ISSN:0975-9646

Cryptographic Techniques, Threats and Privacy Challenges in Cloud Computing

Jissy Ann George[1], Dr.M.Hemalatha [2]

[1]*Research Scholar, Department of Computer Science, Karpagam University Coimbatore, India*

[2]*Professor, Department of Computer Science, Karpagam University Coimbatore, India*

***Abstract*— Cryptography is essential for the security and integrity of the data that is stored in the cloud. Several cryptographic techniques are used to protect the integrity of data for various applications. A particular security method makes use of different cryptographic techniques to encrypt data and make it into an un-readable form, which can then be decrypted only with the help of a key. A number of cryptographic techniques are available for use in protection of data in various applications. Cryptographic techniques are essential for the confidentiality of the data saved. Cloud computing is used to share resource as service, software as service, infrastructure as service, platform as service to the clients. The use of cryptography in the cloud will enable the security of the data being shared. Confidentiality and integrity of data in data security are essential in the cloud. This paper presents an overview of the cryptographic techniques, security and privacy challenges related to public cloud computing.**

***Keywords*— Cloud computing, cryptographic techniques, domains, encryption, security issues, threats**

I. INTRODUCTION

Privacy of data is of extreme need in this present time and cryptography plays a significant role. Security issues need to be addressed in various areas. At present there are a number of cryptographic algorithms which have been designed for the protection of data in various applications. Cryptography [1] refers to the science of designing ciphers, namely, block ciphers, stream ciphers and hash functions. Encryption refers to the method of converting ordinary text to a secret text to protect its integrity. There are primarily two categories of encryption algorithms [2] which are mainly: symmetric algorithms such as DES, AES, Triple DES and asymmetric or public-key encryption algorithms such as RSA, Diffie-Hellman, ECC, etc. The difference is in the way the keys are used. In symmetric key encryption, the person who is sending the data and the person who is receiving the data share a key which is kept secret. This is then used to encrypt and decrypt the messages. In asymmetric key encryption, two keys are involved wherein one is used for encryption (this is publicly available) and the other is used for decryption (this is kept secret).

Cloud Computing is very popular as many companies are now into cloud platforms. A major barrier for cloud adoption is lack of security. Cloud computing security is vulnerable to many issues such as virtualization infrastructure; software platform; identity management and access control; data integrity; confidentiality and privacy; physical and process security aspects; and legal compliance in cloud. Important research directions in cloud security in areas such as Trusted Computing, Information Centric Security and Privacy Preserving Models [3]. Cloud computing enables organizations and individuals to work from anywhere in the world on demand. Cloud computing enables appropriate, on-demand network access to computing resources such as infrastructure, applications and services [4]. Cloud computing can be employed under many models, used in various architectures.

The use of cryptography is very important for the maintenance of security in the cloud. This paper gives a comparative analysis of the several cryptographic techniques utilized in the security process of the cloud. It also addresses the various security issues and domains in the cloud computing environment. There are many cryptographic techniques that have been in use for security in the cloud. This article reviews some of the techniques that have been used in the cloud environment. It gives a mapping of the top nine threats faced in the cloud and the security domains in which these fall into. The paper initially discusses the various security issues and threats in the cloud. An overview of the various cryptographic techniques is presented next. Using the mapping as a reference, various controls can be applied to the threats with the use of the cryptographic techniques that have been used. Finally, possible enhancements that can be done in this area are suggested.

II. PRIVACY CHALLENGES, SECURITY DOMAINS AND TOP THREATS IN THE CLOUD

The privacy challenges in public cloud are namely: lack of user control, potential unauthorized secondary usage, data proliferation, trans border data flow, dynamic provisioning, retention of data, ensuring data has been lost, privacy breaches [5]. Security challenges would include access, control over data lifecycle, availability and backup, lack of standardization, multi-tenancy and audit. Trust challenges [6] are weak trust relationships and lack of customer trust. The different security issues were also classified into levels [7] that exist in cloud environments. Different solutions were provided to deal with the security issues in the cloud as per the type of security provided. Software policies to allow clients to use the security means they need at the levels where the issues happen.

Cloud security was grouped into a model comprised of seven categories [8] which were network security, interfaces, data security, virtualization, governance,

compliance and legal issues. The security guidance provided by the Cloud Security Alliance (CSA) defines fourteen security domains [9] and the top nine threats [10] in the cloud environment and these are listed in Table 1. The table gives a brief account of the guidance that is delivered for each security domain. A mapping of the various threats to the security domains is listed in Table 2.

