International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 06, June-2015

Data Security and Cryptography in Cloud Environment

S. Balamurugan
Research Scholar,
Department of Computer Science
Bharathiar University
Coimbatore, Tamil Nadu, India.

Dr. Sanjay Pande
Professor and Head,
Department of Computer Science & Engineering
G M Institute of Technology, Davangere
Karnataka, India

***Abstract* – Cloud is an intelligent computing delivery service. It provides unlimited service provisioning to users based on their demand. Services are processed by automated APIs(Application Programming Interface) without human interaction. Storage is one of the main services from the Cloud. Users could outsource their data to cloud. Cloud provides reliable storage. Data outsource to cloud are stored in different cloud datacenter located in different geographical location to maintain the reliable storage. Cloud has many challenges like scalability, resource allocation, virtualization, security, trust, service level agreement and etc. Among these challenges, security is the top level concern in cloud storage. Cloud storage has many security related issues. Traditionally, Security is addressed by cryptography techniques. This paper describes the data security challenges, importance of security and security mechanism for cloud storage. Different security mechanisms are addressed in this paper, among them confidentiality, integrity and authentication are important for data security in cloud. An efficient cryptography technique might protect the cloud environment from unauthorized usage.**

Keywords – Cloud Storage; Data Security; Cryptography; Symmetric Encryption; Asymmetric Encryption;

I. INTRODUCTION

Cloud computing is defined as a specializeddistributed computing model, which is dynamically configured and delivered on demand[1].This new massively scalable paradigm is different from traditional networks. It is highlyabstract to deliver three levels of services [2].Economically, the main attractiveness of cloud computing is that users only use what theyneed, and only pay for what they actually use. Resources are available to be accessedfrom the cloud at any time, and from any location through networks [3]. There is no need toworry about how things are being maintained. The US National Institute of Standards andTechnology (NIST) [4]provide a formal definition of the cloud computing as follows:

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand networkaccess to a shared pool of configurable computing resources (e.g., networks, servers, storage,applications, and services) that can be rapidly provisioned and released with minimalmanagement effort or service provider interaction."

The main core area of Cloud computing is Virtualization [5]. Virtualization empowers the cloud as a scalable and elastic service environment. It enables a dynamic datacentre where servers provide a pool of resources that are connected as needed, where the relationship of applications to compute, storage, and network resources changes dynamically in order to meet both workload and business demands[6].

In the Cloud Computing Services Survey conducted during August 08/09 by IDC IT group [7], users were asked to rate their issues and challenges experienced with Cloud computing. The results shown in Figure 1 illustrate that security is the biggest concern. Information security, availability and performance issues still remain in the top 3 for both years the survey was done. Security is the main issue users are concerned with when considering Cloud computing solutions[8].

A. Importance Characteristics of Cloud:

Cloud has five essential characteristics [9] which provide unique features to the cloud than other computing [10].

- On-Demand Self-Service: It enables users to use cloud computing resources without human intervention between the users and the Cloud ServiceProviders (CSP). Instant usage of resources and elimination of human intervention provide efficiencies and cost savings to both the users and the CSPs.
- Broad Network Access: Cloud computing is an efficient and effective replacement for in-house data centres. High-bandwidth communication links must be available to connect to the cloud services. High-bandwidth network communication provides access to a large pool of computing resources.
- Location-Independent and Resource Pooling: Computing resources are pooled to serve multiple users using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to users' demand. Applications require resources. However, these resources can be located anywhere in the geographic locations physically and assigned as virtual components whenever they are needed. There is a sense of location independence that the users generally have no control or knowledge over the exact location of the provided resources. At the same time, this helps to specify location at a higher level of abstraction (e.g., country, state, or datacentre).

