IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-3, Issue-5 E-ISSN: 2347-2693

Comprehensive Review on Encryption Algorithms for Multimedia Cloud Computing

Er. Ramandeep Kaur[1], Er.Gurjot Kaur[2], Er.Reena Sharma[3], Er.Varinder kaur[4]

[1*,2,3,4]Computer Science and Engineering, Chandigarh University, India

www.ijcseonline.org

Received: May/02/2015 Revised: May/10//2015 Accepted: May/24/2015 Published: May/30/ 2015

***Abstract*—** With the advancement on the web, internet interactive media is rising as an administration. To provide rich media services, process, multimedia computing has emerged as a noteworthy technology to produce, edit and examine media contents, such as images, graphics, video, audio and so on. For media application and administrations over the internet and portable remote system, there are solid request for distributed computed computing on account of noteworthy measure of calculation needed for serving a huge number of internet or versatile client in the meantime. This paper audits the brief study on sight and sound distributed computing perspectives and described some security issues in cloud computing, including data integrity, data confidentiality, access control, data manipulation in the encrypted data domain etc. along with security algorithms.

Keywords— Cloud Computing, Multimedia, Cryptography, Internet.

I.INTRODUCTION

The cloud computing is shared the resources like hardware, software and networking. The cloud computing is TCP/IP based high development and integrations of the computer technologies such as fast speed network and fast micro processor.[9] They are refers to internet based services and development.

The cloud computing are used the three types of deployment model:

- Public: The public cloud allows easily services accessible to the general public. They are sell everything over the internet.
- Private: Private cloud allow services to be accessible with an origination. The private cloud is increase the security.
- Hybrid: The hybrid is the mixture of public cloud and private cloud. It is cloud computing environment where origination gives and manages few resources internally and other externally.
- Community: The community cloud is allows services to be access by group of communication. It may be for one origination or for the several origination, but they share the common concern such as their mission[2].

II. CLOUD COMPUTING ARCHITECTURE

The cloud computing is used the three types of the services model:

SAAS: The SAAS is the software as a services. The software as a services is computer based application over internet like email, google docs and games. They are pay-per-use pattern. They reduced the cost.

PAAS: The PAAS is platform as a services. It is run time environment for application and development like database web server and deployment tools. The PAAS is middle bridge between hardware and application.

IAAS: The IAAS is infrastructure as a service. They provide access to fundamental resources such as physical machine, virtual machine and virtual storage[2].

III.SECURITY CHALLENGES IN CLOUD COMPUTING

Security issues are provide the security so data not loss and not theft. The main issues raise while discussing security of the cloud;

- Data Issues
- Security Issues
- Trust Issues
- Privacy Issues
- Infected Application

IV. CRYPTOGRAPHY

The cryptography is technique which data is made secure from the third person and only be used by the authenticated person. Cryptography is used firstly in 1990 B.C.by an Egyptian for war time battle plans. In cryptography is use the plaintext and cipher text. The plaintext is original message, before being transformed and after the message transformed is called the cipher text[1]. The encryption algorithm transfer the plaintext into cipher text. The

description algorithm transfer the cipher text into the plaintext. Two categories of cryptography:

Symmetric: The symmetric is also called the secret key. They are same key used by both parties. In this they are sender uses this key and an encryption algorithm to encrypt data, the receiver uses the same key and the corresponding decryption algorithm to decrypt the data[1]. The main symmetric algorithm are DES, RC5, AES, 3DES and BLOW FISH.

Asymmetric: The asymmetric is also called the public key cryptography. Asymmetric is used the two keys public key and private key. They used private key is kept by the receiver and public key is announced to the public. The main asymmetric algorithm are RSA, DSA, Diffie- Hellman and El-gamal[6].

V. SECURITY ALGORITHMS IN CLOUD COMPUTING

RSA: The calculation was given by the three MIT's Rivest, Shamir and Adleman and distributed in year 1977. The RSA algorithm is a message encryption cryptosystem in which two prime numbers are taken initially and them the product of these values is used to create a public and a private key which is further utilized as a part and a private key, which is further utilized as a part of encryption and unscrambling. [9]The RSA calculation could be utilized as a part of blend with Hash-LSB in a way that original text is embedded in the cover image in the form of cipher text. By using the RSA algorithm we are increasing the security to a level above. In case of steganalysis only cipher text could be extracted which is in the encrypted form and is not readable, therefore will be secure[6].

