like infrastructure security and hardware security are encountered .Virtual level encounters issues like Virtual machine security ,Patch management ,Network Security ,Backup and Recovery ,Risk management and Vulnerability management .Application Level encounters issues like Host Security ,Client Server Protection ,Data Isolation and Recovery ,Disaster Recovery ,Incident management ,access security ,data integrity and privacy.

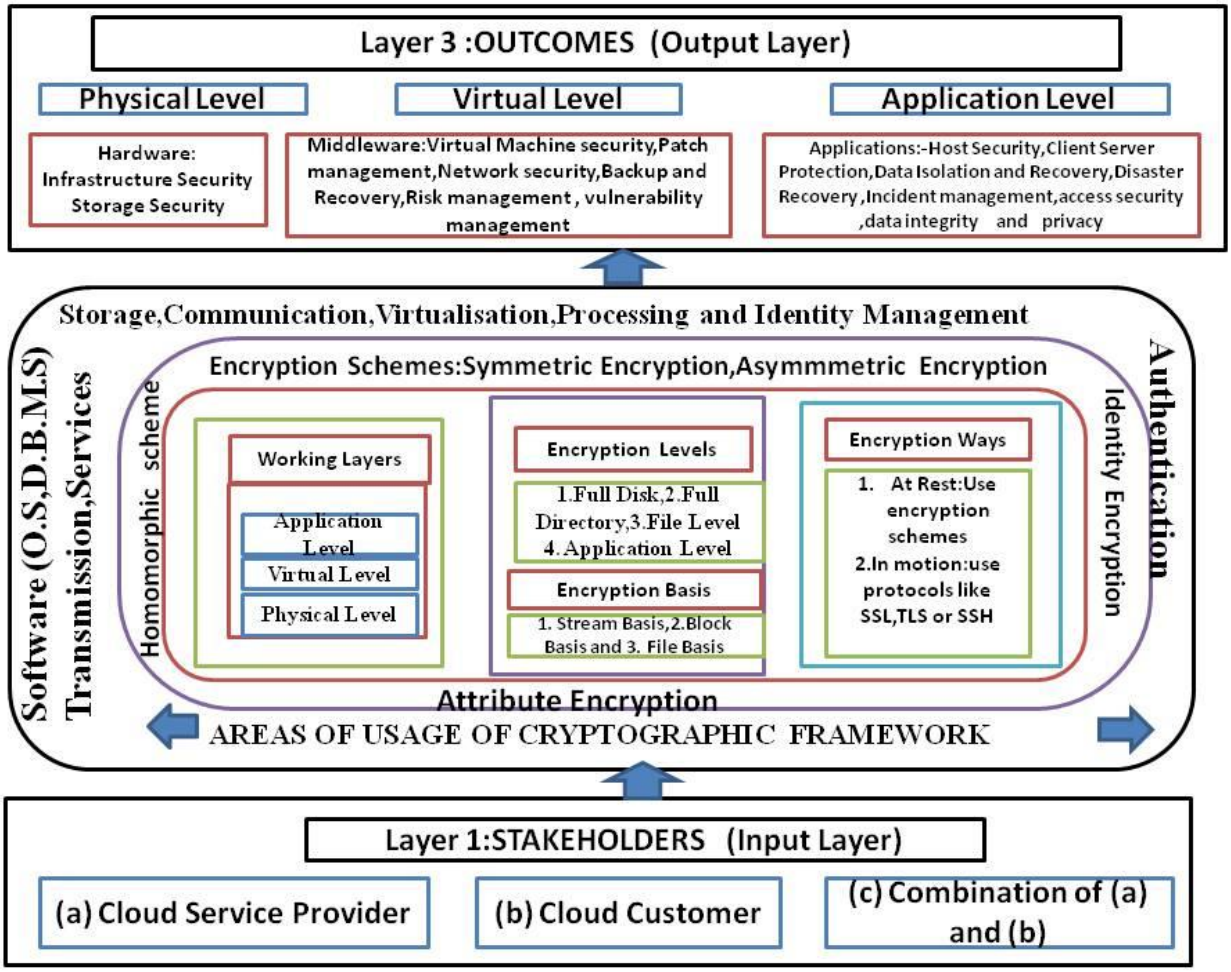

Fig 1:CRYPTOGRAPHIC FRAMEWORK FOR CLOUD

5. CONCLUSION AND FUTUREWORK

This paper discusses a novel cryptographic framework for cloud computing .We discussed important components in proposed framework .The proposed framework can address most of attacks like man-in –the-middle-attack ,packet sniffing ,cookie poisoning ,DNS attacks etc in cloud computing dealing with security in confidentiality ,integrity and availability of data and communication.

In future, the proposed framework may be modified to incorporate additional features and technological advancements to enhance security .We would like to evaluate the performance of proposed architecture .Also we would like to combine various cloud computing frameworks to form a single unified framework.

REFERENCES:-

[1]. Anas BOUAYAD and Asmae BLILA T et al
2012 IEEE Issue No: 978-1-4673-2725-1/12,pp(26-31)

[2]. Yanuarizki Amanatullah and Charles Lim et al Toward Cloud Computing Reference Architecture: Cloud Service Management Perspective IEEE

[3]. Aws Naser Jaber and Mohamad Fadli Bin Zolkipli Use of Cryptography in Cloud Computing Issue No: 978-1-4799-1508-8/13,pp(179-184) 2013 IEEE International Conference on Control System, Computing and Engineering, 29 Nov. - 1 Dec. 2013, Malaysia

[4]. Dr EngSatiar B. Sadkan , Farqad H. Abdulraheem