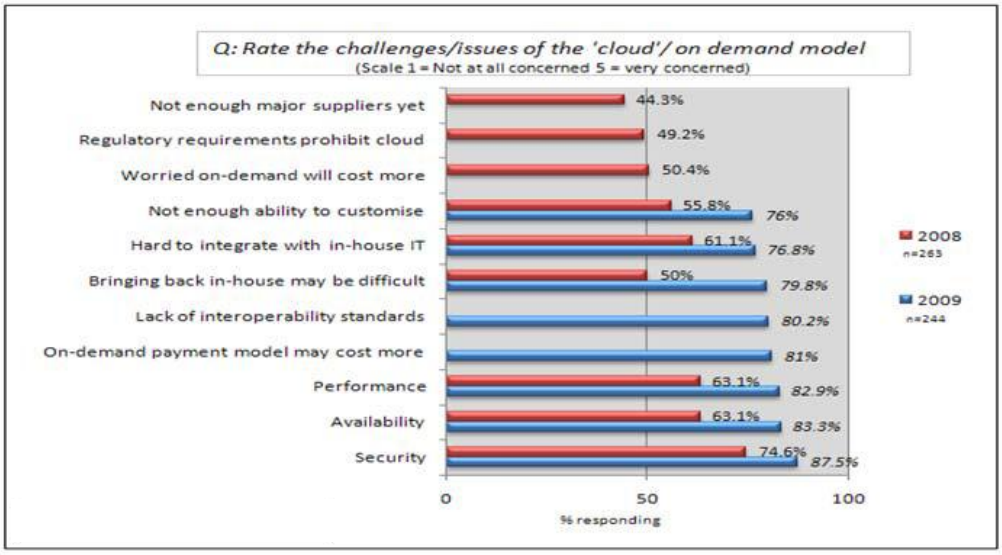

Figure 1.IDC Survey on 08/09 about Cloud Computing Chanllenges [8]

- Scalability: It enables new nodes to be added or dropped from the network like physical servers, with limited modifications to infrastructure set up and software. Cloud architecture can scale horizontally or vertically, according to users'demand.
- Measured Service: The usage of cloud resources by the users are monitored by APIs in the cloud. Users are billed automatically based on the usage of cloud resources. Cloud systems automatically control and optimize resource usageby leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported by providing transparency for both the CSPs and the users of the utilized service.

B. Cloud Services:

The cloud computing services are broadly divided into three categories namely, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) [11].

- Infrastructure as a Service (IaaS)

IaaS is the delivery of huge computing resources such as the capacity for processing, storage and network. For example, when users use the storage service of cloud computing, they just pay the consuming part without buying any storage disks or even knowing nothing about the location of the data they deal with the cloud. Sometimes the IaaS is also called Hardware as a Service (HaaS). The top level infrastructure providers are Amazon EC2, Rack Space, etc.

- Platform as a Service (PaaS)

PaaS generally abstracts the infrastructures and supports a set of API to cloud applications. It is the bridge between hardware and application. Because of the importance of platform, many big companies want to grasp the chance of predominating the platform of cloud computing as Microsoft does in personal computer time. The well-known cloud platform providers are Google App Engine (GAE) and Microsoft's Azure Services Platform (MASP).

- Software as a Service (SaaS)

SaaS aims at replacing the applications running on PC. There is no need to install and run the special software on users' computer if users use the SaaS in the cloud. Instead of buying the software at a relatively higher price, users just follow the pay-per-use pattern which would reduce their total cost. The concept of SaaS is attractive, and softwares run well as cloud computing, but the delay of network is fatal to real time or half real-time applications. The top level software providers are Google, Microsoft, Salesforce.com, etc.

C. *Deployment Models:*

Cloud is deployed in four types of deployment models as defined by NIST such as Public, Private, Community and Hybrid cloud [4].

Private cloud infrastructure is operated solely for a single organization and managed by that organization or a third party. It is also known as internal cloud. Private clouds are hosted by third parties, rather than being hosted on dedicated servers. Hosting companies operate large datacentres and people who require their data to be hosted, buy or lease storage capacity from providers and use it for their storage.

