iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VIII **Month of publication:** August 2017

DOI: http://doi.org/10.22214/ijraset.2017.8214

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VIII, August 2017- Available at www.ijraset.com

Role of Cryptography & its Related Techniques in Cloud Computing Security

G. Kishore Kumar[1], Dr. M. Gobi[2]
[1]*Research Scholar,* [2]*Assistant Professor, Department of Computer Science*
Chikkanna Government Arts College, Tirupur- 641 602, TN, India

Abstract*: Cloud Computing is a fast-growing area and its security issues block the prevalence widely. The organizations are lethargic in accepting it due to these issues and challenges associated with it. Security is the most important concern in cloud computing including the data protection, network security, virtualization security, application integrity, and identity management. Data protection is one of the most important among these issues. The major reason is, organizations will transfer their data to remote machines if and only if the cloud service providers provide guaranteed data protection. Even though many techniques are proposed/recommended for security in cloud computing, however, there are still a lot of challenges in this area. One of the most popular techniques is Cryptography, which can be used in addressing the security issues. The various techniques/algorithms in it playing a vital role in addressing the security issues. This paper enlightens the role of Cryptography, and its various techniques that are helpful in addressing the cloud security issues, in which our research would be focusing.

Keywords: Cloud Computing, Cryptography, Algorithms, Techniques, Public Key, Private Key, ECC, HECC.

I. INTRODUCTION

Cloud Computing refers to the exercise of using a network, which comprises remote servers, hosted on the Internet to process, manage and store data, as opposed to a personal computer or a local server. It is a type of Internet-based computing, which offers shared computer handling resources and data to computers and/or other devices required on demand. It is a pattern for enabling a shared pool of configurable computing resources as on when requested and global access such as computer networks, servers, storage, applications and services. Cloud computing and storage solutions offer various provisions to the users/enterprises for storing and processing own data. This can be either done in a privately owned data centre or owned by the third parties whereas these data centres might be located anywhere in the world. [As per US National Institute of Standards and Technology (NIST)].

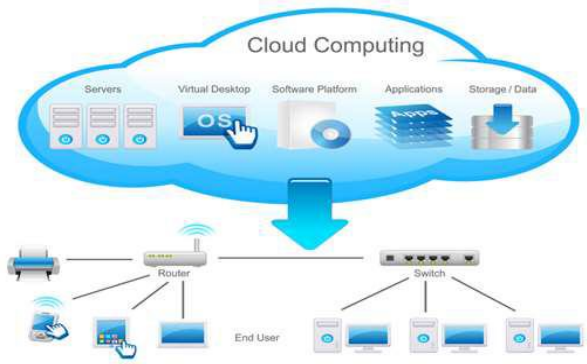


Fig. 1 Cloud Computing Overview

A. Cloud Characteristics

1) On-Demand self-service
2) Ubiquitous network access
3) Location-independent resource pooling
4) Rapid elasticity
5) Measured service

B. Cloud Delivery Models are given below:

1) Application/Software as a Service (SaaS)

2) *Platform as a Service (PaaS)*
3) *Infrastructure as a Service (IaaS)*

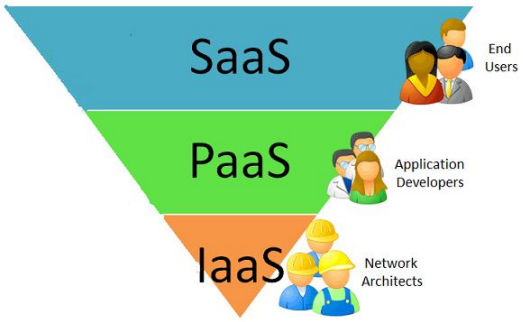


Fig. 2 Cloud Delivery Models

C. *Cloud Deployment Models are as given below:*
1) *Private*
2) *Public*
3) *Community*
4) *Hybrid*

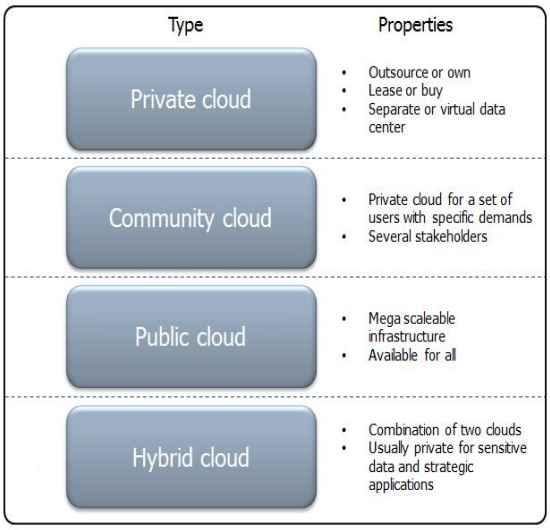


Fig. 3 Cloud Deployment Models

5) *Virtual Private Cloud*[3]*:* A virtual private cloud (VPC) will reside or within a public cloud environment which contains set of configurable group of computing resources on demand and allocated within a public cloud environment. They will provide a certain level of isolation between the different organizations, which are nothing but users.

