Volume 4, Issue 7, July 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Security Issues and Use of Cryptography in Cloud Computing

Jashanpreet Pal Kaur[1],
M.Tech Research Scholar,
Department of Computer Engineering,
Yadavindra College of Engineering,
Talwandi Sabo, Punjab, India

Rajbhupinder Kaur[2]
Assistant Professor,
Department of Computer Engineering,
Yadavindra College of Engineering,
Talwandi Sabo, Punjab, India

Abstract- Cloud computing means provides computing over the internet. The cloud is not a trust worthy. Hence, the cloud data centers are vulnerable assorted attacks. There is a dependency among the layers. So attack at any layer may affect the other layers. This paper focus on cloud security model for servicing to the consumers, security issues, analysis of vulnerabilities and attacks cloud computing frameworks. The paper also discuss the role of cryptography in cloud computing. The purpose of this paper to get insights a new security approach with the implementation of cryptography to secure a data at cloud data centers. So, the cloud data centers are assessed by the authenticated clients only and the approach takes a less time for execution and better security parameter.

Keywords: Introduction, Cloud Security Model, Cloud Security Issues, Use of Cryptography

I. INTRODUCTION

Network is the way of interconnecting of two or more computers together for the purpose of sharing information and data through wireless or wired technology. Computer network requires two computers, a protocol and the hardware to connect them that may increase the cost of sharing.

The Cloud Computing means provides computing over the internet and this word is basically inspired by the cloud. The word cloud is a metaphor for internet. In this, data is stored at remote location and available on demand. It allows clients to use applications without installation the file at any computer with internet facility. By data outsourcing user can get the information from anywhere more efficiently and has no burden on data storage and avoid the extra expenses on software, hardware, and information resources and data maintenances and used more efficiently [1].

The essential features of cloud computing are [2]:

- Resource pooling
- On-demand service
- Broad network access
- Measured services
- Rapid elasticity
- Reduced cost of purchasing hardware and software

A. CLOUD COMPUTING BUILDING BLOCKS

In the cloud computing building block few things come under, which are mentioned below [3]:

a) *Cloud Computing Deployment Models*

Public Clouds: These are hosted, operated, and managed by third party vendor from one or more data centers. The service is offered to multiple customers over common infrastructure. There is a problem of maintaining security and privacy of data at cloud data centers.

Private Clouds: The private clouds are managed or owned by an organization to provide the high level control over cloud services and infrastructure. It provides the services within an organization for maintaining the security and privacy. These are dedicated, community and managed.

Hybrid Cloud: This model comprised both the private and public cloud models where organization might run non - core application in a public cloud, while maintaining core applications and sensitive data in- house in a private cloud.

b) Cloud Service Delivery Model

The cloud Service providers provide services to its users through a layering architecture. The model consists of three layers:

Infrastructure as a Service (IaaS): It provides the complete computer infrastructure such as hardware and network. The customers install and develop their own operating systems, software and applications.

Platform as a Service (PaaS): It provides computing platform such as operating system, hardware and network. The customer installs or develops its own software and applications.

Software as a Service (SaaS): It provides a pre-made application, along with any required software, operating system, hardware, and network.