DES:DES (the Data Encryption Standard) is a symmetric square figure grew by IBM. The calculation utilizes a 56-bit key to encipher/unravel a 64-bit square of information. The key is constantly introduced as a 64-bit hinder, each 8th bit of which is disregarded. Nonetheless, it is normal to situated at every 8th bit so that every gathering of 8 bits has an odd number of bits set to 1[6].

AES: (Advanced Encryption Standard) is a symmetric- key encryption standard. This means that it uses the same key for both encryption and decryption. Each of these ciphers has a 128-bit block size, with key lengths 128,192 and 256 bits[6]. The encryption process consists of 10 rounds of processing for 128-bit keys. 16 byte encryption key, in the form of 4-byte words is expanded into key schedule consisting of 44 4-byte words. The 4* 4 matrix of bytes made from 128- bit input block is referred to as the state array. AES for encryption are used the each round are four steps:

- Sub Bytes
- Shift Rows
- Mix Columns
- Add Round Key

El-gamal Algorithm: The el-gamal algorithm has a public key and it can be divided into three parts: Key generation, Encryption of message and decryption of the message. The el-gamal algorithm is a public-key cryptosystem on the discrete logarithm problem. It consists of both the encryption and signature algorithm. The el-gamal signature algorithm is similar to the encryption algorithm in that the public key and private key are the same[13]. Signature creation depends on the el-gamal signature algorithm. The el-gamal algorithm is public key cryptography which is based on the Diffie- Hellman key change.

VI. RELATED WORK

Akhil Kaushik et al. [1] described the cryptography types like symmetric key and asymmetric key. Symmetric key algorithms are quickest and most commonly used type of encryption. Here, a single key is used for both encryption and decryption. This paper throws some light on the history of cryptography and discusses an innovative approach for encrypting small amount of data, which will be practically useful for the small scale organizations.

Bhavna Makhija et al [2] Proposed Enhanced data security in cloud computing with third party auditor. Cloud computing is environment which enables convenient, efficient, on- demand network access to a shared pool of configurable computing resources that can rapidly provisioned and released with minimal management effort or services providers interaction. cloud is model where user is provided services by cloud services provider on pay per use base. In cloud, there is support for data dynamics means clients can insert, delete or can update data so there should be security mechanism which ensure integrity for same. Here TPA can not only see the data but he can access data or can modify also so there should be some security mechanism against this.

Dr.A.Padmapriya et al [4] Proposed cloud computing: Security challenges and Encryption practices. Cloud computing is a new era of the modern world. Reasons for development of cloud computing are different people and different purpose depends upon the demand. The improvement of the cloud technology also increases the security issues twice. In this paper, we have discussed about computing security mechanisms and presented the comparative study of several algorithms. In future we are going to propose a new plan to solve security issues for both cloud providers and cloud users.

Gurpreet kaur et al [6] Proposed analyzing data security for cloud computing using cryptographic algorithms. Cloud computing is the next generation architecture, which focuses on it enterprise, through which potentiality on delivery of services in an infrastructure is increased. By the means of cloud computing investing in new infrastructure, training new personnel and licensing new software descends. This paper analyze the performance of security algorithm, namely, AES, DES, blowfish, RSA and MD5 on single system and cloud network for different inputs. These algorithms are compared based on two parameters, namely, mean time and speed-up ratio.

Leena Khanna et al [9] proposed cloud computing: security issues and description of encryption based algorithm to overcome them. Cloud computing today is the latest buzzword in the software industry, an evolutionary step which encompasses element from grid computing, utility computing and autonomic computing, into inventive deployment architecture. cloud computing has fuelled concerns on a critical issue for the success of information system, communication and information security. This paper deals with various issues associated with security and focus mainly on the data security and methods of providing security by data encryption. Various encryption methods of block cipher algorithms such as RSA, blowfish are discussed for providing solution to cloud security.

