SCITECH
RESEARCH ORGANISATION|
Volume 5, Issue 1
October 28, 2015
Journal of Information Sciences and Computing Technologies
www.scitecresearch.com/journals

Cloud Computing Security: A Survey

ElahehGolzardi

Department of Electrical and Electronic Engineering, Kurdistan PNU, Iran.

Abstract

Today, the world of Internet and Information technology, which is turned into a crucial part of human life, is growing rapidly. In this direction, the needs of societies` members including: information security, fast processing, immediate & dynamic access and the most important one, cost saving have been taken into consideration. Security issues used to be the main challenge of the systems` users constantly. A crucial achievement, by which users` data are accessed broadly & comprehensively, is cloud computing and storage in clouds, but this requires establishing data security in a very reliable environment.

Cloud based computing, as a new generation of computing infrastructure, was created to reduce the costs of hardware & software resource management and it`s success is due to it`s efficacy, flexibility and it`s security in comparison to other computing approaches. Supporting security of stored data is one of the difficulties and issues discussed in cloud computing field. Our goal is to understand present challenges and solutions in cloud based environment; furthermore, we investigate present algorithms, in terms of application`s speed both in cloud based environment and local networks.

Keywords: Cloud Computing; Decryption & Encryption.

1. Introduction

Today, data storing and retrieving in PCs, small and big networks turned into a critical and costly issue, but by passing the time and introducing cloud computing the technology has been improved significantly. While most of the issues relating to the users and organizations reduced by computing and cloud storage. Some advantages of networking include less costly, accessibility, flexibility, and etc. Although establishing a network makes many state and private organizations to use the service to promote their goals; many businesses don't move toward the cloud, since beside numerous advantages it bears disadvantageous consequently people prefer not to use the technology. In this paper first, we investigate effective intrusion of accessibility, integrated reliability of cloud resources and services, then recommendations and solutions in cloud environment suggested.

2. Literature Survey

In 1990 the world was introduced to the internet and we began to see distributed computing power realized on large scale. Today we have the ability to utilize scalable distributed computing environment within the confines of internet, such a practice is known as cloud computing. As we already know there is lots of hype associated with cloud computing.

In [4] the author says that the US National Institute of Standards and Technology (NIST), an agency of the Commerce Department Technology Administration, has created a cloud computing security group. This group considers its role as promoting the effective and secure use of the technology within government and industry by providing technical guidance and promoting standards NIST has recently released its draft wide to adopting and using the Security Content Automation Protocol which identifies a quite of specifications for organizing and expressing security-related information in standard ways, as well as related data, such as identifiers for software flaws and security configuration issues.

In [1] the author elaborates the various unresolved issues threatening cloud computing adoption and affecting the various stake-holders associated with it. The author presents an approach which is aimed at developing an understanding of the security threats that hamper the security and privacy of a user. The various characteristics of a secure cloud infrastructure (public or private) have been discussed and also its challenges and the ways to solve them.

In [11] the author has worked towards facilitating the client in getting a proof of integrity of the data which he wishes to store in the cloud storage servers with bare minimum costs and efforts. The scheme was proposed by the author to reduce the computational and storage overhead of the client as well as to minimize the computational overhead of the cloud storage server.

In [15] author suggests authentication and encryption for secure data transmission from one cloud to other cloud that requires secure and authenticated data with elliptic curve cryptography. The author has made use of Elliptic curve cryptography to provide confidentiality and authentication of data between clouds.

In [16] author considers the cloud environment as a new computing platform to which the classic methodology of security research can be applied. The author determines to employ an attribute-driven methodology to conduct their review.

In [14] the author analyses the basic problem of cloud's data security. With the analysis of the architecture of HDFS, they get the data security requirements of cloud computing and set up a mathematical data model for cloud computing.