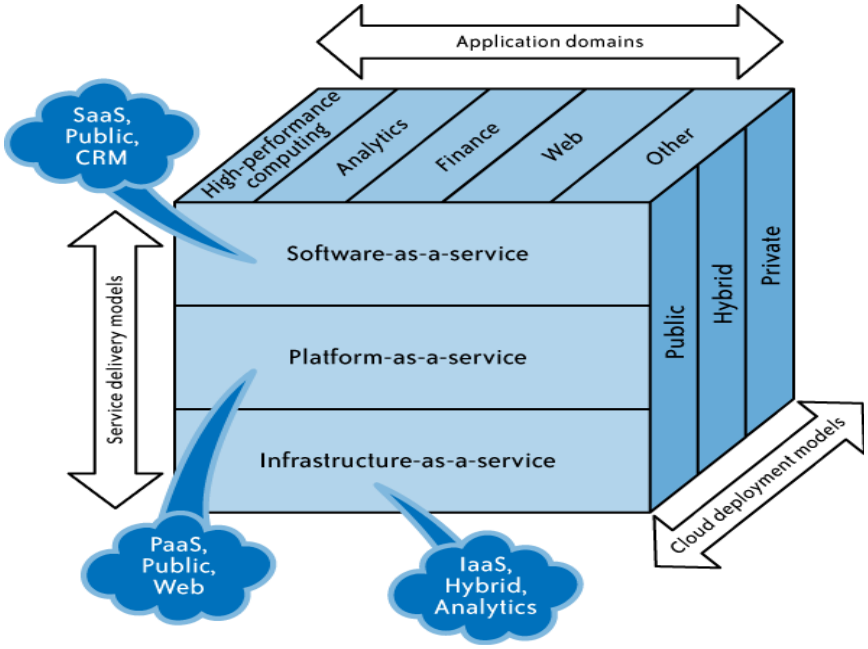

Fig1: SPI Model

c) Cloud Computing Entities

Cloud providers and consumers are the two main entities in the business market. But, service brokers and resellers are the two more emerging service level entities in the Cloud world [6]. These are discussed as follows: -

Cloud Providers: It enables the consumers to access cloud services. Service providers offer different services (e.g., SaaS, PaaS, IaaS, and etc.) to the consumers, the service brokers or resellers.

Cloud Service Brokers: The Service brokers concentrate on the negotiation of the relationships between consumers and providers. There are two major roles for brokers: SLA Negotiation and VM Monitor. The SLA Manager takes care that no Service Level Agreement (SLA) is violated and VM Monitor the current stated of virtual machines periodically at specific amount of time.

Cloud Resellers: Resellers can become an important factor of the Cloud market when the Cloud providers will expand their business across continents. Cloud providers may choose local IT consultancy firms or resellers of their existing products to act as "resellers" for their Cloud-based products in a particular region [8].

Cloud Consumers: End users that requests for the application belong to the category of Cloud consumers. However, also Cloud service brokers and resellers can belong to this category as soon as they are customers of another Cloud provider, broker or reseller.

In the next sections, cloud storage, possible threats and risks for Cloud Computing are listed.

II. CLOUD SECURITY MODEL FOR SERVICING TO THE CONSUMERS

For understanding the complexity of security aspects in cloud environment this model explains how the basic level communication is done between user and CSP for service providing and also describes the dependency among various layer of cloud that poses great impact on security risks.

During *communication process* consumers are front end and cloud service providers are back end. For resource pooling various steps are included :

- User authentication and login process: In this web browser collects all necessary information about the consumer using various security technologies/protocols like SSL/SSH/TLS.
- Web browser provides all information to policy manager which authenticate the consumer using public key infrastructure, certification authority and others.

- After that consumer request to browser for required services using Simple Object Access Protocol.
- Now web browser delegates the QOS requirements to policy manager, which evaluate the requirements according to service level agreement (SLA). For SLA policy manager also use cloud broker and resources engine.
- For resource discovery cloud broker collects the information about other cloud and their services and resource engine delegates the service requirement to VM schedulers which collaborates the required service from various VM / chunks provider.

