CLOUD SECURITY ISSUES: A SURVEY

Akshay Sharda
Department of Computer Engineering & Technology
Guru Nanak Dev University
Amritsar, Punjab, India

Amit Chhabra
Department of Computer Engineering & Technology
Guru Nanak Dev University
Amritsar, Punjab, India

***Abstract*- In today's world consumers are dependent upon cloud computing to get various services. Now a day big companies like Amazon, Google, Microsoft, and IBM etc. are using this technology to maintain and upgrade their position and to enhance their services for a large number of users. However, with the fast development of cloud computing technology issues related with security are offering great challenges. Security concerns like security threat and attack are disaster for both service provider and service consumer. This paper deals with cloud computing architectural principles, cloud computing security threats and cloud computing security attacks with their mitigation techniques.**

***Keywords*: *Cloud Computing, Security Requirements, Security Threats, Security Attacks, Mitigation Techniques*.**

1. INTRODUCTION

In today's era cloud computing becomes the hottest topic due to its ability to reduce the cost associated with computing. Cloud computing provides the on demand services like storage, servers, resources etc. to the users without physically acquiring them and the payment is according to pay per use. Since cloud provides the storage, reduces the managing cost and time for organization to the user but security and confidentiality becomes the one of the biggest obstacle in front of us. The major problem with cloud environment is, the number of user is uploading their data on cloud storage so sometimes due to lack of security there may be chances of loss of confidentiality. To overcome these obstacles a third party is required to prevent data, data encryption, and integrity and control unauthorized access for data storage to the cloud.

With the rapid development of hardware and software cloud computing brings the revolution in the business industry[8]. It provides resources like computational power, storage, computation platform and applications to user on demand through internet. Some of the cloud providers are Amazon, IBM, Google, Salesforce, Microsoft etc. Cloud computing features included resource sharing, multi-tenancy, remote data storage etc. but it challenges the security system to secure, protect and process the data which is the property of the individual, enterprises and governments. [24] Even though, to control the infrastructure of clouds there is no need of knowledge or expertise, it is abstract to the user. Cloud computing providers deploy common online business applications which are accessed from servers through web browser. Data security is the biggest issue in cloud computing and it is not easy to resolve it.

1.1 Security issues in cloud Computing

In cloud environment usual data transmission occurs between client and server using third party. So the confidentiality of your data becomes the primary problem [3]. The system which interconnects a cloud must be secure and the migration from physical machine to virtual machine must be safe. Information security [28] includes encoding the information and additionally guaranteeing that suitable strategies are implemented for information sharing. Cloud security isn't to be mistaken for "cloud-based" security benefit over the conventional danger. This security administration can be upgraded with the distributed computing, ensuring against DDOS, Trojan, Virus and Spam and so on more viably [32] than any other time in recent memory.