3. Cloud Computing

There are various definitions in terms of cloud computing s in the literature. Cloud computing refers to a model to support easy accessibility based on users` applicants via a network to a set of adaptable computing resources (such as networks, servers, storing space, applied programs and services) to be supported and delivered with minimum need to resource management and or direct involvement of service providers.

Cloud computing refers to the users` data storing in a storage system kept by a third party.

3.1. Cloud provides services in various forms

- Software as a Service-SaaS (e.g. Google apps, 2011),

- Platform as a Service-PaaS (e.g. Google app engine (2011)), Microsoft's Azure (Azure services platform, 2011))

- Infrastructure as Service-IaaS (e.g. Amazon web services, 2011(AWS).

3.2. Cloud Computing Architecture Components

- Cloud Consumer: It can be a person or organization who wants to use service from Cloud Providers.

- Cloud Provider: A person or organization who provides the services to the users.

- Cloud Auditor: A party who has to verify whether cloud provider is providing the services to user according to the service level agreement or not.

- Cloud Broker: It is the intermediate between cloud provider and the user.

- Cloud Carrier: It is the transport media by which services are routed to intended user.

3.3. Cloud Development Models

- Private cloud: an organization is the owner of private cloud. In fact, it refers to cloud computing in private networks.

- Public cloud: A service provider (for example Amazon, Google, Microsoft) is the owner of the cloud and it`s sources are sold to the public. Generally end-users are able to manage allocated resources based on their needs.

- Community cloud: It is similar to private cloud but the only difference is that the cloud resources deployed between the group members or some private organizations via data sharing.

- Hybrid cloud: The environment of hybrid cloud combines various models of private and community clouds.

4. Security of Cloud Computing

Cloud computing to a large extent addresses the issues of flexible & elastic architecture. Cloud security is a common reciprocal responsibility between cloud provider and cloud user in which they need a reliable and complementary relationship. The issue of cloud computing security is a vital and critical one because many users and organizations choose the technology to promote their goals. Thus, in next section we will investigate advantages, challenges, and present solutions of the field.

4.1. Security Advantages in Cloud Environments

Current cloud service providers operate very large systems. They have complex processes and expert personnel for maintaining their systems, which small enterprizes may not even have access. Thus, there are many direct and indirect

security advantages for the cloud users. Here we present some of the main security advantages of a cloud computing environment:

-Forensic Image Verification Time Some cloud storage implementations expose a cryptographic check sum or hash. For example, Amazon S3 generates MD5 (Message-Digest algorithm 5) hash automatically when you store an object.

- Incident Response IaaS providers can put up a dedicated forensic server that can be used on demand basis. As soon as, a security violation takes place in the cloud environment, the server can be brought online. In some investigation cases, even a backup of the environment can be easily made and put onto the cloud without affecting the normal course of business.

- Data Centralization In a cloud environment, the cloud service provider takes care of storage issues and small businesses need not spend a lot of money on physical storage devices. Cloud based storage provides a way to centralize the data in a faster and potentially cheaper manner. This is very useful for small businesses, which cannot spend more money on security parameters to secure the data.

- Logging In a traditional computing paradigm by and large, logging is considered an afterthought. Allocating insufficient disk space makes logging either non-existent or minimal. However, in a cloud, storage the need for standard logs is automatically solved.

5. Challenges

5.1. Intrusions to Cloud systems

There are several common intrusions affecting availability, confidentiality and integrity of Cloud resources and services [16].

5.1.1. Insider attack

Authorized Cloud users may attempt to gain (and misuse) unauthorized privileges. Insiders may commit frauds and disclose information to others (or modify information intentionally). This poses a serious trust issue. For example, an internal DoS attack demonstrated against the Amazon Elastic Compute Cloud (EC2).

5.1.2. Port scanning

Port scanning provides list of open ports, closed ports and filtered ports. Through port scanning, attackers can find open ports and attack on services running on these ports. Network related details such as IP address, MAC address, router, gateway filtering, firewall rules, etc. can be known through this attack. Various port scanning techniques are TCP scanning, UDP scanning, SYN scanning, FIN scanning, ACK scanning, Window scanning etc. In Cloud scenario, attacker can attack offered services through port scanning.