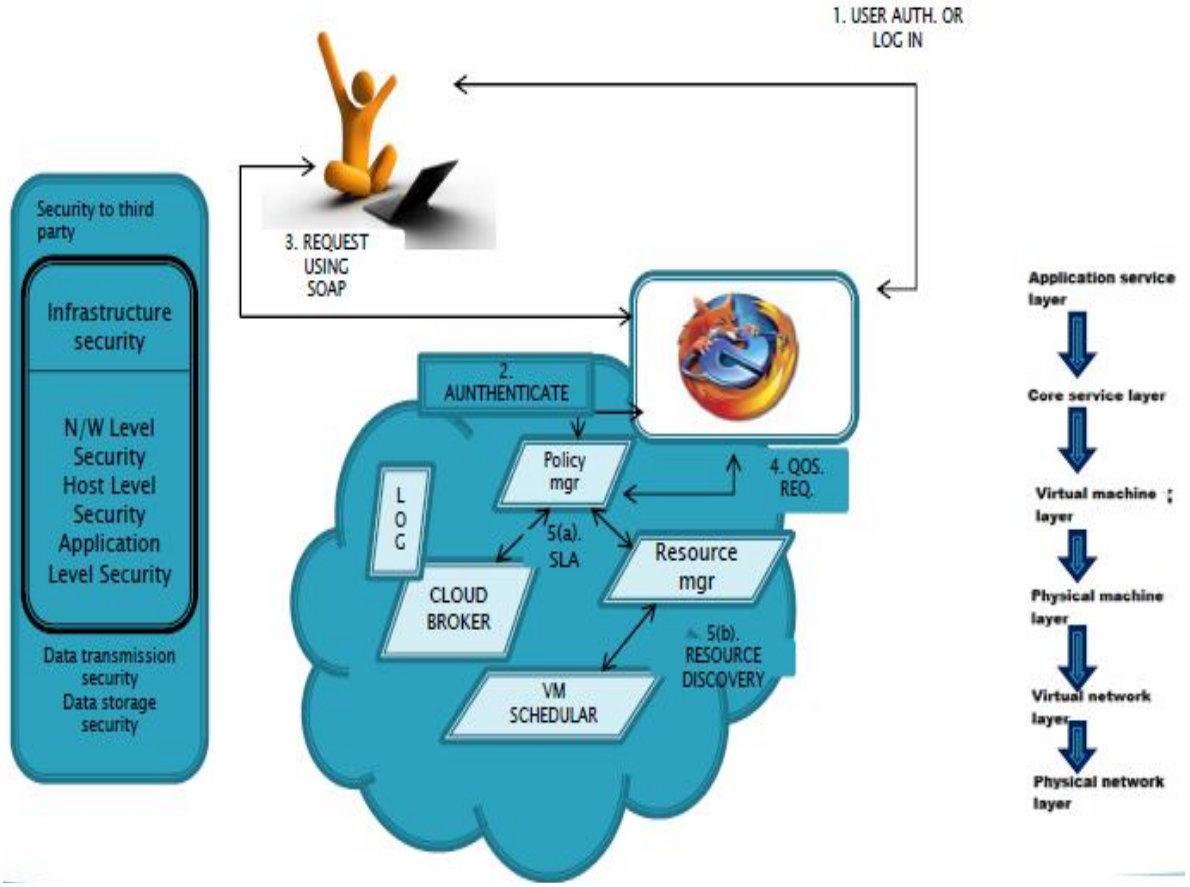

Fig 2. Cloud Security Model

Dependency among Cloud Layers

The application layer and core layer depends upon VMs layer and physical machine layer which further depend upon virtual network layer and physical network layer so damage at any layer also have great impact on other layers.

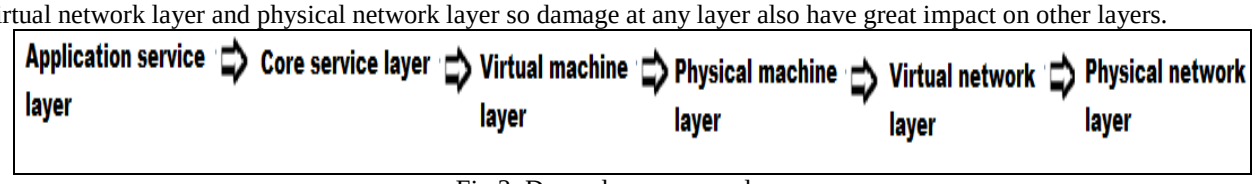

Fig 3: Dependency among layers

Complexity of Security Aspects

When we think about security of organization's core IT infrastructure there is need to provide security at network level, host level, application level and when we talk about data security two aspects are included 'data transmission security and data storage security'.

III. CLOUD SECURITY ISSUES

"Security and privacy are indeed interrelated because the security is provided without having privacy but the privacy is not maintained without security. "

Security is considered a key requirement for cloud computing consolidation as a robust and feasible multipurpose solution.