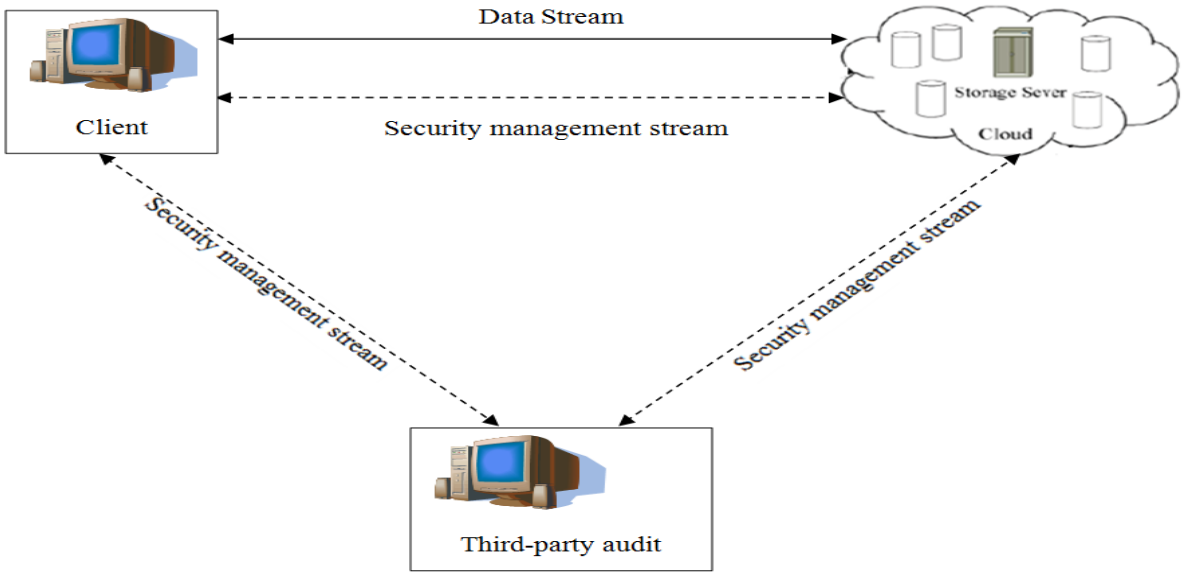

Figure 1: data storage structure of cloud computing

However, the qualities of distributed storage make clients information looked with numerous security dangers, incorporates: (1) the conventional security district parcel is invalid. On account of the distributed storage benefit must be adaptable, security limits and assurance hardware can't be unmistakably characterized, which builds some trouble for the usage of particular assurance measures; (2) the distributed [22] storage transmits information through the system. The benefit interferences, information devastation, data stolen furthermore, altered caused by the noxious assaults in the organize represent a serious test to the security of information correspondences, get to confirmation and classification; (3) from the client's view [20], the distributed storage of information makes distributed computing specialist co-op gets the information get to control, and the client's information is looked with protection security dangers. Individuals stress over that the touchy individual information will be exposure, abuse or missing by putting the information in cloud condition [9]. To tackle the above issues, as of late, scientists made a parcel of research work in the information security to control systems, information respectability, confirmation, [1] cipher text to recover and information encryption system of cloud figuring condition.

There are lots of security issues with cloud computing because of technologies utilization including networks, operating systems, databases, resource scheduling, virtualization [16], load balancing, transaction management, memory management and concurrency control. For example, the network should be secure on cloud so that migration of VM to PM should be secure [5]. Data security not only involves encrypting the data but also gives surety of appropriate policies. Cloud computing suffers from some various security concerns which are given below.

- Server & application access
- Transmission of data
- Secure VM
- Secure Network
- Security of Data
- Privacy of data
- Correctness of Data
- Location of data
- Availability of data
- Segregation of Data

1.2 Cloud Security Challenges

Some of the cloud security challenges that come in front of users are given below:

a. Authentication: The data on the internet is available to all the unauthorized users. Therefore the confidentiality of the data can be lost.

b. Access Control: To give access to only legalized users some control policies are used. [15] These services must be adjustable, well planned, and their allocation is overseeing conveniently.

c. Policy Integration: There are many cloud providers they use their own policies and approaches. Some of them are Amazon, Google who provides services to end users.

d. Service Management: In this different cloud providers such as Amazon, Google [19], comprise together to provide services to meet their customers need.

e. Trust Management: The trust management approach must be developed so that trust remains between both parties such as user and provide.

Cloud security is hampered by the threats which are common in cloud system. These threats are mitigated using the techniques described through the table 1.

Table 1: Types of threats and mitigation strategies.