An Analytical Study for Security Evaluation of Cryptosystems used in Cloud Networking The First International Conference of Electrical ,Communication, Computer, Power and Control Engineering, ICECCPCE'13/December17-18, 2013 IEEE

[5]. Sashank Dara
Cryptography Challenges for Computational Privacy in Public Clouds
Cisco Systems India Pvt Ltd, International Institute of Information Technology ,Bangalore, India IEEE

[6]. Eman M. Mohamed and Hatem S. Abdelkader et al
Enhanced Data Security Model for Cloud Computing The 8th International Conference on Informatics and Systems (INFOS2012) - 14-16 May
Cloud and Mobile Computing Track ,pp(CC12 – CC17)

[7]. Akhil Behl
Emerging Security Challenges in Cloud Computing
Issue No: 978-1-4673-0126-8/11 pp(179-184) 2011 IEEE

[8]. Abdullah Abuhussein, Harkeerat Bedi et al
Evaluating Security and Privacy in Cloud Computing Services: A Stakeholder's Perspective
Issue No:978-1-90830-08-7,pp(388-395) 2012 IEEE
The 7th International Conference for Internet Technology and Secured Transactions (ICITST-2012)

[9]. Fawaz S. Al-Anzi ,Ayed A. Salman et al
Towards Robust, Scalable and Secure Network Storage in Cloud Computing
Issue No:978-1-4799-3724-0/14 pp(51-55) 2014 IEEE

[10]. Dimitrio Zissies , Dmitrios Lekkas
Future Generation Computer Systems
Addresing cloud computing security issues
2010 Elsevier Publication

[11]. Syngress : Securing the cloud –Cloud computer security techniques and tactics.pdf

[12]. Nitin Singh Chauhan and Ashutosh Saxena
Cryptography and cloud security challenges
CSI Communications ,May 2013

[13]. Alok Tripathi and Abhinav Mishra
Cloud Computing security Considerations, IEEE

[14] . Navroz Kaur Kahlon and Preet Kamal
Attacks and Their Countermeasures in Cloud Computing 2014,Discovery Publication,Volume 15,Number 39,(23- 26),April 7,2014

[15]. Kashif Munir1 and Sellapan Palaniappan2
Security Threats/Attacks Present in Cloud Environment
IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.12, December 2012