Today various small and medium size companies moved towards cloud environment because now they are capable to compete with the larger infrastructure companies by simply gaining fast access to best business application at negligible cost. While the cloud offers these advantages there are various issues and risks that reduce the growth of cloud computing. According to the recent IDC enterprise survey Figure shows 74% IT companies has to be taken security as a top challenge prevents the adoption of cloud services. [3]

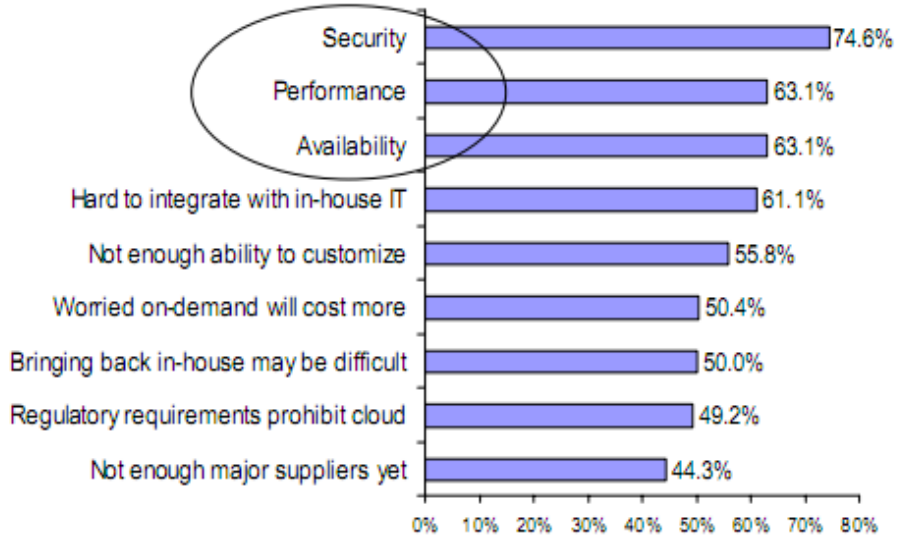

Fig 4: Various issues/challenges to cloud model

The cloud security issues deals with all the challenges associated with securing an organization's core IT infrastructure at the network, host, and application levels as well as the vulnerabilities and attacks related to the data security including: Data-in-transit, Data-at-rest, Processing of data including multitenancy, Data lineage, Data provenance, Data lock-in, . The classification of security issues found within the cloud is [2] [3]:

- Abuse and Nefarious Use of Cloud Computing
- Insecure Application Programming Interfaces
- Malicious Insiders
- Shared Technology Vulnerabilities
- Data Loss/Leakage
- Account, Service and Traffic Hijacking
- Unknown Risk Profile

A. ANALYSIS OF ATTACKS AND VULNERABILITIES IN CLOUD COMPUTING

Due to the nature of cloud system and above mentioned security challenges there are various threats and vulnerabilities that are [2][3][4]:

Network level attacks:

During resource pooling process all data or services flow over the network needs to be secured from following attacks to prevent the leakage of sensitive information:

a) Denial of service/distributed denial of service attack

This attack can overwhelm target's resources so that authorized user is abstained from getting the normal services of cloud. DDOS is also based on DOS attack which can be distributed for more significant effects. This attack is a cause of failure of availability.

b) Eavesdropping

Eavesdropping is an interception of network traffic to gain unauthorized access. It can results in failure of confidentiality.

c) Man in the Middle attack

It is also a category of eavesdropping. The attack set up the connection with both victims that makes conversation and making them believe that they talk directly.

d) Replay attack

The attacker intercepts and save the old messages and then send them later as of participants to gain access to unauthorized resources.

e) Back Door

The attacker gain access to network through bypassing the control mechanisms using "back door" such as modem and asynchronous external connections.

f) Impersonation

It is vulnerability in which malicious node modify the data flow route and lure the node to wrong positions.

g) Sybil Attack
In this a malicious user pretends to be distinct users after acquiring multiple identities and tries to create relationship with honest user if malicious user is successful to compromise one of the honest user then attacker gain unauthorized privileges that helps in attacking process.

h) Byzantine failure
It is a malicious activity which compromised a server or a set of server to degrade the performance of cloud.

Attacks and Vulnerabilities Based on Security Techniques:
If any security technique has weakness in implementation it can cause various vulnerabilities:

- Inside channel attack gain the information from physical implementation of cryptosystem to break the security. The information is like technical knowledge on which encryption implement, time information, power consumption and others.
- SSL/SSH/TLS use the cryptography techniques to secure the data but any crucial flow in implementation of cryptography algorithm can make stronger cryptography technique to weak technique which is a main target of hackers.

