EasyChair Preprint

№ 339

Comparative Analysis of Security Challenges of Cloud Computing Environment- A Survey

Sakshi Kapoor, S.N Panda and Naveen Kumar

July 14, 2018

Comparative Analysis of Security Challenges of Cloud Computing Environment- A Survey

[1]Sakshi Kapoor, [2]S.N.Panda, [3]Naveen Kumar
[1,2]Department of Computer Science and Engineering,
Chitkara University Institute of Engineering and Technology,
Chitkara University, Punjab, 140401, India
[3]Department of Computer Applications,
Chitkara University Institute of Engineering and Technology,
Chitkara University, Punjab, 140401, India

***Abstract*— Cloud computing has now become one of the popular computing models to execute the applications which are computationally intensive and that too in a pay-as-you-go manner. Cloud based applications are in great demand now-a-days and because of continuous and ever-increasing demand, efficient resource allocation as per the user request is very difficult task for service providers to accomplish. Despite the fact that cloud has many advantages for the associations in achieving more and paying less, it also possess some security threats to the private data stored in the cloud. Proper planning of security dangers, vulnerabilities and threats are required in order to implement cloud computing successfully. In this paper, there is an overview of cloud computing followed by different security challenges related to cloud service models.**

I. INTRODUCTION

Cloud computing is a kind of Internet computing where gathering of clouds is considered as web. This way cloud computing is proved to be beneficial for the general public as well as organizations for providing innovation empowered services [1]. Cloud computing empowers advantageous and on-request access to a common pool of configurable computing assets that can be quickly provisioned and discharged with insignificant management efforts. One can view cloud computing from two alternate perspectives: one is cloud application and the other is cloud foundation as building hinder for cloud application. At present the adoption of cloud computing among organizations increases with the goal that they can cut capital consumption, endeavors and control working expenses, which triggers forceful development for cloud appropriation in the business [2].

Cloud computing has numerous potential points of interest on comparision with the traditional IT models. However, when seen from the customer's point of view, security concerns becomes major problem in the adoption of cloud computing. A review from IDCI in 2009 declared that 74% IT chiefs and CIOs prevents them from utilizing cloud due to the security issues. According to Garter in 2009, over 70% CTOs declared information security as well as protection concerns as the reasons for not using cloud services [3]. Cloud computing presents a level of abstraction between the proprietor of the data being stored and processed and physical foundation. The clients of cloud are concealed from hardware and software that backings their computations [4].

The cloud suppliers have numerous services to offer including Infrastructure as a Service or IaaS, Platform as a Service or PaaS, and Software as a Service or SaaS. SAAS is accessible to the cloud clients through web, controlled by cloud service provider and utilized by organizations [5]. It is accessible to clients through web. PAAS services are utilized by the engineers for creating Websites without the need for introducing any software on the framework, and can be executed with no authoritative expertise [6][7]. The maintainance and operation of IaaS services are done by cloud service providers that help different activities like hardware, networking and systems administration [3].

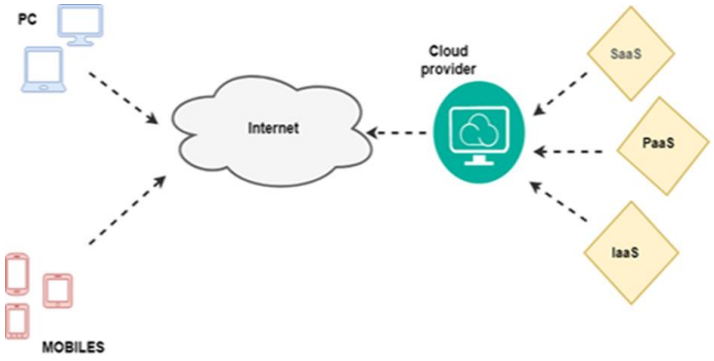

Figure.1 Cloud Framework.