5.1.3. Attacks on virtual machine (VM) or hypervisor

By compromising the lower layer hypervisor, attacker can gain control over installed VMs.

Through these attacks, hackers can be able to compromise installed-hypervisor to gain control over the host.

5.1.4. User to root attacks

Here, an attacker gets an access to legitimate user's account by sniffing password. This makes him/her able to exploit vulnerabilities for gaining root level access to system. For example, Buffer overflows are used to generate root shells from a process running as root. It occurs when application program code overfills static buffer. The mechanisms used to secure the authentication process are a frequent target. There are no universal standard security mechanisms that can be used to prevent security risks like weak password recovery workflows, phishing attacks, key loggers, etc. In case of Cloud, attacker acquires access to valid user's instances which enables him/her for gaining root level access to VMs or host.

5.1.5. Backdoor channel attacks

It is a passive attack which allows hacker to gain remote access to the infected node in order to compromise user confidentiality. Using backdoor channels, hacker can control victim's resources and can make it as zombie to attempt DDoS attack. It can also be used to disclose the confidential data of victim. Due to this, compromised system faces difficulty in performing its regular tasks.

In Cloud environment, attacker can get access and control Cloud user's resources through backdoor channel and make VM as Zombie to initiate DoS/DDoS attack.

5.1.6. Flooding attack

In this attack, attacker tries to flood victim by sending huge number of packets from innocent host (zombie) in network. Packets can be of type TCP, UDP, ICMP or a mix of them. This kind of attack may be possible due to illegitimate network connections. In case of Cloud, the requests for VMs are accessible by anyone through Internet, which may cause DoS (or DDoS) attack via zombies. Flooding attack affects the service's availability to authorized user. By attacking a single server providing a certain service, attacker can cause a loss of availability of the intended service. Such an attack is called direct DoS attack. If the server's hardware resources are completely exhausted by processing the flood requests, the other service instances on the same hardware machine are no longer able to perform their intended tasks. Such type of attack is called indirect DoS attack. Flooding attack may raise the usage bills drastically as the Cloud would not be able to distinguish between the normal usage and fake usage.

5.2. Seven risks

Defines seven risks a user should raise before committing:

- Sensitive data should be processed outside the enterprise only with the assurance that they are only accessible and propagated to privileged users.

- One customer data should be fully segregated from those of another customer.

- A customer needs to verify if the infrastructure complies with some regulatory security requirements.

- The cloud provider should commit to store and process data in specific jurisdictions and obey local privacy requirements on behalf of the customer who do not know where data is stored.

- The cloud provider should offer replication and disaster recovery mechanisms.

- Investigative support needs to be ensured.

- Data should be accessible even when the provider is acquired by another company or if the user moves to another provider.

6. Solutions

Following solutions can be used to address mentioned challenges stated at above:

6.1. Firewalls: common solution to intrusions

Firewall protects the front access points of system and is treated as the first line of defense. Firewalls are used to deny or allow protocols, ports or IP addresses. Firewall (in Cloud) could be the common solution to prevent some of the attacks listed above.

6.2. IDS and IPS techniques: evolution

Another solution is to incorporate IDS or IPS in Cloud. However the efficiency of IDS/IPS depends on parameters like technique used in IDS, its positioning within network, its configuration, etc. Traditional IDS/IPS techniques such as signature based detection, anomaly detection, artificial intelligence (AI) based detection etc. can be used for Cloud.

6.2.1. Various types of IDS/IPS used in Cloud computing

There are mainly four types of IDS used in Cloud: Host based intrusion detection system (HIDS), Network based intrusion detection system (NIDS), Hypervisor based intrusion detection system and Distributed intrusion detection system (DIDS).