Public cloud or external cloud describes cloud computing in the traditional mainstream, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via web applications or web services. The resources are provisioned from an off-site third-party CSPs who bill on a utility computing basis.

Community cloud may be established where several organizations have similar requirements and seek to share infrastructure so as to realize some of the benefits of cloud computing, with the costs spread over fewer users than a public cloud. This option of deployment is more expensive but may offer a higher level of privacy, security and/or policy compliance.

Hybrid cloud is understood as two separate clouds joined together (public, private, internal or external), or a combination of virtualized cloud server instances used together with real physical hardware. By integrating multiple

cloud services, users may be able to ease the transition to public cloud services. A hybrid storage cloud uses a combination of public and private storage clouds. Hybrid storage clouds are often useful to backup functions, allowing data to be replicated to a public cloud.

II. Data Security Challenges

Cloud many challenges among those three main challenges [3] that are closely related to the cloudcharacteristics:

A. *Outsourcing:*

Outsourcing is delegating the responsibility for performing data storageor business functions to a third party [12]. By outsourcing data, users remove the burdenof establishing and maintaining a local storage infrastructure. However, outsourcingalso means that users partially lose control on their data and tasks. Many cloudproviders are not up to the level they should be in order to effectively guarantee trustworthy security architecture. In fact, data may be read, altered or deleted, whenoutsourced. In the sequel, owners have to be aware of these confidentiality, integrityand privacy challenges. They also must worry about the availability of services, theerror recovery of data and the business continuity. Thus, the control loss concern hasbecome one of the root causes of cloud security challenges. Consequently, data andprocess security remains a dominating barrier to the development and widespreaduse of cloud storage. To deal with outsourcing security issues, the cloud providerhas to provide trust and secure data storage. Moreover, outsourced data have tobe protected, controlled and verified to ensure confidentiality, integrity and othersecurity services.

B. *Multi-tenancy:*

Multi-tenancy means that the cloud infrastructure is shared andused by multiple users [13] . As such, in a virtual environment, data belonging to differentusers may be placed on the same physical machine, based on a certain resourceallocation policy. Although multi-tenancy is an essential choice of cloud vendorsdue to its economic efficiency, it provides new vulnerabilities to the cloud platform.That is, malicious users may exploit this co-residence issue to perform flooding attacks[14].

C. *Massive data:*

The scale of data and applications grows exponentially and bringsnew challenges of dynamic data monitoring and security protection, such as imageprocessing and data mining in the cloud context [15]. That is, traditional security mechanismsare insufficient and inefficient, due to heavy computation and communicationoverhead.

As with cloud storage system, there are principalsecurity mechanisms that are highly suggested in cloud storage, namely, confidentiality,integrity and authentication. These properties ensure that users' data are secure and cannot bemodified by unauthorized users. Moreover, data need to be protected when transferredand stored in cloud storage servers.

III. Importance of Security in Cloud Storage

Cloud data storage services bring many challenging issues, considerably due tothe loss of physical control. These challenges have significant influence on the data securityand performances of cloud systems [16].

Data confidentiality is provided in multi-tenant environments, becomesmore challenging and conflicting. This is largely due to the fact that users outsource theirdata on cloud servers, which are controlled and managed by untrusted CloudService Providers (CSPs). It is commonly agreed that data encryption at the client side isa good alternative to mitigate such concerns of data confidentiality [17]. Thus,the client preserves the decrypting keys out of reach of the cloud provider. Nonetheless, thisapproach gives rise to several key management concerns, such as, storing and maintainingkeys' availability at the client side [18]. In addition, the confidentiality preservation becomesmore complicated with flexible data sharing among a group of users. First, it requiresefficient sharing of decrypting keys between different authorized users. The challenge is todefine a smooth group revocation which does not require updating the secret keys of theremaining users,so, the complexity of key management is minimized. Second, theaccess control policies should be flexible and distinguishable among users with differentprivileges to access data. That is, data may be shared by different users or groups, andusers may belong to several groups.