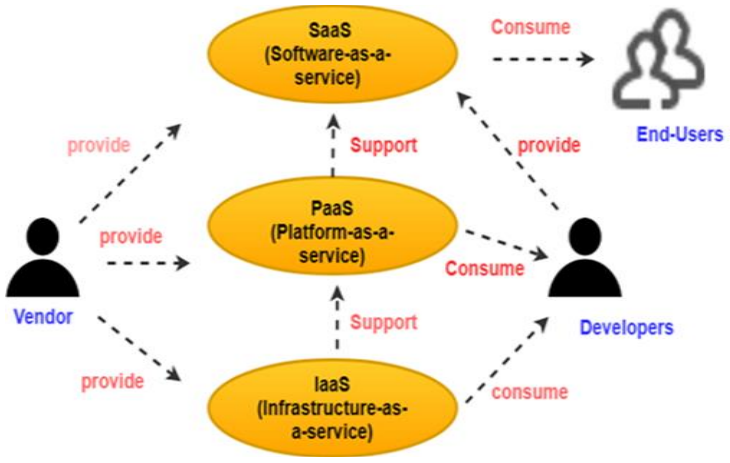

Figure.2 Service models of Cloud

NIST(2009) [3] listed different cloud computing models: private cloud, open or public cloud and hybrid cloud. Public or Open cloud can be utilized in open or in public and is handled by cloud service providers or CSP's, private cloud is the property of an organization, and hybrid cloud combines the features of both open as well as private cloud [8]. Large companies like Google, IBM and amazon provide clients with

existing cloud services. In private cloud, only the approved clients can get required services from the supplier [9].

Security is a big problem in cloud computing. In cloud computing environment, information security is considered as a major issue. Security means copious. Privacy, accessibility, respectability, avoidance of the unapproved data and the anticipation of the unapproved change together refered as security [10]. Information security turns out to be the biggest security challenge in cloud computing because of the information scattering in various storage gadgets and machines. Information security in conventional data systems is less complicated when compared with information security in the cloud. So, there is a need to correct the security worries of the clients in order to make cloud computing more trustworthy for the clients.

All the information or data is put away on the cloud in cloud computing. How secure is the cloud? Will secret information be accessed by unapproved clients ?. Cloud computing organizations mostly says that information is secure, yet it's too soon in the diversion to be totally certain of that. Cloud computing needs consistent and fast web in order to get to your own information, if the internet is dead that means no work, cloud basically does not work when the client is offline [11]. Inspite of the fact that there are various advantages of Cloud Computing, there are also some critical barriers to its adoption like security, consistency and integrity issues [12]. In short, information protection, information insurance, information accessibility, and secure transmission are the issues considered in this survey paper. Multi-tenancy, data loss, threats, outside malicious attacks are also included in the security challenges [10].

II. CLOUD COMPUTING SECURITY ARCHITECTURE

Security in cloud becomes a troubling issue. The clients neither control nor have any knowledge of, what could happen to their own information. This is an incredible worry in situations where the stored data is significant and valuable to a user. There is a great need of the ensurance of the safety of customer's information as clients won't trade off their privacy. Due to security developments, there always be a risk of someone to find a way to disable the security and have access user's personal data. So, it becomes a challenge [13][14].

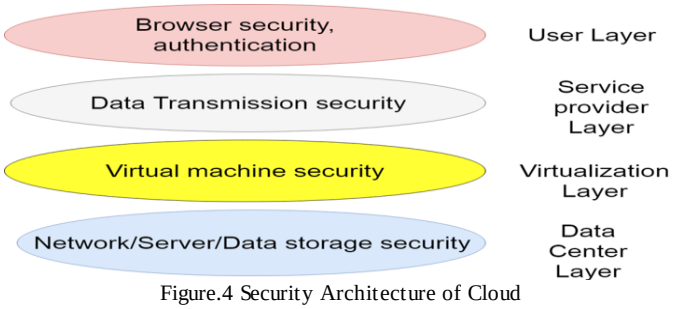

Figure.4 Security Architecture of Cloud

III. SECURITY CHALLENGES OF CLOUD COMPUTING

A. Meta-info spoofing attack

In meta-information spoofing, an attacker might take benefit of the meta information that is exchanged among web browser and web server due to the customer's demand executed in light of verification and approval. In case the attacker gets a success, the services will suffer from the conditions of deadlocks and the users have to wait for the fulfillment of the job that was not created by user itself [15].