TABLE I
GUIDANCE ON THE FOURTEEN SECURITY DOMAINS

Domain No.	**Security Domains**	**Guidance on**
D 1	Cloud Computing Architectural Framework	Conceptual framework for the Cloud
D 2	Governance and Enterprise Risk Management	Identification and implementation of appropriate organizational structures, processes, and controls
D 3	Legal Issues: Contracts and Electronic Discovery	Legal issues that can be raised by moving data to the cloud, and issues in a cloud services agreement
D 4	Compliance and Audit Management	Understanding on the existing compliance and audit standards, processes, and practices
D 5	Information Management and Data Security	Data Security Lifecycle for evaluating and defining cloud data security strategy
D 6	Interoperability and Portability	Designing for portability and interoperability
D 7	Traditional Security, Business Continuity, and Disaster Recovery	Sharing a common understanding of traditional security with cloud service.
D 8	Data Center Operations	Construction or remodelling of data centers for the cloud
D 9	Incident Response	Efficient and effective handling of security incidents that involve resources in the cloud
D 10	Application Security	Practices that must be followed when developing or migrating applications to the cloud
D 11	Encryption and Key Management	Binding cryptographic operations and key management to corporate identity systems
D 12	Identity, Entitlement, and Access Management	Design the common service layers to act independently to enable the removal of applications without sacrificing existing information security policies and procedures
D 13	Virtualization	Virtualization-related security issues
D 14	Security as a Service	Securing systems and data in the cloud through cloud-based services.

TABLE II
MAPPING OF THE NINE CRITICAL THREATS WITHIN THE SECURITY DOMAINS

Threat	**D1**	**D2**	**D3**	**D4**	**D5**	**D6**	**D7**	**D8**	**D9**	**D10**	**D11**	**D12**	**D13**	**D14**
Data Breaches					√					√		√	√	
Data Loss					√					√		√	√	
Account Hijacking		√			√		√		√		√	√		
Insecure APIs					√	√			√	√	√	√		
Denial of Service								√	√	√			√	√
Malicious Insiders		√			√						√	√		
Abuse of Cloud Services		√							√					
Insufficient Due Diligence		√	√					√	√					
Shared Technology Issues	√				√						√	√	√	

III. Cryptographic Techniques In The Cloud

A. Identity Based Encryption

Identity-Based Encryption (IBE) [11] helps in public key and certificate management for Public Key Infrastructure (PKI). Outsourcing computation was put into IBE and an IBE scheme in the server-aided setting was proposed. The key generation operations are given to a Key Update Cloud Service Provider and thus only simple operations are left.

An analysis of the various encryption techniques used such as homomorphic encryption, searchable and structured encryption, identity-based encryption and signature based encryption [12] yielded the following. IBE is a form of public key cryptography in which a third party server uses a simple identifier, such as an e-mail address, to generate a public key that can be used for encrypting and decrypting electronic messages. This kind of encryption reduces the complexity of the encryption process for both users and administrators. In the Linear Search algorithm, a symmetric encryption algorithm is used to encrypt the plain text. An identity based signature scheme is deterministic if the signature on a message by the same user is always the same. Homomorphic encryption alludes to encryption where plain texts and cipher texts both are treated with an equivalent algebraic function. A public key encryption with keyword search (PEKS) scheme contains four polynomial time algorithms. In ABE, the attributes and policies of the message and the user decides which user can decrypt a cipher text. A central authority will create secret keys for the users based on attributes/policies for each user.

B. Attribute-Based Encryption (ABE)

Attribute based encryption are of many types. The most common of them being, key attribute-based and cipher text attribute based. A new encryption technique, multi authority hierarchical attribute based encryption [13] is suggested. This is compared with two types of attribute based encryption techniques which are mainly key policy and cipher text policy. Private Key of user ensures the access policy of the algorithm. The main difference between these two types of attribute based encryption techniques is that one is dependent on the access policy. In Key policy attribute based encryption, the cipher text is connected with set of attributes and provides data owner with key and policy pair. The message is decrypted if the attribute in the cipher text complies with the key access policy. Cipher text is connected with access policy and is decrypted on satisfaction of the attributes. The suggested technique was tested using NIST Statistical test and it was found that the multi authority hierarchical attribute based encryption ensured most security in data.

An enhanced version of CP-ABE was CP-ASBE (Cipher text Policy Attribute Set Based Encryption) [14] scheme. It added a hierarchical structure that provides more scalability and flexibility. This enables the party that manages master keys for distribution and domain authorities who then give the owners data needed for encryption or decryption. Data are also stored on the storage of cloud provider. The security of the scheme is equivalent to security rate in CP-ABE [15].