Mr.prashant rewagad et al [12] proposed use of digital signature with diffie hellman key exchange and AES encryption algorithm to enhance data security in cloud computing. The cloud computing is the apt technology for the decade. It allow user to store larger amount of data in cloud storage. Cloud is the rest on internet, security issues like privacy, data security, confidentiality and authentication is encountered. We have chosen to make use of a combination of authentication technique and key exchange algorithm blended with an encryption algorithm. In this paper, we have proposed to make use of digital signature and differ hellman key exchange blended with AES to protect confidentiality of data stored in cloud. This proposed architecture of three way mechanism makes it tough for hackers to crack the security system thereby protecting data stored in cloud.

VII. CONCLUSION AND FUTURE SCOPE

It is essential for the cloud storage to be equipped with storage security solutions so that the whole cloud storage system is reliable and trustworthy. In this paper, we conducted a brief survey on multimedia cloud computing aspects and described some security issues in cloud computing, including data integrity, data confidentiality, access control, data manipulation in the encrypted data domain, etc along with security algorithms.
Future scope lies in the use of security algorithms to provide security.

REFERENCES

[1] Akhil Kaushik, Krishan Gupta and Satvika, "Ask cipher for small amount of data," 978-1-4799-2995-5/14/$31.00@IEEE, February 2014.
[2] Bhavna Makhija, Vinit Kumar Gupta and Indrajit Rajput, "Enhanced data security in cloud computing with third party auditor," ijarcsse,vol.3, no.2, February2013.
[3] Deyan Chen and Hong Zhao "Data Security and Privacy Protection Issues in Cloud Computing," 2012 IEEE International Conference on Computer Science and Electronics Engineering.
[4] Dr.A.Padmapriya, P .Subhasri, "Cloud Computing: Security Challenges & Encryption Practices," Volume 3, Issue 3, March 2013 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering.
[5] Gartner: Seven cloud-computing security risks InfoWorld 2008-07-02.
[6] Gurpreet Kaur and Manish Mahajan, "Analyzing data Security for cloud computing using cryptographic algorithms," ijera, vol.3, no.5, Sep-Oct 2013.
[7]http://www.mytestbox.com/miscellaneous/cloud-computing-grid-computing-utility- computing-list-top-providers/
[8] K.S.Suresh " Security Issues and Security Algorithms in Cloud Computing," International Journal of Advanced Research in Computer Science and Software Engineering.
[9]Leena Khanna " Cloud Computing: Security Issues And Description Of Encryption Based Algorithms To Overcome Them," Volume 3, Issue 3, March 2013 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering.
[10] Maha TEBAA, Saïd EL HAJJI and Abdellatif EL GHAZI, "Homomorphic Encryption Applied to the Cloud Computing Security," Proceedings of the World Congress on Engineering, Vol.1, WCE 2012, July 4 (2012), London, U.K .
[11] Mr. D. Kishore Kumar "Cloud Computing: An Analysis of Its Challenges & Security Issues," International Journal of Computer Science and Network (IJCSN) Volume 1, Issue 5, October 2012 www.ijcsn.org ISSN 2277-5420.
[12] Mr. PrashantRewagad, and Ms.YogitaPawar, "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data

Security in Cloud Computing," 978-0-7695-4958-3/13 $26.00 © 2013 IEEE.

[13] Randeep Kaur and Supriya Kinger, "Analysis of security algorithms in cloud computing," ijaiem, vol.3, no.3, March 2014.

[14] Uma Somani, Kanika Lakhani, and Manish Mundra "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing," 2010 IEEE 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).

[15] Vahid Ashktorab2, Seyed Reza Taghizadeh1 "Security Threats and Countermeasures in Cloud Computing," International Journal of Application or Innovation in Engineering & Management (IJAIEM).

[16] Volker Fusenig and Ayush Sharma "Security Architecture for Cloud Networking," 2012 IEEE International Conference on Computing, Networking and Communications, Cloud Computing and Networking Symposium.