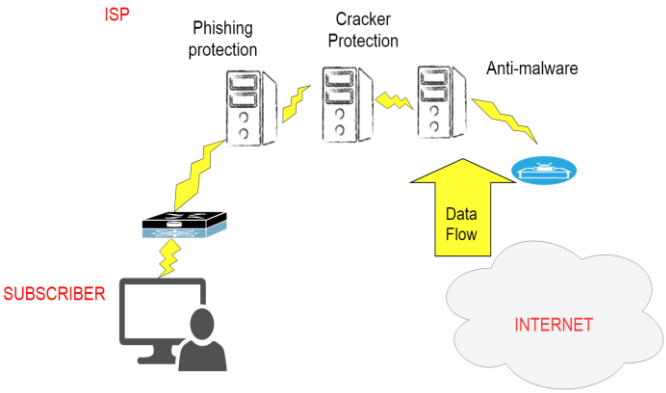

Figure.5 Meta-info spoofing attack

B. Multi-tenancy

SaaS applications can be organized into maturity models having scalability through multi-tenancy. Each customer has its own personalize instance of software in the first maturity model. In second model, the vendor serves distant instances of applications having same application code to all the customers. The third model adds multi-tenancy for a single instance to serve all the customers. There is adequate utilization of resources in this approach but an issue of limited scalability is found. High risk of data leakage is found as data from different tenants is saved in the same database. There is a great need for security policies for the assurance of keeping customer's data separate from other customers [8][16].

C. Loss of control

When data is port in the cloud by the organizations, the location of data is not known by the organization. Since the data can be host anywhere in the cloud by the provider. So, the vital data will not under the control of organizations and also the organizations don't know about any security method set up by the suppliers. Figure.5 depicts loss of control over data by the organizations [16].

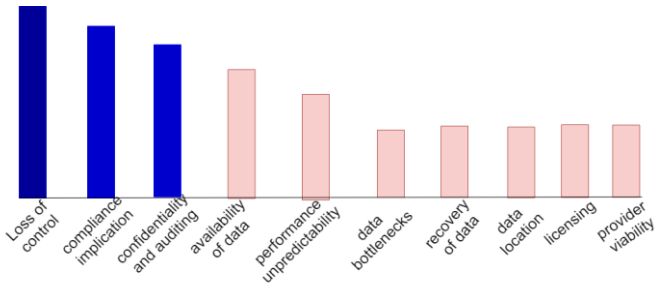

Figure.6 Loss of control is considered as a big security challenge.

D. Data Security

When resources are shared by multiple organizations, there is

a high risk of data misuse. Security of data is the most challenging issue in cloud [14]. Data security means data is confidential, integrate and available all the time. Protection of data from unauthorized modification or deletion is confidentiality [11]. It is the basic requirement of a user in order to store their confidential information in the cloud . Whenever an organization or a business needs to share some data over the cloud, confidentiality issues arises. The type of data that needs to be confidential includes usage data, sensitive information and personal data. Data integrity means data is corrected [6]. Data integrity in cloud must be maintained precisely in order to avoid data lost. For assuring data integrity, any transaction in cloud must follow ACID properties [17]. Data availability is when data is available at time. For achieving the services of cloud computing, HTTP or Hypertext transfer protocol is the common communication protocol. For assuring information security and integrity Secure shell (SSH) and HTTPS are well known protocols. In SaaS, the associations 'information is prepared in plain content and accumulated in the cloud. SaaS supplier is accountable for the information security while the information is being taken care of and set away. Information reinforcement is an interpretive point of view in propelling recuperation in the event of any disaster, however it likewise exhibits some security concerns [18].

E. Data Segregation

Different organizations and users have their data lie together in a shared environment in the cloud. Encryption is not a single solution for this issue. In some cases, customers don't want to encrypt their data because encryption sometimes can leads to violation of data. Encryption schemes should be accessible at all stages which are designed as well as tested by trained professionals [12].

F. Privacy-aware authentication

For authentication purposes, it is necessary for a user to reveal details about him/her. Proxy certificates are found to be helpful in order to reduce the risks regarding the confessing of the details. Proxy certificates are nothing but electronic certificates which contains only those attributes which are considered to be important. For privacy-aware authentication using proxy certificates, the two main requirements are:

a) On the basis of access control policies defined by both users as well as service providers, object and hosts should not demand more attributes than prescribed. On demanding more attributes, service might be negotiated.

b) Credentials that confess data which the identity holder permits can be attained by a trusted third party.

Proxy certificates can be re-utilized and PCAs (Proxy Certificate Authorities) are services supported in the cloud. For attaining stability, hierarchical PCA's can be used [9].