C. Fully Homomorphic Encryption

Homomorphic encryption ensures privacy of data in communication, storage or in use with tools similar to conventional cryptography, but with extra features of computing over encrypted data, searching an encrypted data, etc. The main disadvantage of traditional encryption techniques is that to manipulate the data, it has to be decoded first. Fully homomorphic encryption (FHE) performs computation with the encrypted data and this is sent. A scheme was devised wherein the calculations can be performed securely in the cloud without the server knowing the content of the data sent or what function needs to be performed. The design used symmetric homomorphic encryption [16] to enhance data security which allowed performing computations on encrypted data without using secret key of client. The encryption used is also symmetric thereby reducing the MIPS rate as well.

Another study on Fully Homomorphic Encryption implemented symmetric key encryption scheme with fully homomorphic evaluation capabilities. A fully homomorphic scheme with symmetric keys [17] was incorporated into an application. Majority of the schemes proposed so far only involved a single party, whereas their scheme ensured multiparty computation.

D. Modern Encryption Algorithms

A study was conducted on seven different encryption algorithms namely: AES, DES, 3DES, RC4, Blowfish, RSA, and Diffie-Hellman in XCP cloud environment. The parameters that were taken into consideration were data, size of the input data and the size of the key for the various cryptographic algorithms taken. The data security in cloud environment and performance of the above algorithms was considered. It was seen that the symmetric encryption techniques were [18] [19] [20] faster than the asymmetric encryption techniques. There was an inverse proportion relation between the running time and the size of the input file. As the size of the input file increased, the running time decreased except for the RSA algorithm where the running time changed slightly with the input file size increase.

Another evaluation of the common cryptographic techniques, MARS, AES, DES, 3DES, RC4, RC6, Two-Fish, and Blow-Fish were conducted on a desktop computer and on Amazon EC2 Micro Instance cloud environment [21]. NIST statistical testing was conducted and Pseudo Random Number Generator (PRNG) was used for the randomness test. The algorithms were executed using Java Cryptography Extensions (JCE). The effectiveness of the algorithms were obtained from the simulation results. In Amazon EC2, Blowfish RC6, AES and DES results were a little better than other-encryption methods and AES was concluded as the best but Blow-Fish and DES time-wise. In desktop, RC6, AES, Blowfish, DES and RC4 results were slightly better than other and RC6 was considered best for PC environment, but Blow-Fish is better time-wise.

A working system design for data security in cloud storage with DES algorithm was also devised [22]. The design comprised of components that would provide security at the user and admin level. Components involved in the design were namely, client, system, cloud data

storage, cloud authentication server, unauthorized data modification and corruption, data security, adversary. The system had dynamic data support which included block update, delete, and append operations. Data dependability was ensured through the use of erasure correcting code in the file distribution preparation. Data error localization was achieved with the help of the homomorphic token with distributed verification of erasure coded data. DES algorithm with erasure-correcting technique was used to provide data security with integrity.

Another system which was proposed was efficient hybrid cryptography system, Hybrid Vigenere Caesar Cipher Encryption (HVCCE) [23]. This was aimed in preventing the cloud infrastructure in three main places, client location, network and in server. The system was designed such the time taken for decrypting the cipher text by the hackers would be higher than a single system.

IV. Conclusion

Cryptographic techniques in the cloud must enable data protection, availability of the data and sharing of data. Symmetric or asymmetric encryption methods are not alone sufficient for the needs of cloud computing environment. A combination of two or more of the cryptographic techniques will aid in the security of data. This paper has aimed at giving a general overview of the various cryptographic techniques that are being employed for use in the cloud computing environment. The mapping of the threats under the security domains gives an insight onto the domains that need to be made most secure. Securing the domains that are most often used with a strong cryptographic technique, can enable optimized security in the cloud. Future work in this area will include an analysis of these techniques on a cloud computing environment to find the most optimized algorithm which will ensure data security in the cloud.

References

[1] [Online]. Available: http://en.wikipedia.org/wiki/Cryptography.

[2] Jissy Ann George, "SURVEY OF CRYPTOGRAPHIC TECHNIQUES: A SOLUTION FOR OPTIMIZED SECURITY," AMA INTERNATIONAL UNIVERSITY, CCS JOURNAL, vol. 2, no. 1, pp. 124-136, 2012.

[3] Subhashis Sengupta, Vikrant Kaulgud and Valhi Saujanya Sharma, "Cloud Computing Security-Trends and Research Directions," Services (SERVICES), 2011 IEEE World Congress on, pp. 524-531, 2011.

[4] Wayne Jansen and Timothy Grance, "Guidelines on Security and Privacy in Public Cloud Computing," National Institute of Standards and Technology, Special Publication 800-144, December 2011.