Language and Malicious Program Injection Based Attack:
a) Buffer overflow
In which the hacker takes the advantage of program that is waiting for user's input. But in place of user the hacker would enter the input which results to move control to attack code.

b) Trojan horses/Malware
They are the unauthorized program that are contained or injected by malicious user within legitimate program to perform unknown and unwanted function.

c) XML Signature wrapping Attack
It may result in signed documents remaining vulnerable to undetected modification by an adversary.

Web Application Attack:
Web browser is one of the way of providing the web application virtually to users but at the same time they also creates vulnerabilities that are:

a) Weak authentication or weak username- password
It is one of the main targets of malicious users to gain unauthorized access to the services.

b) SQL injection flaws
In which malicious SQL code is erroneously executed in database backend.

c) Cross-site-scripting (XSS)
In which the malicious java script code is executed erroneously by browser.

Virtual Machine Based Vulnerabilities:
- Any malicious program in VM also transferred between other VMs using shared clipboard technology which is an issue for security.
- Many VMs co-exist on same server share CPU, memory, I/O have virtual boundaries. So securing the virtual boundaries is also a challenge for service provider.
- Hypervisor is main controller that maps the physical resources to virtual resources. So if any hypervisor is compromised, it is possible to trace the VMs operations unencrypted.

IV. USE OF CRYPTOGRAPHY IN CLOUD COMPUTING

In cloud computing the users can upload their information to the centralized large data centers where management of data and services are not trustworthy because information is uploaded by the users into cloud data centers not encrypted hence that is accessed by everyone and lead to above mentioned security challenges. For better security of cloud data centers the information is encrypted by the users by using cryptography techniques before uploading into the cloud data centers.
"The cryptography is the art and science of achieving security by encoding messages to make them non- readable".
The original plain text message is in simple English language that can be understood by everyone. The codified message by cryptographic techniques is called as ciphertext message [6][7].
There are three types of cryptographic techniques shown in fig 5:

1) Symmetric Key Cryptography
2) Asymmetric key cryptography
3) Hash Function Cryptography

Symmetric key Cryptography

The symmetric cryptography techniques use the same key or single key for both encryption and decryption process. Because of single key the encryption decryption is fast but more security risks are here. Hence there is less resource and time consumption and but integrity lost problem because the key can be guessed easily by the attackers. Because of same key these are not secure. The various Symmetric key algorithms are: DES, AES, Blowfish, RC4, and RC5 [6].

Asymmetric Key Cryptography

In asymmetric key cryptography techniques two keys are used one is private key that is kept secret and never shared other is public key that is shared. The private key is used for decryption and the public key is used for encryption process. The asymmetric key cryptography provides a better security because two keys are used for encryption and decryption but big disadvantage is it consumes a more resource and time for encryption and these are very complex require a lot of mathematical calculations, tables for Implementation. The various asymmetric key algorithms are: RSA, Diffie Hellman's key exchange, DSA, Elliptic curve [6].

Hash Function Cryptography

The hash function cryptography (One way cryptography) offers a way of creating a fixed-size blocks of data by using entry data with variable length. It is also known as taking the digital fingerprint of the data, and the exit data are known as message digest or one-way encryption. If the data is modified after the hash function was generated, the second value of the hash function of the data will be different. Even the slightest alteration of the data like adding a comma into a text, will create huge differences between the hash values. The hash values solve the problem of the integrity of the messages [14]. The most used hash function cryptography techniques are: SHA1, MD5.