G. Interoperability

It refers to the capability of two or more systems works together for exchanging data and utilizing that exchanged data. For enabling interoperability and security, efforts are to be made for the development of open as well as proprietary API's. DMTF'S Open Virtualization Format (OVF) is a container format that can be utilized. Interoperability can be retained by supplying common interfaces to the objects in order to access the resources. Trusted Computing Base (TCB) can be considered for the above issue. TCB is the accumulation of executable code as well as the configuration files which are secured and installed as a level over the working framework and further gives application programming interface(API) for the client objects. Interoperability can be expert by introducing TCB on each host and portion of asset through TCB [9][19].

H. Virtualization

Users are allowed to design, build, copy, share, move as well as rollback the virtual machines through virtualization, which may allow them to run many applications. VM security is essential just like the physical machine security, and any defect in either one may influence the other. Virtualized environments are exposed to all the attacks for ordinary infrastructures. Since, virtualization enumerates greater points of entry and more inter-relationship complexity, security is a major concern [19].

I. Data Breaches

Various users as well as organizations have their data lie together in cloud surroundings. Cloud becomes a large value target as breaching into cloud environment will probably violates the user's data . Yet SaaS supporter declares that SaaS providers can provide excellent protection to customers data than by traditional ways, Insiders still have approach data in different means. They do not directly access the database and does not lessen the risk of insider breaches which have a large impact on the security [20].

J. Network Security

In SaaS model, the sensitive data of an organization is managed by the SaaS applications and which is to be supplied at the SaaS vendor end. In order to avert the overflow sensitive data of an organization, it becomes necessary to secure the data which flows over the network. In Amazon web services (AWS), traditional network security concerns like IP spoofing are now overcome by the network layer [21].

L. Virtualization Machine Monitor(VMM)

The Virtual Machine Monitor (VMM) or hypervisor [22] is accountable for the isolation of the virtual machines. If VMM is compromised, its VM's may also be compromised as well. In order to avoid a VM to access or update the software's which are running on the VMM, it is important for a VMM to provide isolation [12]. VMM is known to be a low-level software having the ability to supervise and manage its virtual machines. It is capable to move virtual machines among physical servers for the purpose of fault tolerance as well as load balancing. This feature sometimes can cause security problems.

M. Data Transmission

Encryption process is used in data transmission. During the transmission of data, there will be no change in the data content. Moreover, the data reaches exactly the same location where the user needs it to send. Cloud always require encrypted data. Authentication, auditing as well as

authorization are some access controls which are used for maintaining integrity during the transmission of data within cloud. In cryptographic attack, there is always an attacker placed in the communication path in order to interrupt and change the communications [23].

N. Data Integrity

Data integrity is considered as a serious concern in cloud computing. An individual system having a single database easily achieves data integrity via database transactions. It is necessary that ACID properties should be followed by transactions in order to ensure data integrity. ACID transactions are supported by most databases that helps in guarding data integrity. There are various databases as well as applications in a distributed system. When transactions around multiple data sources are handled safely and correctly, the data integrity will be maintained automatically in a distributed system [6].

O. Accountability-check problem

Cloud follows "no bill, no-use method" in the case of payment. On launching an instance, everything is recorded including the quantity of data that is transmitted in the network, CPU cycles per user, as well as the duration of the instance. Customers are charged according to this data. So, in case when the cloud is engaged by the attacker on running a malicious code or by using any malicious service that uses storage and power from cloud server, the one who is charged for such computation is the account holder. Dispute will arise and the reputation of provider's business will damaged [15].

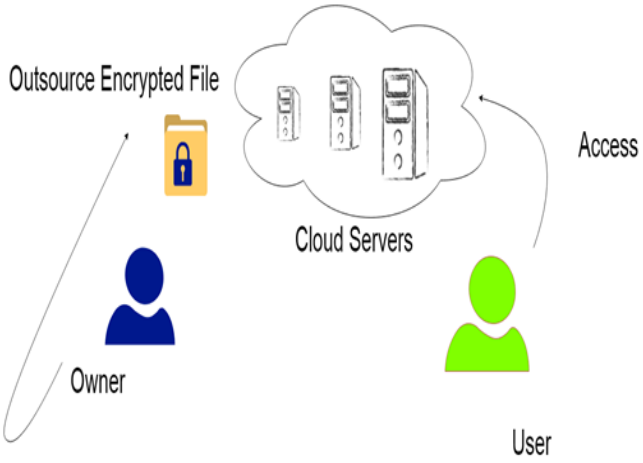

Figure.7 Accoutability-check problem

Table.1 Threats of cloud computing.