- Host based intrusion detection systems (HIDS)

HIDS monitors and analyzes the information collected from a specific host machine. HIDS detects intrusion for the machine by collecting information such as file system used, network events, system calls, etc. HIDS observes modification in host kernel, host file system and behavior of the program. Upon detection of deviation from expected behavior, it reports the existence of attack. The efficiency of HIDS depends on chosen system characteristics to monitor.

Strengths:

- Identify intrusions by monitoring host's file system, system calls or network events.

- No extra hardware required.

Challenges:

- It can monitor attacks only on host where it is deployed.

- Need to install on each machine (VMs, hypervisor or host machine).

- Network based intrusion detection system (NIDS)

NIDS monitors network traffic to detect malicious activity such as DoS attacks, port scans or even attempts to crack into computers. The information collected from network is compared with known attacks for intrusion detection. NIDS has stronger detection mechanism to detect network intruders by comparing current behavior with already observed behavior in real time. NIDS mostly monitors IP and transport layer headers of individual packet and detects intrusion activity. NIDS uses signature based and anomaly based intrusion detection techniques. NIDS has very limited visibility inside the host machines. If the network traffic is encrypted, there is no effective way for the NIDS to decrypt the traffic for analysis.

Strengths:

- Can monitor multiple systems at a time.

- Identify intrusions by monitoring network traffic.

- Need to place only on underlying network.

Challenges:

- Difficult to detect network intrusions in virtual network.

- Difficult to detect intrusions from encrypted traffic.

- It helps only for detecting external intrusions.

- Distributed intrusion detection system (DIDS)

A Distributed IDS (DIDS) consists of several IDS (e.g. HIDS, NIDS, etc.) over a large network, all of which communicate with each other, or with a central server that enables network monitoring. The intrusion detection components collect the system information and convert it into a standardized form to be passed to central analyzer. Central analyzer is machine that aggregates information from multiple IDS and analyzes the same. Combination of anomaly and signature based detection approaches are used for the analysis purpose. DIDS can be used for detecting known and unknown attacks since it takes advantages of both the NIDS and HIDS. In Cloud environment, DIDS can be placed at host machine or at the processing server (in backend).

Strengths:

- Uses characteristics of both NIDS and HIDS, and thus inherits benefits from both of them.

Challenges:

- High communication and computational cost.

- Central server may be overloaded and difficult to manage in centralized DIDS.

7. General Solutions of Cloud Computing Security

7.1. Security Policy

A security policy is a formal statement, comprising a set of rules which should be obeyed and obligated by individuals who access the organization technology and/or information assess. In order to establish the goals, policies should be applied regarding all users, network managers and operational directors of the organization. Generally, the goals are established by focusing on following basic options:

- Delivered services versus delivered security.

- Simple use versus security and immunization`s cost versus the risk of missing information.

The most important goal of security policy is informing the users, network managers and operational directors of the organization in terms of necessary utilities to protect the technology and information assess.

7.2. Understanding Present Network

A list of hardware units and installed applications (and default applications of the system) is required to implement and support the security system meanwhile the index paves the way to measure and recognize related issues.

7.3. TCP/UDP Service Providers and Present Services in Cloud Network

- Any service provider of TCP/UDP in cloud network together with present services on each computer should be recognized and documented.

- If possible, rarely used, unnecessary services and service providers and high vulnerable operational equipment to be inactivated gradually in order to deprive hackers to exploit information

- Access of service providers whose present recognized necessary, limited to computers which are in need of their services

- Sample applications shall not be installed on production systems.

There are two approaches to cope with present threats: 1) Access control and mutual reaction and response. 2) Access Control Mechanism.

8. Comparisons and Charts

Various algorithms are used to establish security in cloud based environment. We discuss several examples of the algorithms and compare them in terms of various aspects, then present the results.

Table 1: Indicates characteristics of encryption algorithms, including utilization method, cloud environment, benefits and weak points shortly.