Type of Threats	Mitigation technique
VM level Threat	IDS and IPS
Abuse and nefarious	Credit card fraud monitoring and coordination.
Loss Of Governance	No proper strategy available for handling this attack
Xml Signature Element Wrapping	Utilization of digital certificate
Browser Security	XML encryption and SOAP encryption
Cloud Malware Injection Attack	Authenticity check
Flooding Attacks	Intrusion detection system is used
Isolation Failure	Authentication and access control
Data Loss Or Leakage	Encrypting and protecting integrity of data
Account Or Service Hijacking	Multifactor authentication techniques

In addition threats could lead to security problems if not tackled at early stage [21]. The security problems could hamper the overall working of the cloud. User data may be corrupted due to the application of attacks. Various attacks along with mitigation strategies are listed in the table 2.

Table 2: Attacks and mitigation strategies

Type of attack	Mitigation technique	Advantage	Disadvantage
Denial Of Services	Clustering based mechanism	Reduce functionality of hijackers	Time consumed more
Authentication Attacks	Access Control	Unauthorized access control	Only utilized for frequent targets
Man in the middle attack	Block Level Parity attack	Gives better prevention	Space is more consumed
DNS attack	IP address validation	Had better performance	Rerouting processing are inadequate
Network stiffing	Encryption algorithms is used	Data is secured	Much Complex
Cross site Scripting	Validating Input	Sensitive data can be secured	Violation of user credential may occur
Cookie Poisoning	Regular cookie cleanup	Removed unauthorized accessed	Must be improved for large data
Distributed Denial of service	Deadline oriented techniques	Early detection of intruder	Used more space
SQL Injection Attack	Special character elimination using buffer allocation	Eliminate intruder	More information can not be added
Side Channel Attack	Nearest Neighbor mechanism	Secured channel using nearest neighbor	Server proxy can be hacked

To optimize better results we will review some paper and find the better results to remove the security barriers. Rest of the paper is organized as follows: Section 1 provide the security concerns in cloud, section 2 provide the literature survey of existing techniques to derive the best possible technique for future enhancements, section 3 present the comparison table, section 4 gives conclusion and future scope.

2. LITERATURE REVIEW

The security challenges in cloud are reported [30]. The security in terms of passwords is established. The offloading is considered. the considered technique utilizes more resources as compared to the existing system. The proposed technique is more expensive as compared to the previous techniques already present.

The encryption mechanism is considered in the prescribed paper [7]. The prescribed paper considered the encryption mechanism which is considered in this scheme is RSA. It is the public key encryption strategy which is used in order to transfer the encrypted data towards the destination. At the receiver end encrypted data is collected and again cipher text is created.

The decoy technique is used in order to enhance the security associated [23] with the cloud. The cloud security mechanism which will distract the malicious user is considered in this case. The cloud security mechanism considered is more secure as compared to previous techniques specified.

The security issues in cloud computing [12] using big data are considered in this case. Users of the data will be of varying intensions so malicious user handling is suggested in the proposed strategy.

The adaptive offloading in WAN is described in [33]. the WAN is wide area network. The data will be migrated over the geographically large area. The WAN will have wireless as well as wired mechanism associated with them. The rate at which offloading is being performed will depend upon the method which is used for offloading. The tool which is used for offloading will use services of cloud computing. The cloud computing security mechanisms are also suggested since cloud is accessible to wide variety of users and some of them can be malicious in nature. The malicious node and data handling mechanism are suggested in this case.

The edge network is considered in [6]. The edge networks will help in transmitting the information by the use of WAN network. This means that boundaries between the large distance is not considered. The VM migration is offline in nature. Which means that the machine which is being migrated is idle during the operation? Hence resources will be wasted in this case.

Offloading in terms of cost and energy is analysed in [25]. The energy will be consumed when the offloading takes place. The energy consumed will depend upon the amount of data which is migrated. The migrated data will go to the cloud. The cost will be encountered on the basis of amount of data which is being used.

The offloading will be performed on the consideration of IaaS [14]. The internet as a service is considered in this case. The internet will be used in order to provide the offloading strategies. The internet has number of resources associated with it. The resources can be used offline or online. The resources present will help in Offloading.