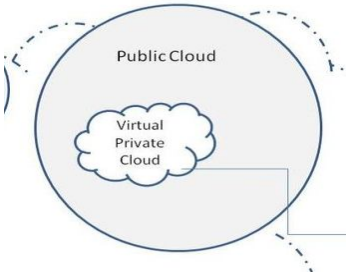


Fig. 4 Virtual Private Cloud

The below diagram illustrates the major benefits of cloud computing:

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VIII, August 2017- Available at www.ijraset.com

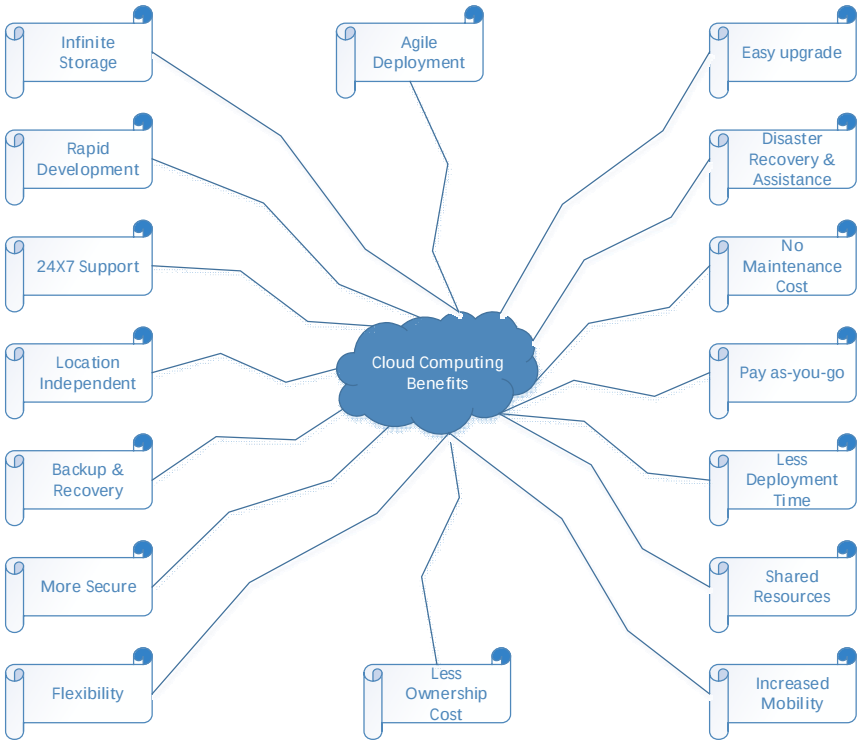


Fig. 5 Cloud Computing Benefits

D. Cloud Computing Security

Security is extremely tough to define in general. The objectives of information security are Integrity, Confidentiality, and Availability. Wide set of policies, controls and technologies are installed in Cloud Computing to protect data, applications and its infrastructure. It is a sub-domain of computer security, network security, and, moreover, information security. [4]

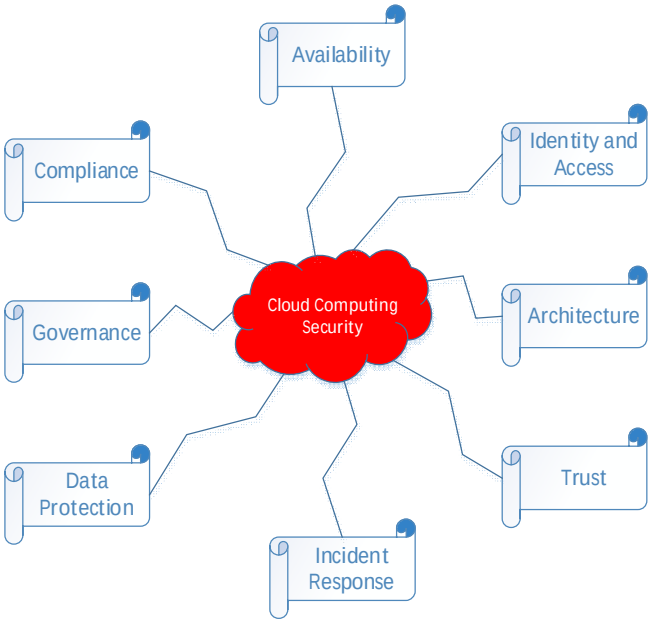


Fig. 6 Cloud Computing Security

The below diagram illustrates about various parameters that affect cloud security:

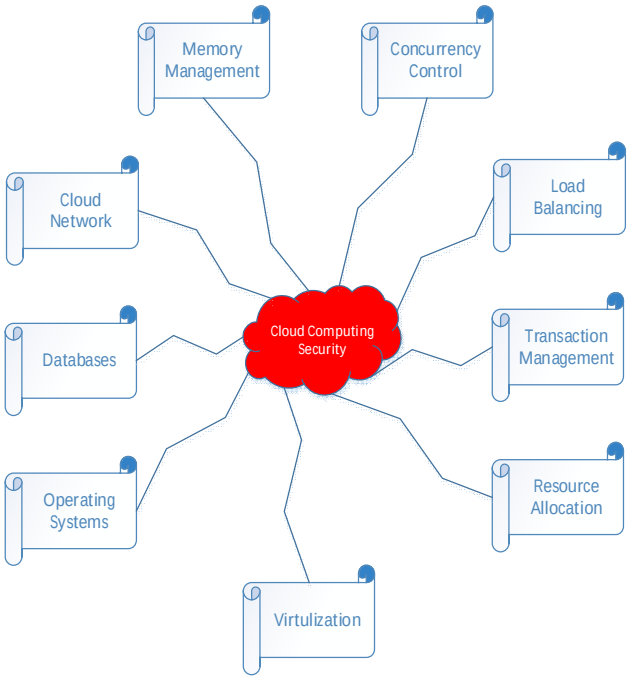


Fig. 7 Parameters that affect Cloud Security

II. BENEFITS OF ENCRYPTION IN CLOUD ENVIRONMENTS

The following are the few benefits of encryption in the cloud environment. The encryption helps to

A. Ensure the privacy of the organization data, where in encrypted data is in the transmission, in use and at storage location as well.

B. Achieve Secure Multi-Tenancy in the Cloud. Encrypting data in the cloud and holding encryption key by which data owner can avoid the cloud service provider to access the data.

C. Provide a Safe Harbor from Breach Notification, if a data breach occurs and personally, identifiable information is lost, the breached party must notify all individuals who are impacted.

D. Provide Confidence of data backups are safe in cloud environment from the breached party.

E. Expand revenue potential to customers with sensitive or regulated data by maintaining the key by cloud data owner and gives cloud service providers a competitive edge.

III. CRYPTOGRAPHY & ITS TECHNIQUES/ALGORITHMS

A. Introduction

Cryptography term is originally from the Greek words κρυπτο, means hidden/Secret and γραφη means writing. Its history periods are back to about 2000 B.C and it's about the study of secret writing scientifically. Cryptography is one of the ancient/olden methods engaged by ancient civilizations for secret method of communications. Particularly the Egyptians are known to have used cryptography on the tombs of deceased kings and rulers. Julius Caesar invented a process called as CAESAR CIPHER for sending secret/confidential messages to his generals during wars. This was one of the prominent methods in the history of Cryptography, which was very easy and fast. This was implemented by the substitution cipher method with alphabet shifts of 3, which would for example shift an "A" to "D" or a "B" to "E".[5]

In current era, cryptography uses complex scientific approaches and the algorithms that are designed for cryptosystems based on computational resistance/stability, which makes it difficult for opponent/challenger to break into the system. Moreover, a modern cryptosystem is about the design and analysis of various techniques/procedures that are interrelated to various aspects in authentication, data security, and integrity. [5]

The following diagram explains the working principle of cryptography/crypto-system in general:

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VIII, August 2017- Available at www.ijraset.com

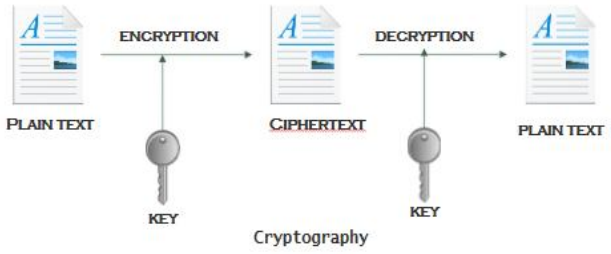


Fig. 8 Cryptography working principle

To ensure that a particular system is secure, the cryptanalysts will try to break the ways/techniques used to build that particular system.

B. Types of Cryptography

The Crypto-System is defined as any system, which comprises cryptography. The security of such system majorly depends upon the below given factors:
Type of algorithms used
Number of keys in the algorithm
Number of rounds etc.