TABLE 1: Cloud security methods

Cloud environment	Algorithm used	Methodology	Benefits	Weakness
Cipher Cloud, AWS	Caesar Cipher	Reverse Caesar Mechanism ACII-Code	Classify the security issues between Consumer & provider	Hacked algorithm &convenint with a one type of file formatting
Drop box, AWS	DES	DES-CBC Architecture design	Provide a trusted environment for store files	Hacked by DPA, mim attack
GoogleApps, Eclipse	RSA, MD5 & AES	Non	Speed up calculation for the 3 different algorithm	Poor samples are taken
Eclipse,Cipher Cloud	AES	BCC-Matrices selective algorithm	Speed of Enc/Dec. files	Loss controller on BCC from the e.user, leaked for quantum attack
AWS, Cipher Cloud	RSA, EC	CCOA architecture	Eliminate the security concerns	Vulnerable to timing attack

Most encryption algorithms were developed and applied in order to prepare more reliable process of data transmit in cloud process environment including: DES, AES, RC4**,** Blowfish&3DES for symmetrical classifying and RSA&DH for asymmetrical classification. The algorithms were investigated with respect to encryption time, decryption, size of coded files` output and to insure data reliability in cloud environment.

Characteristics of symmetric & asymmetric encryption presented in next section and the results are presented in Table2.

TABLE 2: Characteristics of algorithms

Encryption algorithm	Key size (bits)	Input size (bits)	Security against attack	Initial vector size (bits)
RC4	256	256	Bit flipping attack	256
AES	128, 192, 256	128	Choose n-plain, know n-plain text	128
Blowfish	32 – 448	32	Dictionary attack	64
3-DES	112 – 168	64	Brute force attack	64
DES	56	64	Brute force attack	64
RSA	<1024	<1024	Timing attack	-
DH	n-Key exchange	N	Ping attack	-

Regarding the above chart, one can say that symmetric encryption is more popular than asymmetric encryption. Furthermore, asymmetric methods benefit complexities in breaking codes, which is due to using longer key. Meanwhile data transmit in symmetric method is faster than asymmetric one.

In another test, we investigated the speed of various algorithms in terms of different inputs and the results presented below.

In the test, the time of symmetric methods were analyzed via local instruments and cloud network and operation time and input size was calculated in seconds and Kb respectively.