The security assurance is considered in [11]. The cloud is accessible by legion of users. The intension of the user will be uncertain. The malicious nodes can corrupt the data and hence should be avoided from within the network. The nodes can be checked against the malicious entry using certification authority.

The papers used in this literature are given as under:

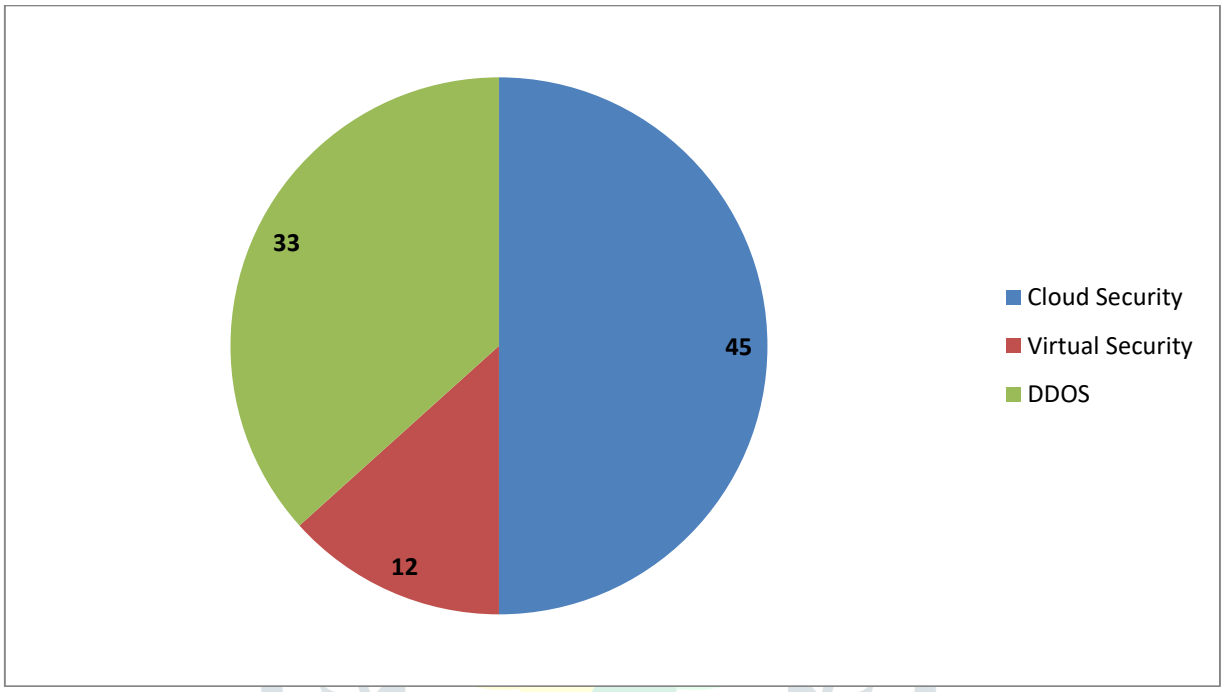

Figure 2: Different techniques of securities used in cloud computing

3. COMPARISON OF TECHNIQUES USED

Cloud computing is the utmost common part used mechanism in order to cache the data by the machines which does not have sufficient storage capabilities. The cloud computing will be the mechanism which allow machines to cache the data above the storage capabilities of the particular machine. As more and more users come in contact with the cloud, the security of cloud is at stakes. The data storage and its security is the area in which legions of work have already been done and legions of work is craved to be done. The proposed paper conducts a review of the assorted mechanisms which deals with the security of data within the cloud. Also data storage is a concern in the proposed paper. So deduplication is also considered in this case. The comparison between the techniques used is as follows

COMPARISON TABLE

Author	Parameters / Method Used	Encryption technique	Complexity	Storage	Security Strength	Performance enhanced
R. Chen, Y. Mu, G. Yang, and F. Guo[8]	BL-MLE	RSA Technique	High, In terms of iterations required	Repeated bits present hence high storage requirements	Least since no security slandered are followed	Better Handling of redundancy