THREATS	DESCRIPTION	POSSIBLE SOLUTIONS
Data breach:	A data breach can reveal sensitive information of a customer, trade secrets, intellectual property which in turn causes serious consequences. There are less chances of data loss on keeping a backup of sensitive data offline but it will definitely increase the risk of data exposure. Side channel timing data can be easily accessed by a virtual machine in order to derive private cryptographic keys which are used by some other virtual machine in similar network. It is an excellent aspect of multitenancy. If not architectured in a proper way, may allow an attacker to access users' data easily.	• Prefer to choose a best, proper and trustworthy Cloud provider. • To make data secure, it is necessary to install a proper encryption systems
Account/Service Hacking:	Extortion, phishing, software exploitation are those attacks which usually happened upon gaining access to someone's account in an illegal way or stealing credentials. Hacking of account can ruin a person's integrity and reputation [12]. With hacking of record, an aggressor may access the delicate data, releases private information, introduce harmful sources into the victim's system.	• Sharing of credentials among users should be restricted. • A strong two-way authentication process should be used. • Tracking employees activities for the detection of unauthorized acts.
Malware attack:	A cloud environment is more prone to malware attacks due to lower visibility and more vulnerabilities. As cloud providers may not give information about how they track a user, allocate	. • Introducing human resource requisites in legal agreements. • Requirement for complete and unrestricted visibility in the security mechanism.

	access to the software or other functionalities, which in turn allow the attackers to introduce malicious viruses and software's.	
Cloud abuse	One of the cloud's service model known as IaaS or infrastructure as a service which is popular for offering virtualization of devices, networks does not have secured procedure for registration. This means anyone with a suitable credit card can have access to cloud by completing the signup process. Due to this, cloud can become vulnerable to various crimes like spam mails, malicious attacks etc.	• Need of authorization in registration as well as validation processes. • Monitoring of credit card processes for averting frauds. Completely examine the network traffic.
Malicious insiders	Since company's resources are accessible to the employees who are working in cloud service provider, there is a need for proper security guidelines in order to track employees' actions. As there is no proper security measures or policies which are to be followed by cloud service provider, employees can be easily accessible to the sensitive information without being detected.	• Provide different user access level control. • The attack surface of the network should be minimized so, in case a malicious insider does gain access to the confidential data, it is confined to one area. In case of unknown malicious insiders, Block access to the sites where malware arrives or flourishes.

Table.2 Vulnerabilities of cloud

VULNERABILITIES	DESCRIPTION	POSSIBLE SOLUTIONS
Session hijacking and riding:	Session hijacking is a malicious attack in which an attacker yields unauthorized access into the computer system of an authorized user by using a valid session key. Session riding is fooling a user to visit a destructive website where the user's information is removed by sending commands to web applications.	• A system with strong firewalls should be used by the users
Virtual Machine Escape:	In this vulnerability, there is direct communication of attacker with the host operating system through the splitting of isolation layer which isolates the virtual machine from the host operating system. This causes increase in the attack surface for the attacker	• All through there is no proper solution of these vulnerabilities but we can minimize the VM escape by doing these steps: • By keeping VM software patched. • Install only that resource-sharing features that is really need. • Install minimum software, because each program has its own vulnerabilities
Insecure Cryptography	There is a novel method for all cryptographic algorithms which is determined by the attackers in order to breach the cryptography which in turns resulting in insecurity. The faults and defects in the cryptographic algorithms are common to identify which makes a strong encryption turns into weak encryption. The virtual machines utilized on the cloud are prone to various attacks as they	• The data centric approach as it focuses on security of data itself whereas other techniques considers security of application & networks.

	don't have sufficient sources of entropy	
Internet-dependency	Internet connectivity is required for accessing cloud services. If for some reason internet connection fails, client won't be able to access cloud services. Businesses will gradually lose money as the users won't be able to connect to the cloud which is necessary for business operations	• There should be a smartphone application seeking data from cloud which can be used for emergency situations

IV. CONCLUSION:

Cloud computing helps the organizations in not only increasing their efficiency but also reduces the operating costs. Even though cloud computing become popular in today's world but still it's security issues needs more attention. An overview of cloud computing followed by various security issues, threats and vulnerabilities with possible solutions are presented in this paper. Data security, integrity, loss of control, data segregation are some of the security issues that needs a great attention in order to increase the adoption of cloud computing in businesses. It is believed that end-to-end security is difficult to obtain in cloud because of it's security. The above issues are the principal reasons behind the organizations which prefers to store their personal information in their own local machines rather than cloud. So, to make cloud computing more established and efficient, it is important to focus on various parameters in which security is must.