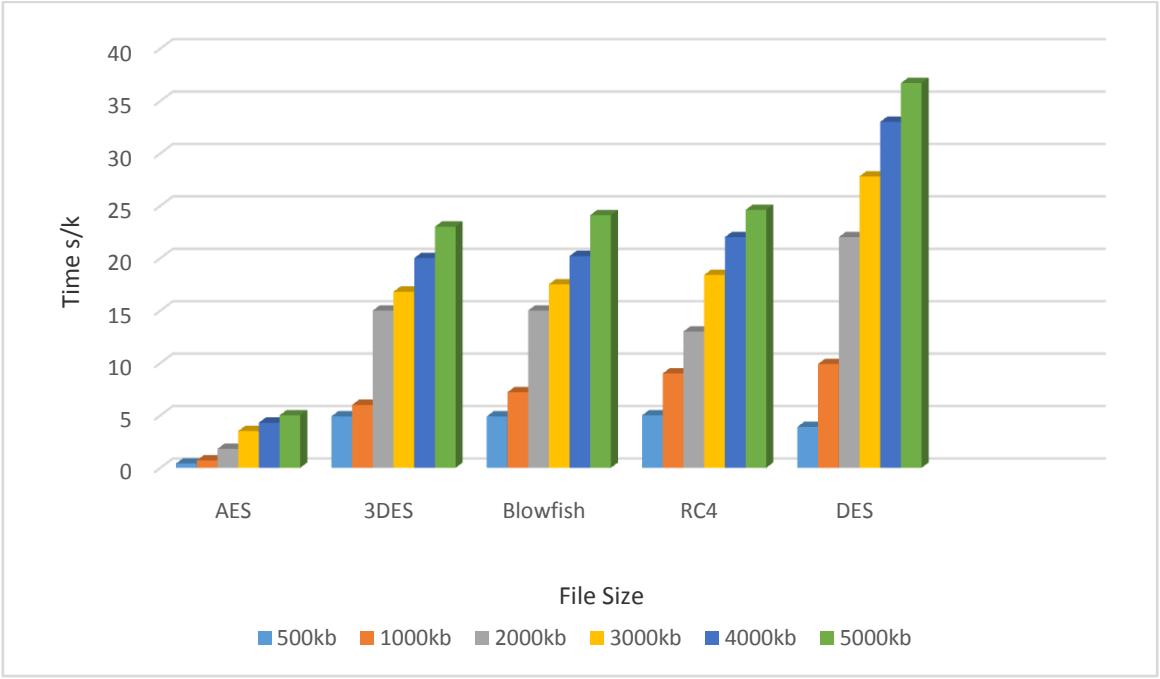

FIGURE 1: Comparison of the time of algorithms` operation in local network

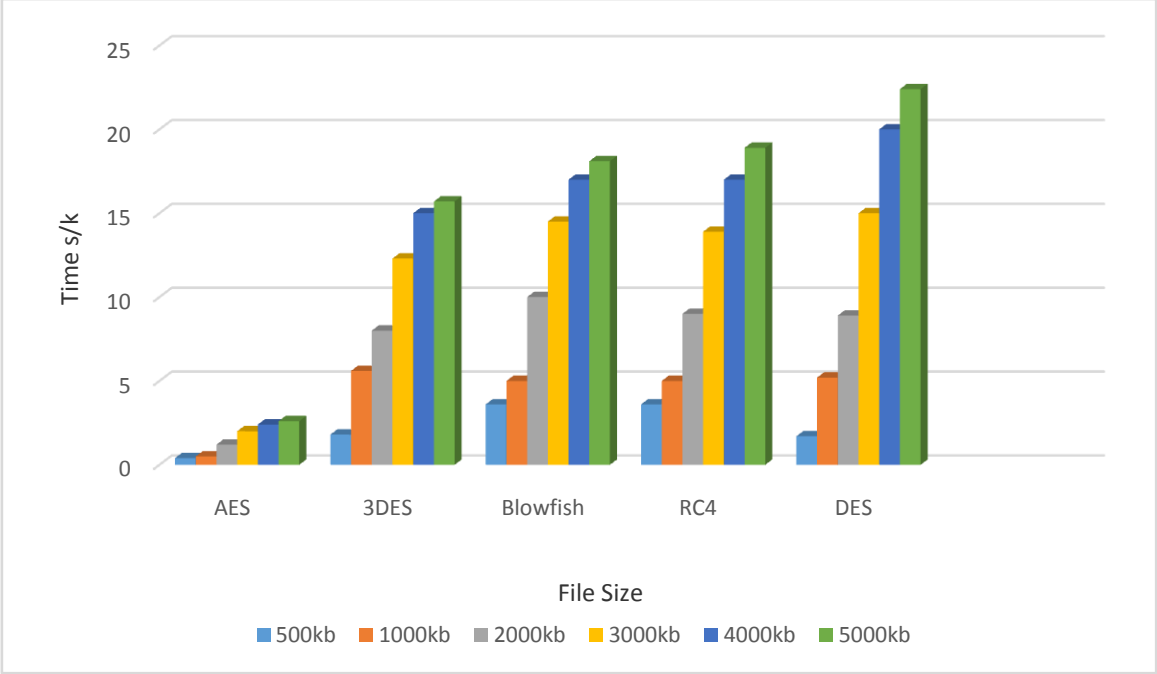

FIGURE 2: Comparison of the time of algorithms` operation in cloud network

According to the result mentioned above, we conclude that:

- Running time of data transmit in cloud network is faster than that of local machine

- There is a reversed ratio between running time and input file size, meaning that increasing input file`s size decreases running time.