[5] Siani Pearson and Azzedine Benameur, "Privacy, Security and Trust Issues Arising from Cloud Computing," in 2nd IEEE International Conference on Cloud Computing Technology and Science, USA, 2010.

[6] Mhammed Chraibi, Hamid Harroud and Abdelilah Maach, "Classification of Security Issues and Solutions in Cloud Environments," in IIWAS '13 Proceedings of International Conference on Information Integration and Web-based Applications & Services, New York, 2013.

[7] Issa M. Khalil, Abdallah Khreishah and Salah Bouktif, Azeem Ahmad, "Security Concerns in Cloud Computing," in 2013 10th International Conference on Information Technology: New Generations, China, 2013.

[8] Nelson Gonzalez, Charles Miers, Fernando Redígolo, Tereza Carvalho, Marcos Simplicio, Mats Näslund and Makan Pourzandi, "A quantitative analysis of current security concerns and solutions for cloud computing," in 2011 Third IEEE International Conference on Coud Computing Technology and Science, Greece, 2011.

[9] CSA, "Security guidance for critical areas of focus in cloud computing," Cloud Security Alliance, Tech, Rep., 2011.

[10] Aaron Alva et. al, "The Notorious Nine Cloud Computing Top Threats in 2013," Cloud Security Alliance, 2013.

[11] Jin Li, Jingwei Li, Xiaofeng Chen and Chunfu Jia, "Identity-based Encryption with Outsourced Revocation in Cloud Computing," IEEE TRANSACTIONS ON COMPUTERS, vol. 64, no. 2, pp. 425-437, 2015.

[12] Simarjeet Kaur, "Cryptography and Encryption In Cloud Computing," VSRD International Journal of Computer Science and Information Technology, vol. 2(3), pp. 242-249, 2012.

[13] R. Manjusha and R.Ramachandran, "Comparative study of attribute based encryption techniques in cloud computing," Embedded Systems (ICES), 2014 International Conference on, pp. 116-120, 2014.

[14] Wan Z, Liu and J, Deng R, "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing," Information Forensics and Security, IEEE, vol. 7, no. 2, pp. 743-754, 2012.

[15] Bobba R,, Khurana H and Prabhakaran M., "Attribute-sets: A practically motivated enhancement to attribute-based encryption," Computer Security–ESORICS 2009, pp. 587-604, 2009.

[16] Bhabendu Kumar Mohanta and Debasis Gountia, "Fully homomorphic encryption equating to cloud security: An approach," IOSR Journal of Computer Engineering (IOSR-JCE), vol. 9, no. 2, pp. 46-50, 2013.

[17] C.P. Gupta and I. Sharma, "Fully Homomorphic Encryption Scheme with Symmetric Keys," in Network of the Future (NOF), 2013 Fourth International Conference on the, Pohang, 2013.

[18] Omer K.Jasim , Safia Abbas, El-Sayed El-Horbaty and Abdel-Badeeh M. Salem, "A Comparative Study between Modern Encryption Algorithms Based on Cloud Computing Environment," The 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013), pp. 531 - 535, 2013.

[19] Krunal Suthar, Parmalik Kumar, Hitesh Gupta and Hiren Patel, "Analytical Comparison of Symmetric Encryption and Encoding Techniques for Cloud Environment," International Journal of Computer Applications, vol. 60, no. 19, pp. 16-19, 2012.

[20] Abha Sachdev and Mohit Bhansali, "Enhancing Cloud Computing Security using AES Algorithm," International Journal of Computer Applications, vol. 67, no. 9, pp. 19-23, 2013.

[21] Sherif El-etriby, Eman M. Mohamed and Hatem S. Abdul-kader, "Randomness testing of modern encryption techniques in cloud environment," Informatics and Systems (INFOS), 2012 8th International Conference on, pp. CC1-CC6, 2012.

[22] Sunita Sharma, Amit Chugh and Ajay Kumar, "ENHANCING DATA SECURITY IN CLOUD STORAGE," International Journal of Advanced Research in Computer and Communication Engineering, vol. 2, no. 5, pp. 2132-2134, 2013.

[23] Nandita Sengupta and Jeffrey Holmes, "Designing of Cryptography Based Security System for Cloud Computing," 2013 International Conference on Cloud & Ubiquitous Computing & Emerging Technologies, pp. 52-57, 2013.

[24] Sashank Dara, "Cryptography Challenges for Computational Privacyin Public Clouds," Cloud Computing in Emerging Markets (CCEM), 2013 IEEE International Conference on, pp. 1-5, 2013.