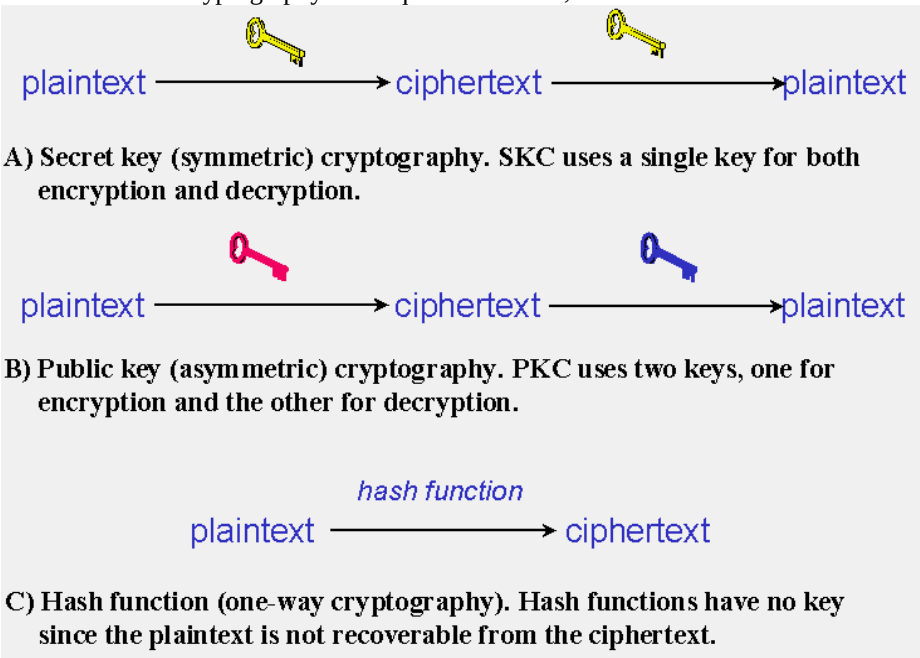

Fig 5: The main three cryptographic techniques

Table 1: Comparison table for three cryptographic techniques

Parameters:	**Symmetric Key:**	**Asymmetric Key :**	**Hash Function :**
Computational Speed Up:	Fastest	Slow	Fast
Collision Resistant:	No	No	Yes
Key agreement/ exchange:	A big problem	No problem at all but requires a lot of mathematical calculations.	No such problem at all
Complexity:	Less	More complex	Less than asymmetric
Delays:	Less	More	Less than asymmetric
Security:	Easily breakable	Better than symmetric key	Impossible to break
Software Implementation:	Difficult, require tables & complex programs	Difficult, require tables & complex programs	Simple, does not need any large programs or complex tables

The symmetric, asymmetric key cryptography techniques are too complex and take a more time. If delays are more then security risks are more. But the hash function cryptography is not complex. It takes less time for execution than above. If takes less time means delays are less and security risks are less.

The cryptography is also a dynamic key and static key. In dynamic key the each time a message is encrypted with different key. But in static key same key is used every time. Hence it is more vulnerable to attacks.

Even the single cryptographic techniques do not provide the better security. Each technique has its own advantages and disadvantages. So, hybrid approaches proposed for it. The hybrid approaches are the combination of advantages and disadvantages of one or more cryptographic techniques.

V. RELATED WORK

Dr. K.V.V. Satyanarayana et. al prescribed an effective cloud security application for how effectively the information is uploaded to the virtual data centers to ensure the privacy. To enhance the privacy the available existing cryptography techniques are symmetric and asymmetric in nature.

Aws Naser Jaber et. al define how effectively the cryptography is used in cloud computing. This paper is a survey of specific security issues brought by the use of cryptography in a cloud computing system**.**

Tanisha et. al proposed a methodology suggests a new security scheme for the files to be uploaded on the cloud. The integrity and confidentiality is ensured by encrypting the data using a combination of two tier hybrid encryption and the digital signature scheme that provides access to the data only on successful authentication.

Gurpreet Kaur et. al analyzes the performance of security algorithms, 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.

HanumanthaRao. Galli et. al proposed a method that uses hybrid encryption and digital signature scheme. The integrity of the data can be achieved by generating message digest using MD5 algorithm. By using Blowfish algorithm data can encrypted for providing confidentiality. Authentication takes place by RSA algorithm.

Khushdeep Kaur et. al proposed a combination of DSA, RSA and MD5as a hybrid link for wireless devices. It considered case study for Manet networks so that to suggest the applications of proposed algorithm.

Kawser Wazed Nafi et. al proposed a newer security structure for cloud computing environment with AES for file encryption, RSA system for secure communication, Onetime password to authenticate users and MD5 hashing for hiding information.