- AES is the fastest symmetric method and scalable on different hard-wares and it is operated simply.

- Symmetric encryption operates faster than asymmetric one.

- In symmetric encryption, size of input file changes in terms of operation of coded file. Meanwhile in asymmetric methods, the input file`s volume is fixed.

9. Conclusion

Cloud computing has had significant advances in recent years and the advantages of cloud computing are visible for everyone. This method has more memory, flexibility, and finally reducing the costs.

We investigated many intrusions that can threat integrity of cloud environment since Firewall may not suffice for solving the issues of cloud security. Furthermore, we compared symmetric & asymmetric algorithms and investigated them through various inputs.

Through the comparisons, we concluded that cloud environment is more effective than local machine and AES encryption algorithm is more resistant in coping with hack attacks but it suffers from quantum attacks. Since encryption is one of important operations of data security, one can promote and develop security and privacy by selecting an appropriate algorithm.

10. References

[1] A. Sangroya, “Towards Analyzing Data Security Risks In Cloud Computing Environments,” JULY, August 2010.

[2] Ch. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, “A Survey Of Intrusion Detection Techniques In Cloud,” Journal of Network and Computer Applications, pp. 42–57, 2013.

[3] Grobauer, T. Walloschek, and E. Stocker, "Understanding Cloud Computing Vulnerabilities," IEEE Security and Privacy, vol. 99, 2010.

[4] K. J. Harauz. “Data security in the world of cloud computing,” IEEE Computer and Reliability Society, 2010.

[5] K. S. Wagh, R. Jathar, S. Bangar, and A. Bhakthadas, “Securing Data Transfer in Cloud Environment,” International Journal of Engineering Research and Applications, Vol. 4, pp. 189-193, 2014.

[6] M. A. Morsy, J. Grundy, and I. Muller, "An Analysis of the Cloud Computing Security Problem," In ProcApsec 2010 Cloud Workshop, 2010.

[7] M. Firdhous, O. Ghazali, and S. Hassan, "Trust Management in Cloud Computing: A Critical Review," International Journal on Advances in ICT for Emerging Regions, vol 04 (02), pp. 24 – 36, 2011.

[8] P. Kresimir and H. Zeljko, "Cloud Computing Security Issues And Challenges," In PROC Third International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, pp. 344-349, 2010.

[9] S. Kumar, and N. K. Dogra, "Cloud Storage and its Secure Overlay Techniques," International Journal of Engineering Research and Applications, Vol. 4, pp. 33-37, 2014.

[10] S. Ramgovind, M. M. Eloff, and E. Smith, "The Management of Security in Cloud Computing," In PROC 2010 IEEE International Conference on Cloud Computing, 2010.

[11] S. S. Kumar R, "Data integrity proofs in cloud storage," 2011.

[12] S. SHARMA, and A. CHUGH, "Survey Paper on Cloud Storage Security," International Journal of Innovative Research in Computer and Communication Engineering, vol. 1, 2013.

[13] S. Subashini, and V. Kavitha, "A Survey on Security Issues in Service Delivery Models of Cloud Computing," J Network ComputAppl doi:10.1016/j.jnca.2010.07.006, 2010.

[14] T. Ch. Dai Yuefa, and Wu Bo, "Data Security Model for Cloud Computing," pp. 21-22, 2009.

[15] V. Gampala, "Data Security in Cloud Computing with Elliptic Curve Cryptography," International Journal of Soft Computing and Engineering (IJSCE), vol.2, 2012.

[16] Zh. Xiao, and Y. Xiao, "Security and Privacy in Cloud Computing," IEEE COMMUNICATIONS SURVEYS and TUTORIALS, 2015.

[17] I. M. Khalil, A. Khreishah, & M. Azeem, "Cloud Computing Security: A Survey," *Computers*, *3*, 1-35; doi:10.3390/computers3010001, 2014.