Data integrity is considered as a relevant concern, in cloudenvironments[19]. That is, the responsibility of securely managing outsourced data is splittingacross multiple storage capacities. Such distribution provides resilience against hardware.

Cloud Storage is an evolving paradigm, shifting the computing and storage capabilities to external service providers. Especially due to this loss of direct control on outsourced data, users are reluctant for adopting cloud services [20]. The data security and privacy concerns are quite legitimate, given the latest mediated revelations.

Therefore, several security measures have to be set up, in order to cope with the emerged cloud concerns, namely,

- Outsourcing encrypted data and
- Periodically checking data integrity and availability.
- However, the choice of effective security mechanisms has to take into consideration peripheral challenges.

For example, storing encrypted data yields to a cumbersome key management and access control, and regularly checking huge amounts of data tightens the bandwidth consumption [22].

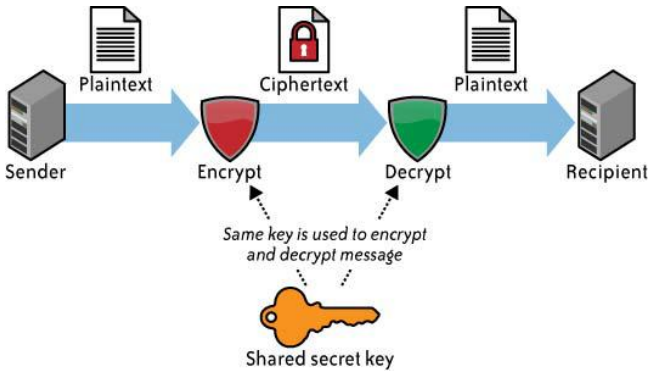

Figure 2. The symmetric cryptosystem [23]

IV. Cryptography in Cloud Storage

Cryptography is a technique applied for encryption and decryption. In the field of cryptography there are several techniques available for encryption/decryption[24]. These techniques can be generally classified into two major groups, i.e. Conventional and public key Cryptography [25]. Conventional cryptography is also referred as symmetric encryption or single key encryption. Same key is used for encryption and decryption. Public key cryptography is referred as asymmetric encryption or public key encryption. Separate keys are used for encryption and decryption. Figure 2 represents the symmetric cryptosystem.The original intelligible message, referred as plaintext, is converted into apparently random ambiguous message, referred as ciphertext. The encryption process consists of an algorithm and a key. The key is a value independent on the specific of the plain text. The algorithm will produce a different output depending on the specific key being used at that time. Changing the key changes the output of the algorithm. Figure 3 represents the asymmetric cryptosystem. It uses two key for encryption and decryption. Each side users have two keys that are public and private key. Sender of the message encrypts the message using receiver public key and upon the receiver uses their private key to decrypt the data. Asymmetric cryptosystem takes time process large amount data. So for Cloud environment, symmetric cryptosystem is more suitable and process large volume of data[23].

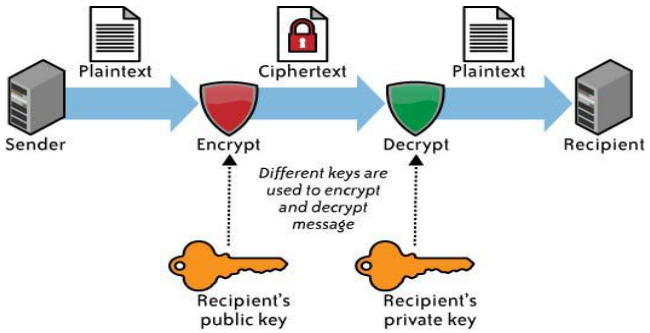

Figure 4. The symmetric cryptosystem [23]

A. *Limitations of Traditional Cryptographic Systems for Cloud Storage:*

Despite traditional cryptographic systems provide strong security guarantees, they maybe inadequate for modern storage systems [3]. In fact, several limitations reduce the accountof these traditional schemes, especially due to the huge amounts of outsourced data.