The cryptographic systems are classified as follows:

1) Symmetric Key Cryptography
2) Asymmetric Key Cryptography

The following diagram illustrates about Symmetric key cryptography in which same key will be used for both encryption and decryption and will be shared with receiver for decryption. The sender uses a key for encryption and the receiver uses the same key for decrypting the data, which is agreed by both users.

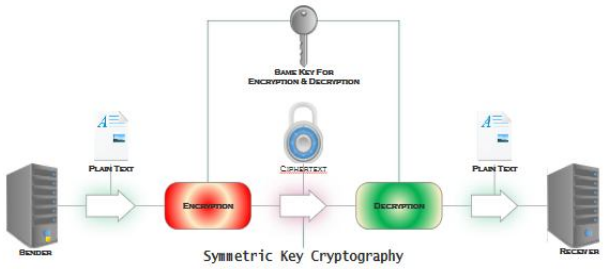


Fig. 9 Symmetric Key Cryptography

The following diagram illustrates about asymmetric key cryptography in which two different keys will be used for encryption and decryption. The sender uses a key to encrypt the plaintext, and another one to decrypt the cipher text. One of these keys is distributed or public and the other one is kept as private key.

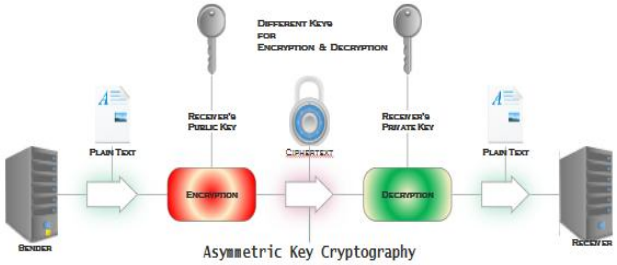


Fig. 10 Asymmetric Key Cryptography

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VIII, August 2017- Available at www.ijraset.com

C. Various Available Algorithms/Techniques

The encryption algorithms play vital role and acting as necessary tool for data protection and secured network communication. The encryption algorithms convert the data into jumbled form by using the "key" and the decryption can be done by the user only using the same key. [4]

The following are the various algorithms available in cryptography:

1) *DES- Data Encryption Standard:* DES is an out-of-date symmetric-key method of data encryption. DES uses the same key to encrypt and decrypt a message; hence, the sender and the receiver both must have and use the same private key. DES has been superseded by more secure Advanced Encryption Standard (AES) algorithm, which was originally designed by researchers at IBM in the early 1970s. The U.S. government as an official Federal Information Processing Standard (FIPS) in 1977 adopted later on DES.
2) *AES- Advanced Encryption Standard (AES) :* It is a symmetric-key encryption standard. It uses 10, 12, or 14 rounds. Each of the ciphers has a 128-bit block size, with the key sizes of 128, 192 and 256 bits, respectively. It ensures that the hash code is encrypted in a highly secure manner. Its algorithm steps are as follows:

a) *Key Expansion*
b) *Initial round*
c) *Add Round Key*
d) *Rounds*
e) *Sub Bytes*
f) *Shift Rows*
g) *Mix Columns*
h) *Add Round Key*
i) *Final Round*
j) *Sub Bytes*
k) *Shift Rows*
l) *Add Round Key*

3) *RC2:* This algorithm is a conventional (secret-key) block encryption algorithm, which can be considered as a proposal for a DES replacement. The input and output block sizes are 64 bits each wherein the key size is variable ranging from one byte up to 128 bytes, even though the current implementation uses eight bytes. The algorithm is designed for easy implementation on 16-bit microprocessors. On an IBM AT, the encryption runs about twice as fast as DES.
4) *3DES – Triple DES or Triple DEA:* In this Triple Data Encryption Algorithm, the DES Cipher being used with a symmetric-key block cipher, which is being applied to each block three times. The actual cipher's key size was 56-bits when DES algorithm was designed originally. In general, this was adequate as well, but the computational power availability made the brute-force attacks feasible by being increased. This issue was overcome by Triple DES, which provided a moderate-n-easy method in which the key size is being increased to safeguard such attacks. In addition, this overrides the necessity of designing a complete new block cipher algorithm.
5) *SDES - simplified DES :* Professor Edward Schaefer of Santa Clara University developed this simplified DES. The encryption algorithm uses input as an 8-bit block of plaintext and a 10-bit key. The output would be an 8-bit block of ciphertext. The decryption algorithm uses an input of 8-bit block of ciphertext produced in encryption process and the same 10-bit key used in ciphertext production, wherein the output would be the original 8-bit block of plaintext.
6) *RC5 – Rivest Cipher or Ron's Code*

RC5 is a symmetric-key block cipher distinguished by its simplicity. Ronald Rivest designed this during 1994. In RC5 both the encryption and decryption expand the random key into 2 (r+1) words that will be used in sequence. These will be used only once each during the encryption and decryption processes. RC5 will be using a variable block size of 32/64/128 bits, key size of 0-2040 bits and number of rounds would be 0-255, wherein the parameters proposed in original was 64 bits of block size. A key feature of RC5 is the use of data-dependent rotations; one of the objectives of RC5 was to swift the study and evaluation of such operations as a cryptographic primitive/with citation. RC5 also comprises of a number of modular additions and eXclusive OR (XOR) s.