[1] F. B. F. Shaikh and S. Haider, "Security threats in cloud computing," *2011 Int. Conf. Internet Technol. Secur. Trans.*, no. December, pp. 214–219, 2011.

[2] D. Puthal, B. P. S. Sahoo, S. Mishra, and S. Swain, "Cloud computing features, issues, and challenges: A big picture," *Proc. - 1st Int. Conf. Comput. Intell. Networks, CINE 2015*, pp. 116–123, 2015.

[3] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," *2012 Int. Conf. Comput. Sci. Electron. Eng.*, no. 973, pp. 647–651, 2012.

[4] K. Dahbur, B. Mohammad, and A. B. Tarakji, "A survey of risks, threats and vulnerabilities in cloud computing," *Proc. 2011 Int. Conf. Intell. Semant. Web-Services Appl. - ISWSA '11*, pp. 1–6, 2011.

[5] H. Kaur, "Cloud Computing : Rain-Clouds System," vol. 2, no. 10, 2012.

[6] S. S. Deshmukh and G. R. Bamnote, "Access to Encrypted Data in Cloud Database," pp. 347–350.

[7] O. Kuyoro, S; Ibikunle, F; Awodele, "Cloud computing security issues and challenges," *Int. J. Comput. Networks*, no. 3, pp. 344–349, 2010.

[8] S. C. Rachana, "Emerging Security Issues and Challenges in Cloud Computing," vol. 3, no. 2, pp. 485–490, 2014.

[9] D. T and G. R, "Platform-as-a-Service (PaaS): Model and Security Issues," *TELKOMNIKA Indones. J. lectr. Eng.*, vol. 15, no. 1, pp. 151–161, 2015.

[10] Y. Sun, J. Zhang, Y. Xiong, and G. Zhu, "Data Security and Privacy in Cloud Computing," *Int. J. Distrib. Sens. Networks*, vol. 2014, 2014.

[11] M. Kaur and H. Singh, "a Review of Cloud Computing Security Issues," *Int. J. Adv. Eng. Technol.*, vol. 8, no. 3, pp. 22311963–397, 2015.

[12] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," *J. Internet Serv. Appl.*, vol. 4, no. 1, pp. 1–13, 2013.

[13] R. Padhy, M. Patra, and S. Satapathy, "Cloud Computing: Security Issues and Research Challenges," *... Inf. Technol. Secur. ...*, vol. 1, no. 2, pp. 136–146, 2011.

[14] A. Srivastava, "A Detailed Literature Review on Cloud Computing," *Asian J. Technol. Manag. Res.*, vol. 4, pp. 2249–892, 2014.

[15] G. Kulkarni, N. Chavan, and R. Chandorkar, "Cloud Security Challe n ges," pp. 88–91, 2012.

[16] A. Behl, "Emerging Security Challenges in Cloud Computing An insight to Cloud security challenges and their mitigation," pp. 217–222, 2011.

[17] R. Velumadhava Rao and K. Selvamani, "Data security challenges and its solutions in cloud computing," *Procedia Comput. Sci.*, vol. 48, no. C, pp. 204–209, 2015.

[18] H. Kaur and E. V. Gautam, "International Journal of Computer Sciences A Survey of Various Cloud Simulators," no. 9, pp. 3–6, 2014.

[19] H. Takabi, J. B. D. Joshi, and G.-J. Ahn, "Security and Privacy Challenges in Cloud Computing Environments," *IEEE Secur. Priv. Mag.*, vol. 8, no. 6, pp. 24–31, 2010.

[20] S. V. K. Kumar and S. Padmapriya, "A Survey on Cloud Computing Security Threats and Vulnerabilities," *Int. J. Innov. Res. Electr. Electron. Instrum. Control Eng.*, vol. 2, no. 1, pp. 622–625, 2014.

[21] M. M. Potey, "Cloud Computing – Understanding Risk , Threats , Vulnerability and Controls : A Survey What Comprises Cloud Computing ?," *Int. J. Comput. Appl.*, vol. 67, no. 3, pp. 9–14, 2013.

[22] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 1–11, 2011.

[23] R. BHADAURIA, R. CHAKI, N. CHAKI, and S. SANYAL, "Security issues in cloud computing.," *Acta Tech. Corviniensis - Bull. Eng.*, vol. 7, no. 4, pp. 159–177, 2014.