In cloud storage environments, bandwidth, memory and power consumptions are a big concern,as they impact the availability and performances of delivered services[26]. Consequently,the selection of adequate cryptographic tools for security support is accurate [27] [28].

First, under an untrusted service provider security model, the client generally choosesto encipher data before outsourcing to remote servers. Thus, the usage of traditionalasymmetric algorithms is overly cumbersome for large amounts of data, and computationcapacities at the client side are significantly reduced, even by using elliptic curves.

Second, classical asymmetric algorithms require deploying PKI and certificate managementfunctions for the generation and delivery of certificates to authenticated entities. Inaddition, the periodic downloading of revocation lists by the clients from the CertificationAuthority (CA) is necessary to verify the validity of certificates. Thus, the bandwidthconsumption, and then, availability requirements are deteriorated.

Third, while using symmetric cryptographic schemes to encipher data at the client side,this latter preserves the decrypting keys out of reach of the service provider. However, theconfidentiality provision becomes more complex with flexible data sharing among a groupof users. That is, it requires efficient sharing of decrypting keys between different authorizedusers. The challenge is to define a smooth group revocation which does not requireupdating the secret keys of the remaining group members. Therefore, the complexity ofkey management is minimized.

Finally, as these traditional cryptographic tools are mostly deterministic, they arenot malleable and do not allow operations over encrypted data, such as the search overenciphered texts. Search is a convenient method for retrieving outsourced data informationon remote servers. Hence, several applications, that index data, have emerged to allowquick search, namely, Apple Spotlight and Google Desktop.

Modern cryptography provide much more flexible decryption mechanisms, and explicitlyallow malleability on ciphertexts, namely search over encrypted data, Proofs of DataPossession (PDP) and Proofs of data Retrievability (PoR). These promoting approachesare greatly interesting in a multi-tenant cloud environment.

V. Data Security Attacks in Cloud Storage

Cloud storage is attacked in different ways. The possible attacks in cloud storage are described in this section. Most of the attacks to the cloud networks find their root in the traditional network [29][30][31][32][33][34].

Denial of service: In cloud computing, hacker attack on the server by sending thousands of requests to the server that server is unable to respond to the regular clients in this way server will not work properly. Counter measure for this attack is to reduce the privileges of the user that connected to a server. This will help to reduce the DOS attack.

Side Channel Attack: An attacker could attempt to compromise the cloud by placing a malicious virtual machine in close proximity to a target cloud server and then launching a side channel attack. Side-channel attacks have emerged as a kind of effective security threat targeting system implementation of cryptographic algorithms. Evaluating a cryptographicsystem's resilience to side-channel attacks is therefore important for secure system design

Man in the Middle Attack: This type of attack occurs when the secure socket layer (SSL) is not properly installed when two parties are communicating with each other then there is a possibility that all the data communication between two parties could be hacked by the middle party. Therefore countermeasures are required to be taken to protect the data from the middle attack.

Network Sniffing: When the unencrypted data is send on the cloud through the network then the hacker can sniff the passwords from the data on transit.

Port Scanning: There may be some issues regarding port scanning that could be used by an attacker as Port 80(HTTP) is always open that is used for providing the web services to the user. Other ports such as 21(FTP) etc are not opened all the time it will open when needed therefore ports should be secured by encrypted until and unless the server software is configured properly. Counter measure for this attack is that firewall is used to secure the data from port attacks.

Insider Attack:Employee, entrepreneur and associateswhich are still or former attended who can or could accessthe whole information system with privileged authority aredefined as *insider*. Insider attacks are organized and runby these individuals to harm or temper knowledge aboutconsumers or providers and include every kind of attackswhich can be executed from inside.

SQL Injection Attack: SQL injection attacks are the attacks where a hackers uses the special characters to return the data for example in SQL scripting the query end up with where clause that may be modified by adding more information in it.