7) *RC6 - Rivest cipher 6:* Ron Rivest, Matt Robshaw, Ray Sidney, and Yigum Lisa Yin designed RC6, which is a symmetric key block cipher. This was designed to meet the necessity of AES competition & derived from RC5. It has 128-bits of block size and supports 128,192 and 256 bits of key sizes upto 2040-bits. But it may be parameterized like RC5 to support a wide variety

of word-lengths, key sizes, and number of rounds. RC6 and RC5 are similar in structure. Both would be using data-dependent rotations, modular addition, and XOR operations. In reality, RC6 could be viewed as interlacing two parallel RC5 encryption processes, although RC6 does use an extra multiplication operation, which is not present in RC5. This is to make the rotation dependent on every bit in a word, and not just the least significant few bits.

8) *SSL Encryption – Secure Socket Layer:* SSL is the standard security technology for launching an encrypted/encoded link between a web server and a browser to make sure that all data distributed between the web server and browsers persist private and integral. In SSL communications, the server's SSL Certificate comprises a pair of asymmetric public and private keys. The session key created during the server and the browser SSL Handshake is symmetric. The below given diagram illustrates this process:

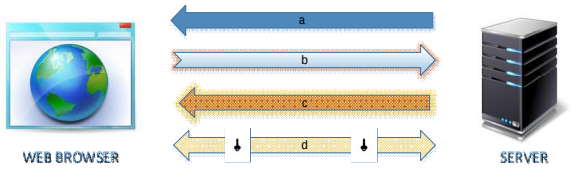


Fig. 11 Browser-Server Communication using SSL

a) Server sends a copy of its asymmetric public key.
b) Browser creates a symmetric session key and encrypts it with the server's asymmetric public key. Then sends it to the server.
c) Server decrypts the encrypted session key using its asymmetric private key to get the symmetric session key.
d) Server and Browser now encrypt and decrypt all transmitted data with the symmetric session key.

This process makes a secure channel as only the browser and server know the symmetric session key. In addition, the session key is only used for that particular session. If the browser connects to the same server after that, a brand new session would be created.

9) *GEO Encryption:* Geo-encryption is another type of encryption. The objective of this is to limit the data decryption to a specific location/time/position of the receiver. In this, the traditional encryption is enhanced, which uses any physical location or time to have additional security and its features. In addition, this does not replace any of the conventional algorithms, wherein an extra layer of security is added. The decryption/access of information is restricted to specified locations and/or times. The standard encryption algorithms like AES, 3DES, RSA etc. are used in building this Geo-encryption algorithm provided that the encryption key "geo-locked" is added on top of them using location/time/position of the anticipated recipient. The location-based encryption ensures that the decryption cannot be done outside a particular facility/location; otherwise, this will result in decryption failure.

10) *HABE (Hierarchical Attribute Based Encryption):* A user can delegate the private key corresponding to any subset of an attribute set while he has the private key corresponding to the attribute set. Moreover, the size of the ciphertext is constant, but the size of private key is linear with the order of the attribute set in the hierarchical attribute-based encryption scheme.

11) *Key-policy Attribute-Based Encryption (KP-ABE):* The first KP-ABE construction was delivered by Goyal et al., The system was verified selectively secure under the Bilinear Diffie-Hellman assumption. KP-ABE schemes are suitable for structured organizations, wherein they are with rules, which deals with particular documents reading. Secure forensic analysis and target broadcast are typical applications of KP-ABE, wherein the ciphertexts sent by sender labelled with a set of descriptive attributes. The user's private key is specified by a trusted attribute authority policy by which the decryption of ciphertexts are defined.

12) *CP-ABE (Ciphertext Policy Attribute Based Encryption):* This CP-ABE algorithm comprises of Setup, Encrypt, KeyGen, and Decrypt processes. The inputs for this process would be a security parameter and attribute universe description wherein the PK-public parameters and MK-master key will be the output. In CP-ABE scheme, the user's private key/decryption key will be linked/tied to a set of attributes that will signify the concerned user's permissions. When a ciphertext is encrypted, a set of attributes is designated for the encryption, and only users tied to the relevant attributes are able to decrypt the ciphertext.