R. Miguel[24]	Homomorphic Deduplication	Homomorphic Encryption	High, in terms of length of code	Bit level duplication showing high storage	Key is used hence medium security is present	Better data Handling
G. Zhu, X. Zhang, L. Wang, Y. Zhu, and X. Dong[3]	Intelligent Back Up system	RSA Technique	Length of code ensure complexity	Multiple copies of data ensures high storage	No security slandered established	Back is improved
H. Nagarajaiah, S. Upadhyaya, and V. Gopal[28]	Embedded Processor Dedupliation	AES Algo	Calculations in AES makes it complex	Repeated data elimination techniques ensures less storage requirements	Private and public keys ensure high security	Security is improved
S. C. Satapathy, P. S. Avadhani, S. K. Udgata, and S. Lakshminarayana[32]	Critical Infratructure is considered	None	Length of code in terms of LOC is less	Redundancy is handled hence space requirement is low	No security standards are used	Infrastructure capabilities are considered
J. J. Park, A. Zomaya, H.-Y. Jeong, and M. Obaidat[22]	Frontier Technique	None	Multiple algorithms ensure complexity	Length of code required maximum storage	Security standards ensure high security	A new Technique where storage compression is considered
K. He, C. Huang, H. Zhou, J. Shi, X. Wang, and F. Dan[20]	Public auditing technique	RSA algorithm	Complexity in terms of calculations is high	Storage requirements is high since LOG is maintained	Security Mechanisms are used	Public auditing for encrypted data with client-side deduplication in cloud storage
X. Li, J. Li, and F. Huang[9]	Fuzzy deduplication	Fuzzy Algorithm	Low complexity since logical values in terms of 0 and 1 is used	Low storage requirements since result is stored in terms of Boolean values	Fuzzy storage has least security associated with it	A secure cloud storage system supporting privacy-preserving fuzzy deduplication
N. Christin and R. Safavi-Naini, Eds[5]	Financial cryptography	Cost Based Encryption	Complexity in terms of calculations is high	Redundancy is handled hence space requirement is low	Security Mechanisms are used	A cost is a factor on which deduplication is considered
F. Rashid, A. Miri, and I. Woungang[15]	Secure Enterprise Data Deduplication	AES Algo	Complexity in terms of calculations is high	Redundancy is handled hence space requirement is low	Security Mechanisms are used	High security in data deduplication
W. K. Ng, Y. Wen, and H. Zhu[29]	Private cloud data deduplication	None	Length of code in terms of LOC is less	Storage requirements are high in terms of multiple data	Security is low since no security slandered s are used	Only private cloud is considered

C. Wang, Q. Wang, K. Ren, and W. J. Lou[17]	Ensuring Data Storage Security in Cloud Computing,	AES Encryption	Complexity in terms of calculations is high	Redundancy is handled hence space requirement is low	Security Mechanisms are used	Data security is high
Y. Yuan, X. Wu, and Y. Lu, Eds[4]	*Trustworthy Computing and Services*	None	None	None	None	Trust parameter is considered
C.-I. Fan, S.-Y. Huang, and W.-C. Hsu[26]	Hybrid data deduplication in cloud environment	Cost based Encryption	Complexity in terms of calculations is high	Redundancy is handled hence space requirement is low	Security based standards are used	Hybrid deduplication is considered
F. Rashid, A. Miri, and I. Woungang[10]	A secure data deduplication framework for cloud environments	Encryption based on cost	Complexity is high in terms of LOC	Storage requirements are high since code is complex	Data security mechanism are required	A security is provided
X. Zhang and J. Zhang[31]	Data Deduplication Cluster Based on Similarity-Locality Approach	Cluster based encryption is used	Complexity is high since cluster of information is present	High storage requirements in terms of clusters	Encryption standards ensure high	Cluster based approch is used
P. Puzio, R. Molva, M. Onen, and S. Loureiro[2]	ClouDedup: Secure Deduplication with Encrypted Data for Cloud Storage	Encryption based Secure deduplication	Complexity is high in terms of LOC	Storage requirements are high since code is complex	Data security mechanism are required	Secure Deduplication is used
W. Leesakul, P. Townend, and J. Xu[27]	Dynamic Data Deduplication in Cloud Storage	AES Encryption	Complexity in terms of calculations is high	Redundancy is handled hence space requirement is low	Security Mechanisms are used	Dynamic deduplication is used
T. Johansson and P. Q. Nguyen, Eds[18]	Cryptography advancement is used	Cipher Text is used	Low complexity in terms of lease code utilized	Redundancy is handled hence low storage requirements	Security Mechanisms are used	Cryptography is used
V. Inukollu, S. Arsi, and S. Ravuri[13]	Security Issues Associated With Big Data in Cloud Computing	Encryption based on DES	Complexity in terms of calculations is high	Redundancy is not handled hence storage requirement is high	Security mechanism prevent malicious attacks	Fast Encryption is used