Cross Site Scripting: It is a type of attack in which user enters the correct URL of a website and hacker on the other site redirects the user to its own website and gain access to its credentials.

Security threats are usually more common with data protection, browser, and web service.The data stored on the cloud can be easily accessed by the hackers if proper security is not provided to the data. Various methods are elaborated in the literature to overcome these issues some of them are,

XML Signature Element Wrappings: It is used to defend a component name, attribute and value from unauthorized party but unable to protect the position in the documents, the attacker targets the component by operating the SOAP messages and putting anything (malicious modification) that attacker like, so it is difficult for the user to protect his documents.

Browser Security: The browser is expected to make use of SSL (secure socket layer) to encrypt the credentials to authenticate the user prior the data is transmitted over the network. SSL support point to point communication means if there is third party, intermediary host can decrypt the data. If hacker installs sniffing packages on intermediary host, the attacker may get the credentials of the user and use in these credentials in the cloud system as a valid user.

Data Protection: Data protection in cloud computing is very important factor it could be complicated for the cloud customer to efficiently check the behavior of the cloud supplier and as a result he is confident that data is handled in a legal way, but it does not like that this problem is intensify in case of various transformation of data. Counter measure for this attack is that a consumer of cloud computing should check data handle and established whether it is handled lawfully or not.

Incomplete Data Deletion: Incomplete data deletion is very risky in cloud computing environment. It does not remove completed data because replicas of data are placed in other servers. Counter measure is that Virtualized private networks should use for securing the data and used the query that will remove the complete data from the main servers along with its replicas.

VI. Security Mechanisms

There are five security mechanisms namely confidentiality, integrity, availability, identification and privacy [35]. When dealing with clouds, confidentiality implies that client's data and computation tasks have to be kept secret from cloud providers and other unauthorized users. Confidentiality remains as one of the greatest concerns with regards to clouds, largely due to the loss of physical control. Similar to confidentiality, the notion of integrity in clouds concerns both data and process integrity [3].

Confidentiality is needed when the message sent or stored in the cloud contains sensitive data which should not be read by others. Hence it must not be sent in a comprehensible format. A loss of confidentiality is the unauthorized disclosure of information. Confidentiality relates to security and encryption techniques can be obtained by encrypting messages so that only intended recipients have access to read them.

Data integrity implies that data should be honestly stored on cloud servers, and any violations (e.g. data are lost, altered or compromised) have to be detected.Computation integrity implies that programs are executed without being distorted by malware, cloud providers or other malicious users, and that any incorrect computation has to be detected.

Availability is one of the most critical information security requirements in Cloud computing because it is a key decision factor when deciding among private, public or hybrid cloud vendors as well as in the delivery models. The service level agreement is the most important document which highlights the trepidation of availability in cloud services and resources between the cloud provider and client[8].

Authentication is the process of verifying a user's or other entity's identity. This is typically done to permit someone or something to perform a task. A strong authentication system ensures that the authenticators and messages of the actual authentication protocol are not exchanged in a manner that makes them vulnerable to being hijacked by an intermediate

malicious node or person. That is, the information used to generate a proof of identity should not be exposed to anyone other than the person or machine it is intended for.

Privacy is yet another critical concern with regards to cloud environments, due to the fact that clients' data reside among remote distributed servers, maintained by potentially untrusted cloud providers[36]. Therefore, there are potential risks that the confidential data or personal information are disclosed to unauthorized entities. Obviously, in order to guarantee privacy preservation, confidentiality and integrity become essential, ensuring that data and computation are kept secret and uncorrupted. Contrary, accountability may undermine privacy since these two securities attributes usually conflict. That is, accountability implies the capability to of identifying a party, with undeniable evidence. In fact, a fine-grained identity may be employed to identify a specific entity or even a maliciousprogram.