13) *Blowfish:* Blowfish is a symmetric-key block cipher, designed in 1993 by Bruce Schneier. This is being used in a huge number of cipher suites and encryption products. Blowfish provides a good encryption rate in software. At the same time till date no effective cryptanalysis of it has been identified. Nevertheless, the Advanced Encryption Standard (AES) now gets more attention. The DES or IDEA can use blowfish as drop-in replacement wherein it takes 32-448 bits of a variable-length key for both domestic and exportable uses. This process uses large key-dependent S-boxes and a 16-round Feistel cipher, which resembles CAST-128 in structure where fixed S-boxes are used.

14) *MA-ABE Multi-Authority Attribute-Based Encryption:* A multi-authority ABE system comprises of any number attribute authorities and users as well. In the systems a set of global public parameters are defined. An user can select an attribute authority and attain the equivalent decryption keys. The authority executes the corresponding attribute key generation algorithm and the result is reverted to the user. Global public parameters used in the encryption process and the ciphertext is produced based an attribute set. In the same way, the decryption is also set using attribute set. [19]
15) *RSA:* RSA algorithm is used for public-key cryptography and it is an asymmetric algorithm being the first and still most commonly used. It involves two types of keys – public and private keys. The public key is known to all and used for encrypting messages. The encrypted message with a public key can be decrypted only by using private key.
16) *MD5- (Message-Digest Algorithm 5):* Cryptographic hash function algorithm which is a widely used one with a 128-bit hash value and processes a variable length message into a fixed-length output of 128 bits. In this, the input message is broken up into chunks of 512-bit blocks then the message is padded so that its total length is divisible by 512. Also, the sender of the data use the public key to encrypt the message and the receiver uses its private key to decrypt the message.
17) *Digital Signature:* Public key algorithms used in Cryptographic digital signatures for delivering data integrity. In this authentication scheme, public key authentication is implemented in the server by signing a unique message using a private key, thus creating is called as a digital signature. Then the signature is returned to the client and later it is verified using the server's known public key.

IV. PROPOSED APPROACH / RELATED WORK

Following are the few security measures suggested/identified by few researchers, which can be taken into consideration for warranting the security in a cloud environment: [4]

A. *File Encryption*

The hackers can very easily steal all the critical information from the machines in a cluster, as the entire data is present & stored in them. Hence, an encryption technique is a must while storing the data, at the same time various different encryption keys/techniques can be used on different machines and the key information can be stored behind a firewall stored centrally. By using these methods, the encryption helps to securely store & manipulate the data.

B. *Mobile – Cloud Server Communication*

The encryption is mandatory in another type of communication happen in the cloud between mobile and server located in a cloud environment. As the usage of mobile is also drastically increased nowadays, the encryption is necessary for this area as well.

C. *Data Privacy in the Cloud*

The privacy in the cloud would have been managed by converting the data into encrypted form and providing the key to the user only in case of just data storage, but cloud serves the user in not only data storage but also various activities like searching, access control decisions, transformations etc. Hence, the prevailing challenge is to incorporate a strong type of encryption for serving both the above-said activities in the cloud storage.

D. *Network Encryption*

As per the industry principles, encryption must be applied in all the network communication happen. Whatever be the RPC procedure call, which takes place, should happen over an SSL. Hence, even though the hacker taps into the network communication packets, useful information cannot be extracted or manipulated.

V. FUTURE RESEARCH DIRECTIONS

Security plays a vital and critical role in cloud computing widely, especially in major areas like Storage, Middleware, Data, Network and Application. The major reason for this would be the number of users being increased day-by-day. Encryption Algorithms play an essential/critical role in overcoming the security issues in data storage, communication channels, etc. Various cryptographic techniques available would help in addressing the security issues in the above-mentioned areas in Cloud. This paper discusses various available cryptographic techniques and by using them either individually or combining or enhancing them to ensure the data security and integrity. Our future research would be focusing on enhancement/combining the existing security frameworks/techniques for highly secured data using any of the cryptographic techniques discussed in this article. Our research goal is to offer a more trustworthy security in cloud computing for the authorized users while accessing the data.

TABLE 1: ABBREVIATIONS AND ACRONYMS

Abbreviation	Meaning
CSA	Cloud Security Alliance
ECC	Elliptic curve cryptography
HECC	Hyperelliptic curve cryptography
SLA	Service Level Agreement
MCC	Mobile Cloud Computing
IBE	Identity Based Encryption
PKI	Public Key Infrastructure
RPC	Remote Procedure Call

REFERENCES

[1] US National Institute of Standards and Technology (NIST, http://csrc.nist.gov).