4. CONCLUSION

Cloud computing is a very fascinating technology which is cost effective and provide extraordinary measurable services that allow enterprises to monetize their business, raise their level of productivity and profit while saving their costs. Cloud computing has complex and dynamic nature so it demands much more than traditional security. A lot of research is being conducted on cloud security to resolve its issues but because of the rapid growth in this technology the researchers and security engineers have been unable to provide competitive solutions in accordance with the rapidly growing problems encountered in this area. This survey summarizes many of the security threats and security attacks with their mitigation techniques and also categorizes them in terms of the cloud services they affect and the network layers where they reside.

REFERENCES

[1] Behl, A. 2011. "Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation," in World Congress on Information and Communication Technologies (WICT), Mumbai, India.

[2] Bhadauria Rohit, S. S. 2012 "Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques," International Journal of Computer Applications, 47(18).

[3] Bones, N. T. T. G. M. 2011. "Cloud Computing Security Issues and Challenges," International Journal of Computer Networks (IJCN), 3(5).

[4] Char Sample, D. K. 2016. "SearchCloudSecurity," [Online]. Available: http://searchcloudsecurity.techtarget.com/tip/Cloud-computingsecurity-Routing-and-DNS-security-threats. [Accessed Oct 2016].

[5] Cloud Security Alliance, 2010. "CSA: Top Threats to Cloud Computing".

[6] Darsena, D. Gelli, G. Manzalini, A. Melito, F. and Verde, F. "Live migration of virtual machines among edge networks viaWAN links" : 1–10.

[7] Date, P. April 2014. "Encryption in the Cloud" : 1547–1551.

[8] Dimitrios, Z. and Dimitrios , L. 2012. "Addressing cloud computing security issues," *Future Generation Computer Systems*, 28(3): 583-592.

[9] ENISA, 2009. "Cloud Computing-ENISA-Benefits, risks, and recommendations for information security".

[10] Freier, P. K. A. 2017 "Netscape Communications," August 2011. [Online]. Available: https://tools.ietf.org/pdf/rfc6101.pdf. [Accessed March 2017].

[11] Hashizume, K. Rosado, D. G. Fernández-Medina, E. and Fernandez, E. B. 2013. "An analysis of security issues for cloud computing," J. Internet Serv. Appl. 4(1) : 5.

[12] Inukollu, V. Arsi ,S. and Ravuri, S. 2014. "Security Issues Associated With Big Data in Cloud Computing," Airccse.Org, 6(3) : 45–56.

[13] Jeng Albert B., C.-C. T. D.-F. T. J.-C. W. 2010. "A Study of CAPTCHA and Its Application to User Authentication," in International Conference on Computational Collective Intelligence.