VII. CONCLUSION

Cloud gains more attention from the IT Enterprises, because of its advantages. Cloud supports on-demand computing. It reduces the cost of installing and maintaining storage servers. Though the cloud storage provides many benefits and advantages to cloud users, it has many security related issues. Cryptography is one of the techniques suitable for data security. Data are accessed from either in rest or in transit. To protect the data in transit, it needs an efficient security protocol. To protect the data in rest, cryptography techniques are used. Symmetric cryptosystem is preferred for cloud storage. Symmetric encryption processes large volume of data without any latency. Hence, in future, it is necessary to develop security mechanism and cryptography technique to protect the outsourced data in public cloud storage.

REFERENCE

[1] Katarina Stanoevska-Slabeva, Thomas Wozniak, Cloud Basics – An Introduction to Cloud Computing, Grid and Cloud Computing: A Business Perspective on Technology and Applications, Springer-Verlag Berlin Heidelberg, 2010, pp. 47-61.

[2] Tyrone Grandison, E Michael Maximilien, Sean Thorpe, Alfredo Alba, Towards a Formal Definition of a Computing Cloud, IEEE 6th World Congress on Services, pp. 191-192.

[3] NesrineKaaniche,Cloud data storage security based on cryptographic mechanisms,IT Telecommunications and Electronics of Paris, 2014, pp. 17-41

[4] Peter Mell and Tim Grance, The NIST Definition of Cloud Computing, Technical Report-800-145, Version 15, National Institute of Standards & Technology, Gaithersburg, MD, United States, 2011.

[5] Zhang Q, Lu Cheng, and RaoufBoutaba, Cloud Computing: State-of-the-Art and Research Challenges, Springer Journal of Internet Service Application, Volume 1, Issue 1, 2010, pp. 7-18.

[6] Longji Tang, Jing Dong, Yajing Zhao, Liang-Jie Zhang, Enterprise Cloud Service Architecture, IEEE 3rd International Conference on Cloud Computing, pp. 27-34.

[8] Ramgovind S, Eloff MM and Smith E, The Management of Security in Cloud Computing, Proceedings of IEEE InternationalConference Information Security for South Africa, 2010, pp. 1-7.

[7] Gens F, New IDC IT Cloud Services Survey: Top Benefits and Challenges, 2009,IDC eXchange, viewed on February 2013, from <http://blogs.idc.com/ie/?p=730>.

[9] M. Malathi, Cloud Computing Concepts, IEEE, pp. 236-239.

[10] IlangoSriram, Ali Khajehhosseini, Research Agenda in Cloud Technologies, Proceedings of ACM Symposium on Cloud Computing, 2010, pp. 1-11.

[11] Chunye Gong, Jie Liu, Qiang Zhang, Haitao Chen and Henghu Gong, The Characteristics of Cloud Computing, IEEE International Conference on Parallel Processing Workshops, 2010, pp. 275-279.

[12] Ammar Khalid, Husnainmujtaba, Data Processing Issue in Cloud Computing, IEEE Second International Conference on Machine Vision, pp. 301-304.

[13] FarzadSabahi, Cloud Computing Security Threats and Responses, IEEE, pp. 245-249

[14] K. Zunnurhain, Fapa: A Model to Prevent Flooding Attacks in Clouds. In Proceedings of the 50th Annual Southeast Regional Conference, ACM, 2012, pp. 395–396.

[15] David Teneyuca, Internet cloud security: The Illusion of Inclusion in Formation Security, Technical Report, Elsevier, 2011, pp. 102-107.

[16] Kamal Dahbur, Bassil Mohammad, AhmadBisherTarakji,A Survey of Risks, Threats and Vulnerabilities in Cloud Computing, ISWSA'11, Amman, Jordan, 2011, pp. 1-6.

[17] Sanjay Ram M, Vijayaraj A**,** Analysis of the Characteristics and Trusted Security of Cloud Computing, International Journal on Cloud Computing: Services and Architecture,Volume 1, Issue 3, 2011, pp. 61-69.

[18] Dr. L. Arockiam, S. Monikandan, AROMO Security Framework to Enhance Security of Data in Public Cloud,International Journal of Applied Engineering Research,Volume 10, Issue 9, 2015, pp. 6740-6746.

[19] ChiragModi, Dhiren Patel, BhaveshBorisaniya, Avi Patel, MuttukrishnanRajarajan, A Survey on Security Issues and Solutions at Different Layers of Cloud Computing, Springer ScienceBusiness Media New York, Journal of Super Computer, 2013, pp. 1-32.

[20] YuanqiuLuo, Frank Effenberger, and Meng Sui, Cloud Computing Provisioning over Passive Optical Networks, IEEE International Conference on Communications in China: Optical Networks and Systems,2012, pp. 255-259.

[21] Diogo A. B. Fernandes, Liliana F. B. Soares, João V. Gomes, Mário M. Freire, Pedro R. M. Inácio, Security issues in cloud environments: a survey, International Journal Information Security, Springer-Verlag Berlin Heidelberg, 2013, pp. 1-58.

[22] Farhan Bashir Shaikh, SajjadHaider, Security Threats in Cloud Computing, IEEE International Conference on Internet Technology and Secured Transactions, 2011, pp.214-219.

[23] Tim Mather, SubraKumaraswamy, and ShahedLatif, Cloud Security and Privacy, O"Reilly Media, Inc, 2009, pp 61-71,.

[24] Dr. L. Arockiam, S. Monikandan, Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm, International Journal of Advanced Research in Computer and Communication Engineering, Volume 2, Issue 8, 2013, pp. 3064-3070.

[25] William Stallings, Cryptography and Network Security: Principles & Practices, Fifth edition, Prentice Hall, ISBN-13: 978- 0136097044, 2010.

[26] Dr. L. Arockiam, S. Monikandan, G.Parthasarathy, Cloud Computing: A Survey, International Journal of Internet Computing, and ISSN No: 2231 – 6965, Volume-1, Issue-2, 2011, pp. 26-33.

[27] DimiterVelev and PlamenaZlateva, Cloud Infrastructure Security, International Federation for Information Processing, LNCS 6555, Springer, 2011, pp. 140–148.

[28] HuagloryTianfield, Security Issues In Cloud Computing, IEEE International Conference on Systems, Man, and Cybernetics, 2012, pp. 1082-1089.

[29] S. Vanimounika, Preetiparwekar, Survey on cloud data storage security techniques, Indian Journal of Research in Pharmacy and Biotechnology, Special Issue 1, 2014, pp. 95-98.

[30] Ajey Singh, Dr. ManeeshShrivastava,Overview of Attacks on Cloud Computing, International Journal of Engineering and Innovative Technology, Volume 1, Issue 4, 2012, pp. 321-323.

[31] Adrian Duncan, Sadie Creese, Michael Goldsmith,Insider Attacks in Cloud Computing, IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012, pp. 857-862.

[32] D. M. Cappelli and R. F. Trzeciak, "Best practices for mitigatinginsider threat: Lessons learned from 250 cases," [Online]. July 2013,Available:http://www.cert.org/archive/pdf/RSA-CERTInsiderThreat.pdf.

[33] C. 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, Volume 36, Issue. 1, 2013, pp.42–57.

[34] U. Oktay and O.K. Sahingoz, Attack Types and Intrusion Detection Systems in Cloud Computing, International Information Security & Cryptology Conference, 2013, pp. 71-76

[35] Dr. L. Arockiam S. Monikandan, Efficient Cloud Storage Confidentiality to EnsureData Security, IEEEInternational Conference on Computer Communication and Informatics, 2014, pp. 355-359.

[36] Miao Zhou a, YiMua,n, WillySusilo a, JunYan b, LijuDonga,c, Privacy enhanced data outsourcing in the cloud, Journal of Network and Computer Applications, Elsevier, Volume 35, 2012, pp. 1367–1373.