[2] Cloud Security Alliance (CSA)

[3] Mashrufee Alam, Israt Jahan, Liton Jude Rozario, Israt Jerin ,"A Comparative Study of RSA and ECC and Implementation of ECC on Embedded Systems",International Journal of Innovative Research in Advanced Engineering(IJIRAE) ISSN: 2349-2763 Issue 03, Volume 3 (March 2016)

[4] Dr. M.Gobi,Kishore Kumar G,"Current Trend in Cloud Computing Security & Future Research Challenges", INTERNATIONAL JOURNAL FOR RESEARCH & DEVELOPMENT IN TECHNOLOGY (IJRDT), Volume-7,Issue-6, (June-17)

[5] Jyotirmoy Das,"A Study on Modern Cryptography and their Security Issues",International Journal of Emerging Technology and Advanced Engineering, Volume 4, Issue 10, October 2014

[6] Maninder Singh Bajwa, Himani, "A Concern towards Data Security in Cloud Computing", International Journal of Computer Applications (0975 – 8887) Volume 114 – No. 11, March 2015

[7] Changyou Guo and Xuefeng Zheng, "The Research of Data Security Mechanism Based on Cloud Computing", International Journal of Security and Its Applications Vol. 9, No. 3 (2015), pp. 363-370

[8] Hasan Omar Al-Sakran,"ACCESSING SECURED DATA IN CLOUD COMPUTING ENVIRONMENT", International Journal of Network Security & Its Applications (IJNSA) Vol.7, No.1, January 2015

[9] Abdullah, Imran & Fida Hussain,"The Secure Data Storage in Mobile Cloud Computing",Computer Engineering and Intelligent Systems ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online) Vol.6, No.5, 2015

[10] S.Selvi & Dr.R.Ganesan,"An efficient Access Control Protocol for cloud data security using Hyper Elliptic Curve Cryptography",IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501 Vol.6, No 4, July-August 2016

[11] Ali Gholami and Erwin Laure, "SECURITY AND PRIVACY OF SENSITIVE DATA IN CLOUD COMPUTING: A SURVEY OF RECENT DEVELOPMENTS",NETCOM, NCS, WiMoNe, CSEIT, SPM - 2015 pp. 131–150, 2015. © CS & IT-CSCP 2015 DOI : 10.5121/csit.2015.51611

[12] Neha Tirthani & Dr.Ganesan R,"Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography"

[13] Bhushan Patil & Punam Patil,"An Efficient Algorithm for Securing Data in Cloud Computing",Volume 1, Issue 1, April 2016 ISSN: 2456-0006 International Journal of Science Technology Management and Research

[14] Sultan Aldossary & William Allen,"Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions",(IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 7, No. 4, 2016

[15] Ramalingam Sugumar & Sharmila Banu Sheik Imam,"Symmetric Encryption Algorithm to Secure Outsourced Data in Public Cloud Storage",Indian Journal of Science and Technology, Vol 8(23), DOI:10.17485/ijst/2015/v8i23/79210, September 2015

[16] S.SUDHA, V.MADHU VISWANATHAM," ADDRESSING SECURITY AND PRIVACY ISSUES IN CLOUD COMPUTING", Journal of Theoretical and Applied Information Technology, Vol. 48 No.2

[17] Mayank Patwal and Tanushri Mittal, "A Survey of Cryptographic based Security Algorithms for Cloud Computing"

[18] Hugo a.w. Ideler,"Cryptography as a service in a cloud computing environment",EINDHOVEN UNIVERSITY OF TECHNOLOGY, Department of Mathematics and Computing Science

[19] Dr. M.Newlin Rajkumar, Ancy George, Brighty Batley C,"An Overview of Multi-Authority Attribute Based Encryption Techniques",International Journal of Advanced Research in Computer and Communication Engineering,Vol. 3, Issue 9,September 2014

[20] Er. Ashima Pansotra and Er. Simar Preet Singh,"Cloud Security Algorithms", International Journal of Security and Its Applications Vol.9, No.10 (2015), pp.353-360

[21] John Bethencourt,Amit Sahai,Brent Waters,"Ciphertext-Policy Attribute-Based Encryption"

[22] Guojun Wang, Qin Liu,Jie Wu,"Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services",CCS'10, October 4–8, 2010, Chicago, Illinois, USA

[23] Nallamalli Ramesh, Gorantla Praveen, V.P. Krishna Anne, Dr. Rajasekhara Rao Kurra,"Implementation of MA-ABE for Better Data Security in Cloud",IJCST Vol. 3, Issue 1, Jan. - March 2012

[24] V.S. Sajitha, V. Reena Catherine,"Hierarchical Attribute-Based Encryption: A Survey",2017 IJEDR | Volume 5, Issue 2

[25] Kalyani P. Karule, Neha V. Nagrale,"Comparative Analysis of Encryption Algorithms for Various Types of Data Files for Data Security",International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-2, Issue-2, February 2016