[14] Katsipoulakis, N. R. Tsakalozos, K. and Delis, A. 2013. "Adaptive Live VM Migration in Share-Nothing IaaS-Clouds with LiveFS," in 2013 IEEE 5th International Conference on Cloud Computing Technology and Science, 2 : 293–298.

[15] Liu, Anyi. Y. Y. D. W. 2009. "SQLProb: A Proxy-based Architecture towards Preventing," in Proceedings of the 2009 ACM Symposium on Applied Computing.

[16] Luo Shengmei, Z. L. X. C. Z. Y. J. C. 2011. "Virtualization security for cloud computing services," in International Conference on Cloud and Service Computing.

[17] Louw, Mike Ter V. V. May 2009. "BluePrint: Robust Prevention of CrossSite scripting attacks for existing browsers," 30th IEEE Symposium on Security, :331-346.

[18] McIntosh Michael, P. A. 2005. "XML Signature Element Wrapping Attacks and Countermeasures," in Proceedings of the 2005 workshop on Secure web services, Fairfax, VA, USA.

[19] Meiko Jensen, J. S. N. G. L. L. I. 2009. "On Technical Security Issues in Cloud Computing," in IEEE International Conference on Cloud Computing, Bangalore, India.

[20] Minqi Zhou, R. Z. W. X. W. Q. A. Z. 2010. "Security and Privacy in Cloud Computing: A Survey," in Semantics Knowledge and Grid (SKG), 2010.

[21] Modi, C. P. D. B. B. e. a. February 2013. "A survey on security issues and solutions at different layers of Cloud computing," The Journal of Supercomputing, 63(2) : 561-592.

[22] Ramgovind, M. M. E. E. S. S 2010. "The Management of Security in Cloud Computing," in Information Security for South Africa (ISSA).

[23] Science, C. and Studies, M. 2014. “Securing user data on cloud using Fog computing and Decoy technique,” 7782 : 104-110.

[24] Shuai Zhang, S. Z. X. C. X. H. 2010. "Cloud Computing Research and Development Trend," in Second International Conference on Future Networks, Sanya, Hainan, China.

[25] Strunk, A. and Dargie, W. 2013. “Does Live Migration of Virtual Machines Cost Energy?,” in 2013 IEEE 27th International Conference on Advanced Information Networking and Applications (AINA) : 514–521.

[26] Suranjith Ariyapperuma, C. J. M. 2007. "Security vulnerabilities in DNS and DNSSEC," in The Second International Conference on Availability, Reliability, and Security, Vienna, Austria.

[27] Trabelsi Zouheir, H. R. K. K. 2004. "Malicious Sniffing System Detection," Proceedings of the 2004 International Symposium on Applications and the Internet (SAINT'04), : 201-207.

[28] Vaquero, M. Luis M.L. L. R.-M. J. C. A. "A Break in the Clouds: Towards a Cloud Definition," ACM SIGCOMM, 39(1): 50-55.

[29] Vogt, F. N. N. J. E. K. C. K. a. G. V. P. 2007. "Cross-Site Scripting Prevention with Dynamic Data Tainting and Static Analysis," in Proceedings of the Network and Distributed System Security Symposium (NDSS’07).

[30] Wang, Q. Wang, C. Ren, K. Lou, W. and Li, J. May 2011, “Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing,” IEEE Trans. Parallel Distrib. Syst., 22(5) : 847–859.

[31] Yow, R. L. a. K. C. "Mitigating DDoS Attacks with Transparent and Intelligent Fast-Flux Swarm Network," IEEE Network, 25(4) : 28-33.

[32] Zhang, Q. C. L. &. B. R. 2010. "Cloud computing: State-of-the-art and research challenges," Journal of Internet Services and Applications, 1(1): 7-18.

[33] Zhang, W. Lam, K. T. and Wang, C. L. 2014. “Adaptive Live VM Migration over a WAN: Modeling and Implementation,” in 2014 IEEE 7th International Conference on Cloud Computing : 368–375.