Kumar Dubey et. al prescribed a new cloud computing environment where we approach a trusted cloud environment. For it RSA and MD 5 algorithm are applied.

VI. CONCLUSION AND FUTURE DIRECTIONS

In this review different kind of cloud computing security issues are discussed that exploit the security system. From the whole survey, the notion of data privacy is addressed that is impossible to maintain without security and the degree of trust afforded to a cloud service provider is analysed. Hence it is required for the cloud service providers to secure a data transmission at cloud data centers. The different approaches are proposed for security as discussed in related work. But all these are combination of all three cryptographic techniques that are too complex in terms of computational efficiency. This work will be extended for new algorithm defend the existing work or provides more efficient results than existing methods in near future.

REFERENCES

[1] D. Subbiah, S. Muthukumaran, T. Ramkumar**,**, "The enhanced survey and proposal to secure the data in cloud computing environments", IJEST, vol.5, no.01, January 2013.

[2] Liu, P. You, Y. Peng, "Security Issues and Solutions in Cloud Computing", IEEE-computer society, 2012.

[3] R. Padhy, M. Patra and S. Satapathy, "Cloud Computing: Security Issues and Research Challenges", IJCSITS, Vol. 1, No. 2, December 2011.

[4] M.Walloschek, B.Grobauer, E.Stöcker,"Understanding of Cloud Computing Vulnerabilities", IEEE Computer and Reliability Society, 2011.

[5] S. Hariri, Y. Al - Nashif, "Resilient Cloud Data Storage", ACM-NSF Center for Cloud and Autonomic Computing, 2013

[6] William Stalling, A Handbook on "Cryptography and network Security" by Pearson Education, 2009

[7] A. Jaber, M. Fadlili, "The Use of Cryptography in Cloud environment", IEEE International Conference and Computing and Engineering, December 2013.

[8] D.Rajesh Kumar, R. Gupta, Tanisha, "File Security in Cloud using Two-tier Encryption and Decryption", IJARCSSA, vol.3, issue 7, July 2013.

[9] A Tejaswi, K. Satyanarayana, Radhika G, "Efficient Framework for Deploying Information in Virtual Datacenter with Cloud Security Application", International Journal of Emerging Technology and Advanced Engineering, vol.3, issue 1.

[10] Gurpreet Kaur, Manish Mahajan, "Analyzing the Data Security for a Cloud Computing Using Cryptographic Algorithms", International Journal of Engineering Research and Applications, vol.3, issue 5, pp.782-786, Sep-Oct 2013.

[11] H. Galli, Padmanabham, "Data Security in Cloud using the Hybrid Encryption and Decryption", IJARCSSE, vol.3, issue 10, Oct.2013.

[12] Hashem, K. Nafi, Tonny S. Kar, S. Hoque, "The Newer user authentication, File encryption & Distributed server based Cloud Computing security architecture", International Journal of Advanced Computer Science and Applications, vol.3, no.10., 2012

[13] K. Kaur, Er. Seema, "The Hybrid Algorithm with DSA, RSA and MD5 Encryption Algorithm for wireless devices", International Journal of Engineering Research and Applications, vol.2, issue 5, Sep-Oct 2012.

[14] K. Dubey, M. Namdev, S. Shrivastava, "Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment", IEEE sixth international conference, 2012.

Authors Bibliography:

Er. Jashanpreet Pal Kaur has received her B.Tech degree in Computer Science and Engineering from MIMIT, Malout under PTU, Jalandhar in 2012. She is pursuing M.Tech (Regular) degree in computer engineering from Yadvindra College of Engineering, Punjabi University Guru Kashi Campus, Talwandi Sabo (Bathinda). Her research interest is in the field of networking (Cloud computing).

Er. Rajbhupinder Kaur has received her M.Tech Degree from Punjabi University, Patiala in 2010 and B.Tech degree from Punjab Technical University, Jalandhar in 2006. She is working as Assistant Professor in Yadavindra College of Engineering, Talwandi Sabo, Bathinda Punjab. Her research interests are in the fields of Mobile Ad-Hoc Network, Network Security, Nanotechnology, wireless sensor networks. She has published many national & international papers.