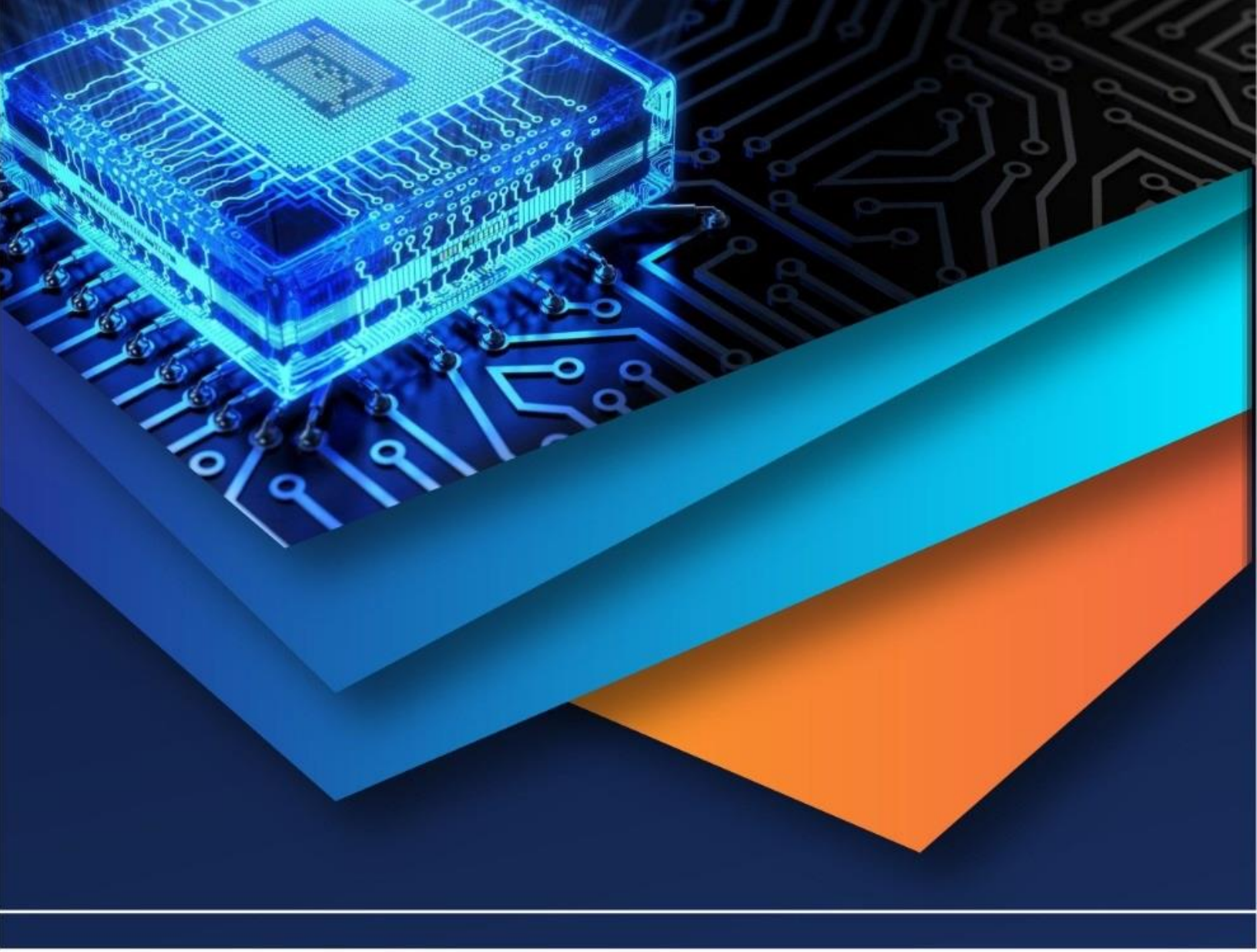
[26] Nigel Smart,"Cryptography: An Introduction (3rd Edition)"

[27] INTRODUCTION TO CRYPTOGRAPHY

[28] Pooja Bindlish,"Optimization of Cryptography Algorithms in Cloud Computing",International Journal of Computer Trends and Technology (IJCTT) – Volume 46 Number 2 April 2017

[29] Sharmila Rajasudhan,Nallusamy R,"A Study on Cryptographic Methods in Cloud Storage", International Journal of Communication and Computer Technologies Volume 02 – No.01 Issue: 02 March 2014

[30] Vinod Kumar,Lalita Devi,"RSA Public Key Cryptography for Data Protection in Cloud Computing Environments",INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT,April, 2014 Vol 3 Issue 4.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY