International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 12, 2017 ISSN: 2348-6600
Reference ID: IJCS-213 PAGE NO: 1329-1334
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

AN ANALYTICAL STUDY ON SECURITY ALGORITHMS USED IN CLOUD COMPUTING

R.Abinaya[1], Dr.T.Ramaprabha [2],
[1]M.Phil Full time Research Scholar, PG and Research Department of Computer Science
[2]Professor,PG and Research Department of Computer Science.
Vivekanandha College of Arts and Sciences for Women (Autonomous)
Tiruchengode,Tamilnadu,Namakkal-637 205,
ramaradha1971@gmail.com[1]
abinayaramani8@gmail.com[2]

ABSTRACT- Cloud Computing is a new technology in providing web oriented services. No secret that cloud computing is becoming more and more popular and is ever increasing due to fast growth in the field of "cloud computing " increases serious security concerns in the large companies as they share valuable resources in a cost effective way. Due to increasing demand for more clouds there is a security threat, these security threats can be a danger to cloud computing and they have to be avoided. Since Cloud computing stores the data and disseminated resources in the open environment, security has become the major issue which is hampering the deployment of Cloud environments. Even though Cloud Computing is promising and efficient; there are many challenges in data security for the Cloud user.

Keywords — Cloud Computing, Data Security, RSA algorithm, 3DES, Encryption, and Decryption.

I. INTRODUCTION

Cloud computing refers to Internet based development and services. Cloud is simply the trendy term for a network or remote servers that can be addressed via an internet connection store and manage information. The three main aspects of cloud computing are Software as a service (SaaS) is a model of software deployment where an application is hosted as a service provided to customers across the Internet. cloud computing vendors are Amazon Simple Storage Service (S3) and Amazon Elastic Compute cloud (EC2) are well known examples of cloud computing.

II.CLOUD COMPUTING DEPLOYMENT MODELS

Cloud computing is a new model for providing business and IT services. The service delivery model is based on future development consideration while meeting current development requirements. The three levels of cloud computing service (IaaS, PaaS and SaaS) cover a huge range of services. Besides computing and the service delivery model of storage infrastructure, various models such as data, software application, programming model etc.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 12, 2017 ISSN: 2348-6600
Reference ID: IJCS-213 PAGE NO: 1329-1334
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

Types of Cloud

- Public cloud
- Private cloud
- Community cloud
- Hybrid cloud

PUBLIC CLOUD

The Public Cloud allows systems and services to be easily accessible to the general public. Public cloud may be less secure because of its openness.
e.g., E-mail, Google, Amazon, Microsoft offers cloud services via Internet.

PRIVATE CLOUD

The Private Cloud allows systems and services to be accessible within an organization. It offers increased security because of its private nature.

COMMUNITY CLOUD

The Community Cloud allows systems and services to be accessible by group of organizations.

Fig. 2: Types of Cloud computing

It can also be applicable to cloud computing. More importantly, the cloud computing model involves all aspects of enterprise transformation in its evolution, so technology architecture is only a part of it, and multi-aspect development such as organization, processes and different business models
should also be under consideration. Based on standard architecture methodology with best practices of cloud computing, a Cloud Model Application Methodology can be used to guide industry customer analysis and solve potential problems and risks emerged during the evolution from current computing model to cloud computing model. This methodology can also be used to instruct the investment and decision making analysis of cloud computing model, determine the process, standard, interface and public service of IT assets deployment and management to promote business development.

Advantages of Cloud computing.

Broad network access
Resource pooling
Rapid elasticity.
Measured service

IV.CLOUD COMPUTING SERVICE CATEGORIES

Software-as-a-Service(SaaS), Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS). Cloud is a metaphor to describe web as a space where computing has been pre installed and exist as a service; data, operating systems, applications, storage and processing power exist on the web ready to be shared. To users, cloud computing is a Pay-per-Use-On-Demand mode that can conveniently access shared IT resources through the Internet.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 12, 2017 ISSN: 2348-6600
Reference ID: IJCS-213 PAGE NO: 1329-1334
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

Fig .3: Cloud computing services.

Where the IT resources include network, server, storage, application, service and so on and they can be deployed with much quick and easy manner and least management and also interactions with service providers. Cloud computing can much improve the availability of IT resources and owns many advantages over other computing techniques. Users can use the IT infrastructure with Pay-per-Use-On-Demand mode; this would benefit and save the cost to buy the physical resources that may be vacant.

V.CLOUD COMPUTING SECURITY

Security in cloud computing is a major concern. Data in cloud should be stored in encrypted form. To restrict client from direct accessing the shared data, proxy and brokerage services should be employed.

Fig.4 : Security in Cloud Computing.

Security remains a primary concern for businesses contemplating cloud adoption -- especially public cloud adoption. Public cloud providers share their underlying hardware infrastructure between numerous customers, as public cloud is a multi-tenant environment. This environment demands copious isolation between logical compute resources. At the same time, access to public cloud storage and compute resources is guarded by account logon credentials.

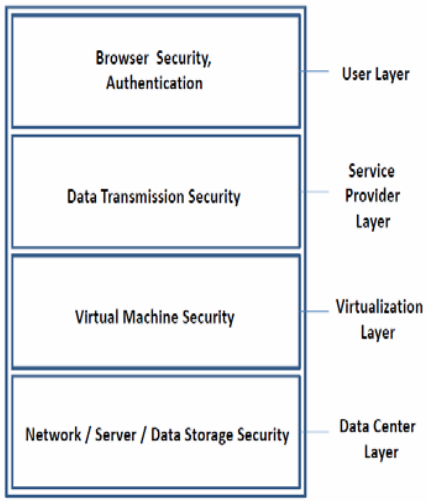

Fig.5: High Level Security Architecture of Cloud Computing.

Some organizations have been focusing on security issues in the cloud computing. The Cloud Security Alliance is a non-profit organization formed to promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing. The Open Security Architecture (OSA) is another organizations focusing on security issues.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 12, 2017 ISSN: 2348-6600
Reference ID: IJCS-213 PAGE NO: 1329-1334
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

RSA Algorithm

RSA is a Public-Key cryptography algorithm. RSA stands for Ron Rivest, Adi Shamir and Len Adleman, who first publicly described it in 1977 at MIT. RSA algorithm uses the product of two prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret, using RSA algorithm encrypt the data to provide security so that only the concerned user can access it. By securing the data, we are not allowing unauthorized access to it.

RSA Algorithm is a asymmetric public key algorithm it uses two different keys one is public key and another is private key this algorithm involves multiplying two large prime numbers that constitutes the public key and private key, once the keys have been developed ,the original prime numbers are no longer important and can be discarded. The private key in RSA algorithm never needs to be sent across the internet. Private Key is used to decrypt text that has been encrypted with the public key. RSA is a block cipher, in which every message is mapped to an integer. User data is encrypted first and then it is stored.

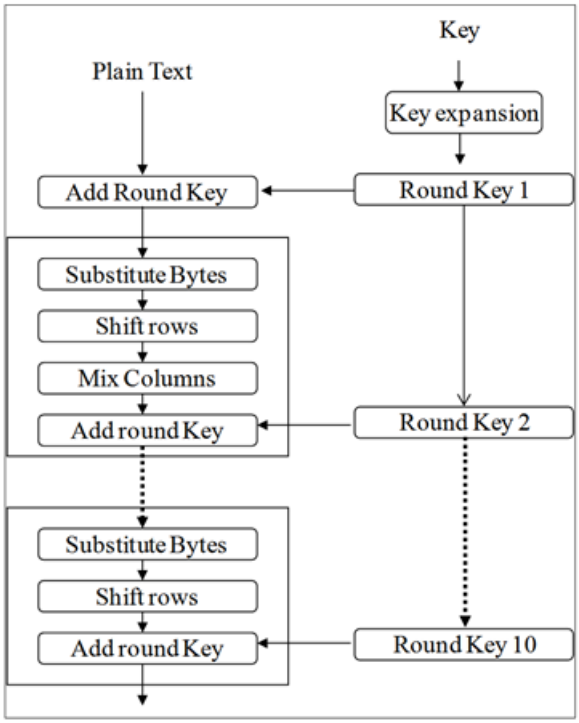

Fig.6: RSA algorithm

RSA algorithm involves three steps:

RSA Algorithm uses two keys public and private and which are asymmetric because one is used for encryption and another is used for decryption.

The public-key encryption system has mainly three phases:

- ✓ Key Generation
- ✓ Encryption
- ✓ Decryption

Protecting privacy in cloud providers is a technical challenge. In cloud environment, this challenge is complicated by distributed nature of clouds and lack of subscriber knowledge over

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 12, 2017 ISSN: 2348-6600
Reference ID: IJCS-213 PAGE NO: 1329-1334
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

where the data is stored i.e. about data center and accessibility of the users. Suppose a user wants to login to a secured cloud system.

Triple DES (3DES)

3DES or the Triple Data Encryption Algorithm (TDEA) was developed to address the obvious flaws in DES without designing a whole new cryptosystem. Data Encryption Standard (DES) uses a 56-bit key and is not deemed sufficient to encrypt sensitive data. 3-DES simply extends the key size of DES by applying the algorithm three times in succession with three different keys. The combined key size is thus 168 bits (3 times 56). TDEA involves using three 64-bit DEA keys (K1, K2, K3) in Encrypt-Decrypt- Encrypt (EDE) mode, that is, the plain text is encrypted with K1, then decrypted with K2, and then encrypted again with K3 [17]. The standards define three keying options:

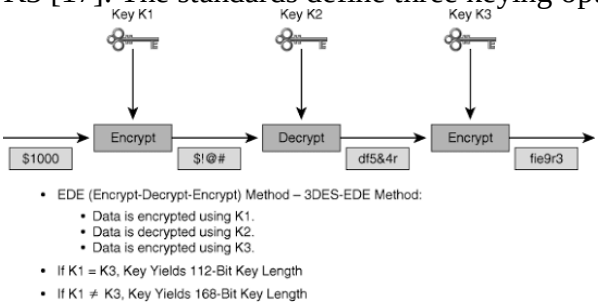

Fig.7: 3DES algorithm

Option 1: The preferred option, employs three mutually independent keys (K1 ≠ K2 ≠ K3 ≠ K1). It gives key space of 3 × 56 = 168 bits.

Option 2 : Employs two mutually independent keys and a third key that is the same as the first key (K1 ≠ K2 and K3 = K1).This gives key space of 2 × 56= 112 bits.

Option 3: Is a key bundle of three identical keys (K1 = K2 = K3). This option is equivalent to DES Algorithm.

In 3-DES the 3-times iteration is applied to increase the encryption level and average time. It is a known fact that 3DES is slower than other block cipher methods.

VI.CONCLUSION

Cloud Computing is still a new technology where the cloud services are readily accessible as on a pay-per-use basis. Once the organization takes the decision to move to the cloud, it loses control over the data. Thus, the amount of protection needed to secure data is directly proportional to the value of the data. Security of the Cloud relies on trusted computing and cryptography.

Factors	RSA	3DES
Created By	Ron Rivest, Adi Shamir,and Leonard Adleman.In 1978	IBM IN 1978
Key Length	Depends on number of bits in the modulus n where n=p*q	168 bits (k1, k2 and k3) 112 bits (k1 and k2)

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 12, 2017 ISSN: 2348-6600
Reference ID: IJCS-213 PAGE NO: 1329-1334
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

Round(s)	1	48
Block Size	Variable	64 bits
Cipher Type	Asymmetric Block Cipher	Symmetric Block Cipher
Speed	Slowest	Very Slow
Security	Least Secure	Adequate Security

Table .1: Comparision of RSA and 3DES

REFERENCES

[1] Sunita Rani and Ambrish Gangal "Security issues of banking adopting the application of cloud computing" International Journal of Information Technology and Knowledge Management July-December 2012, Volume 5, No. 2, pp. 243-246.

[2] Daniel Benton and Walid Negm, "Banking on cloud", 2010.

[3] Ram govind S, Eloff MM, Smith E ,"The Management of Security in Cloud Computing", School of Computing, University of South Africa, Pretoria, South Africa ©2010 IEEE.

[4] Alok Tripathi, Abhinav Mishra," Cloud Computing Security Considerations", IT Division, DOEACC Society, Gorakhpur Centre Gorakhpur, India, 2010, IEEE.

[5] Cong Wang, Qian Wang, and Kui Ren," Towards Secure and Effective Utilization over Encrypted Cloud Data", 2011 31st International Conference on Distributed Computing Systems Workshops, 2011 IEEE.

[6] "3DES", http://www.cryptosys.net/3des.html