ISSN: 2616-5325

SURVEY ON DATA SECURITY AND PRIVACY ISSUES IN CLOUD COMPUTING AND EXISTING SECURITY TECHNIQUES

Tehseen Afzal[1], Saman Saeed[2]

Capital University of Science and Technology, Islamabad, Pakistan
tehseen_fjwu@yahoo.com[1], *Samansaeed836@gmail.com*[2]

Abstract

Cloud computing is an ever-growing technology and need of the hour as it allows the optimum use of resources as well as it provides efficient services to cloud users including storage, computations etc. Users' data is stored and processed over cloud. However, many organizations are reluctant to share their data on cloud due to data security and privacy concerns. Several techniques have been adopted to deal with data security issues and win the cloud users' trust. Therefore, it is very essential to use security measures to reduce the data security risks of cloud users. In this paper, a survey study has been conducted on data security issues in cloud and discussed some existing techniques which are used to secure data that is stored over cloud. The concepts of cloud computing and current security mechanisms are briefly discussed in this paper, after thorough study of different data issues and security mechanism, a few recommendations are given at the end to improve the protection of data on cloud.

Keywords

Security, Privacy, Mechanisms, Cipher Text, Encryption, Cloud Computing

1. INTRODUCTION

Cloud Computing has received increased interest in both academia and industry [2]. The term cloud computing is derived from cloud in which cloud represents the network and internet [3]. Cloud computing provides shared computer processing resources on demand that can be immediately provisioned and released [1]. Cloud computing resources are accessible to anyone, anywhere and anytime. It consists of three service models and four deployment models [1]. The data security and privacy in cloud computing are critical aspects. Several surveys have been conducted on data security and privacy in cloud computing. However, we will focus on different data security, privacy issues and effects of these issues in cloud computing layers. We will discuss some existing solutions. In section 2 of this paper, we will define cloud architecture in which deployment models and services models of cloud computing will be discussed [1], [6]. Section 2 will also explain the characteristics of cloud computing [5]. Section 3 will discuss data security and privacy issues in cloud computing. Furthermore, section 4 will explore existing solutions. Finally, in Section 5, a few suggestions have been given to improve the data security over cloud.

2. Cloud Architecture

Cloud computing provides hosted services over the internet. The name "Cloud computing architecture" refers to different components and subcomponents, a cloud is made up of. Cloud computing has four deployment models [1], [5]. Commonly used models are Private Cloud, Public Cloud and Hybrid Cloud whereas Community Cloud model is less commonly used deployment model. The brief description of deployment models is given below:

ISSN: 2616-5325

- Many organizations tend to utilize their resources to their maximum and also minimizing the cost. To attain this objective, organization builds its own cloud therefore this model is basically the cloud of an organization [1]. The organization itself manages the whole cloud or private cloud is controlled by some third party [5]. Resources of the cloud are utilized by the single organization only.

- Public cloud is available to general public or some very large industrial group [1]. A public cloud is set of resources provided by third party organizations. These services and resources are shared among all the users of cloud [5]. The physical infrastructure of the cloud is placed away from the consumer and is controlled by cloud service provider (CSP).

- Community cloud is shared by more than one organization, based on some common communal concerns and mutual benefits such as mission etc [1]. This type of cloud may be controlled by any one of the organizations or a third party [5].

- Hybrid cloud is a mixture of one or two types of clouds [1]. It combines the usage of two clouds for the same organization [5].

The National Institute of Standards and Technology (NIST) classifies the services provided by the cloud in to three categories; Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) [1], [6].

- Software as a Service (SaaS) enables cloud service consumers to run existing online applications via internet [1]. User only pays for the usage of service based on the subscription [6].

- Platform as a Service (Paas) provides application environment in which developers can develop their applications without building the infrastructure. This service provides pre-build infrastructure. PaaS does not allow the users to control the underlying infrastructure but simply they are moved to the cloud [6].

- The Infrastructure as a Service (IaaS) provides hardware infrastructure to the clients on demand. Infrastructure includes the memory, network, processor, storage and a variety of other infrastructure. These resources are accessed through internet. The Cloud Service Provider has a control over the complete set of resources. [6].

2.1 Essential Features of Cloud Computing

Cloud computing is one of the rapidly growing technologies. A number of key characteristics of cloud computing has been identified. Few of them are briefly discussed below:

On-demand self service: Cloud customer can access resources anytime on demand. Resources are easily accessible from anywhere and no human interaction required [1], [8].

Broad network access: It enables the users to access resources using broad access network which include wired, fibre and wireless networks [1], [5].

Resource Pooling: Shared computer processing resources in cloud computing are pooled in a multitenant environment. User does not have any idea about the location of provision resources. User simply accesses the resources on demand [1], [5].

Rapid Elasticity: Cloud computing provides shared computer resources on demand to the user that can be immediately provisioned and released [5], [8].

ISSN: 2616-5325

Measured Service: Cloud resources are automatically optimized. The capability of resources is maximized according to the nature of service. (e.g. storage, processing, bandwidth, etc). Provider and consumer can control the resources usage of service used [1], [7].

Scalability of Infrastructure: Cloud computing provides scalability. We can add or drop nodes from the network by making few changes in the cloud infrastructure [5].

Cost Effectiveness: Cloud cost is decreased by building large clouds in close proximity to economically inexpensive power station [5].

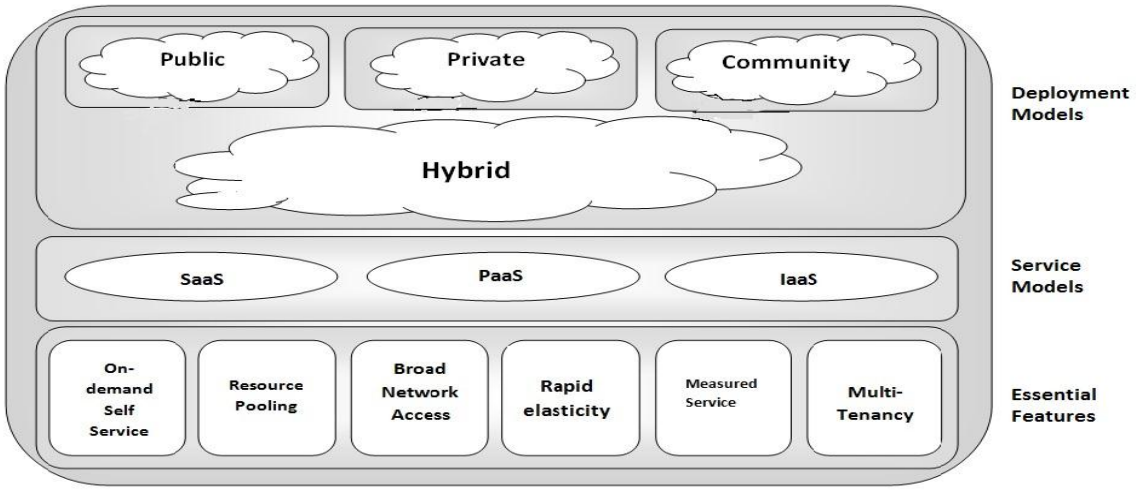

Fig. 01: Cloud Deployment Models, Service Models and Features

3. SECURITY ISSUES IN CLOUD COMPUTING

Due to a variety of advantages and potential risks, cloud computing has attracted researchers. Cloud services are provided over the internet. The users utilize these services. They do not need to purchase or install software at their own computers. In cloud environment, mostly the data and software reside at remote location. Such situation has a created a sense of concern as how users' data is kept and the services are managed over cloud.

Following are the data protection issues in cloud computing environment [8].

Identity Management is a one of the important issues in cloud environment. Unauthorized users use different identity tokens and access user private data. An IDM system should be able to provide strong authentication for the protection of private information related to users [8].

Trust is another big issue in cloud computing. A key inhibitor to adoption of cloud services is lack of consumer trust. An efficient trust management system must be used to establish trust between users and cloud service provider [8].

ISSN: 2616-5325

Availability is the feature of a system that it is only accessed by authorized users or systems on request. Timely and on-demand services provision is ensured by the system availability. Therefore cloud service providers need to make the resources available almost all the time [8].

Authentication and Authorization policies require to be made more effective to make the cloud secure and build trust among the cloud service providers and cloud service consumers. Password authentication along with other identification strategies should be used to verify a cloud user as a legitimate one [8].

Confidentiality means protected data is accessed by authorized users and systems only. An increase in number of access terminals, users, systems and applications result in increase in security risk to data stored over cloud. Data confidentiality means to make protected data secure from unauthorized access. It needs user authentication. [8] Users' account theft prevention is a type of measure to restrict access to memory, applications etc.

Administrative Security: Some cloud service providers are not the certified providers. They may be replication of a Web page that already exists, to dodge and persuade users into giving private or their passwords [9].

Data Security: The cloud service providers need to backup data regularly to recover data efficiently in due to accidental or intentional loss or data corruption and to avoid unintended leaching. Strong encryption methods are also required to keep the data secure and inaccessible by unauthorized people [26].

Malicious insiders: In cloud environment, the data of different parties is stored together. Risks to data of all the users are increased due to breaching into the surroundings of cloud. Though cloud service providers claim that they provide improved protection to users' data, still is accessed by insiders in different manners. Although insiders are not provided direct access to database; that does not reduces hazards to data due to insider breaching. It still has deep impact on the data security in cloud [21].

Data integrity is an extremely serious issue of any organization, user or network. Data integrity can be achieved easily in a standalone system with single database. However in distributed systems like cloud computing, there are multiple applications and database, therefore, in a distributed system environment, the data transactions across all the resources require to be handled in a secure and fool proof way. One approach to verify the integrity of data is by using hash values. by using a pre-defined algorithm, a set of data values are merged to generate a single unique value called hash value [8].

Security Gap in Web Applications: Different types of software components and frameworks are used to develop applications in cloud computing environment. The cost of a conventional software product and deploying a new software solution is decrease by using these tools. Security gap in web applications creates a limitation to the cloud environment. As a result of this situation, this weakness may have potentially unfavourable impacts on all the cloud users. New security risks are brought due to web applications. These risks are not able to be protected against at network level in an effective manner and do not need defences at application level.

4. EXISTING SECURITY SOLUTIONS

It is the demand of intensive growth of cloud environments in industry that new solutions to data security issues must be devised. Faulty cloud environments have given birth to a large number of security issues throughout the time which may have proven the cloud difficult for some industries. Many researchers have furnished the cloud computing history with their research efforts by contributing different security mechanisms and techniques to make data secure over cloud and increase the level of interest among cloud service providers and users. In this section, we are going to discuss current security mechanisms used in cloud environment.

4.1 Encryption (or Cryptography)

ISSN: 2616-5325

Encryption is the technique which is one of the most straight forward security measures to apply in cloud environment to preserve the confidentiality of user data and its security [11]. Encryption methods can be divided in to three categories: symmetric key algorithms (Private Key), the asymmetric key algorithm (public key) and hybrid key algorithm [12].Encryption makes data secured from unauthorized users on cloud. However, it requires careful implementation because it does not guarantee complete security [8]. Therefore encryption products from reliable sources must be used. Encryption is used to protect the user data in cloud computing. [13]

"Sharing in the Rain" protocol is proposed by [36]. The said protocol ensures cloud users' to share data securely by following the predefined policies of protocol. The proposed protocol is based on Attribute-Based Encryption (ABE) which allows users to encrypt data based on policies and attributes. Secondly, revocation of access is also part of the Attribute-Based technique according to which we can securely remove access to certain files or data for a user who is miss-conducting or is no more part of the user group, without changing policies or re-encrypting original data. [36] has contributed in enhancing infrastructure of cloud as well security mechanisms for secure sharing of data. [37] has proposed Excalibur, a mechanism to encrypt data on user nodes according to the policy of the mechanism using cipher text-policy attribute-based encryption[38] but this protocol does not define any revocation policy. Sharing in the rain overcomes this limitation of revocation of access. Symmetric Searchable Encryption (SSE) scheme has also been discussed by [1].

4.2 Fully Homomorphic Encryption

Fully homomorphic encryption is an important mechanism which was first created in 2009. In this technique, cloud services are used by the party that holds cipher texts (Encrypted texts) to perform different operations on cipher text which reflect the equivalent operation on plain text. The data is completely secure. Even the cloud cannot decrypt the data [14].

4.3 Trusted Third Party

Trust is an important issue and as a key concern in cloud environment. A key inhibitor to adoption of cloud services is lack of consumer trust. Trust between CSP (Cloud Service Provider) and CSC (Cloud Service Consumer) holds a great significance. More is the trust, more businesses will deploy clouds and it will automatically flourish the cloud environment. [5] Proposed to introduce Trusted Third Party (TTP) to assure certain security features in cloud environment. Trusted Third Party (TTP) ensures secure interaction between the users and cloud or other users in cloud environment. Trusted Third Party delivers trust regarding cloud services and data security. [15] Trusted Third Party in some clouds is also responsible for encrypting data of cloud users to provide secure data and avoid misuse of data if an unauthorized person gets access to users' data.

4.4 Authentication and Certification in Cloud Computing

This security measure is used to prevent unauthorized access to cloud. It ensures that only authorized user is accessing data provided by the cloud service provider. Authentication assurance refers that the identity of user is proved for accessing stored information in cloud. A registering authority (RA) is responsible for registering cloud users. Any new user to cloud must get registered with RA and then given access to resources and cloud services. RA provides certification and authentication to cloud users in order to restrict unauthorized person to access cloud resources.

We can say that there are many authentication mechanisms for securing data in cloud which include: knowledge based authentication, two factor authentication, adaptive authentication, multifactor authentication and single password authentication. [25]

4.5 Intrusion Detection (IDS) and Intrusion Prevention System (IPS)

Intrusion detection systems are implemented to detect intruders and take measures to make data secure in cloud. Intrusion detection systems detect some data patterns (signatures) as done in antivirus programs which can mark any

ISSN: 2616-5325

data packet as secure or that of an intruder. Only secure packets are allowed to move through cloud. All suspicious packets are discarded and not transmitted to other users. There are following types of IDS:

- Network Intrusion Detection Systems (NIDS)
- Host Intrusion Detection Systems (HIDS)

Intrusion Prevention Systems prevent intruders to access cloud resources or data.

IPS has following types:

- Network Intrusion Prevention Systems (NIPS)
- Host Intrusion Prevention Systems (HIPS)

IDPS (Intrusion Detection and Prevention) systems detect as well as prevent intruders to achieve their mischievous objectives [21].

4.6 Access Control in Cloud Computing

Access control can be considered as one of the important security technique to make data secure in cloud computing. By applying access control, data stored over cloud is accessible to only authorized users. Intrusion detection systems, firewalls and segregation of obligations can be implemented on different network and cloud layers. [25]

4.7 Fragmentation-Redundancy-Scattering (FRS) Technique

In this technique, confidential information is broken down into insignificant fragments and then these fragments are scattered across distributed systems like data centres according to different algorithms. All the fragments are never stored on a single node; therefore if some of the fragments are recovered by a hacker, the attack will be of no use. Even if any intruder gets all the fragments, still it is impossible to assemble then in correct order to get the actual information. The fragments are stored on n servers so attackers need to access n servers to access all fragments. EFRS (Encryption-Fragmentation-Replication- Scattering) uses encrypted fragments scattered across distributed systems which makes data more secure. When the data is encrypted by EFRS and *n* fragments are generated, the intruder needs to cryptanalyze combinations of (n!) fragments. This technique provides mechanism to tolerate intrusions. [24]

4.8 Multi-agent system

This approach allows to make a secure cloud by using multi agent system architecture to make data secure on cloud storage. This architecture uses specialized self-governing agents for particular security services and enables them to interact and to facilitate security of Cloud Data Storage (CDS). [33]

4.9 Role-Based Access Control (RBAC)

Role-based access control (RBAC) is a mixture of mandatory and optional access control [22]. In RBAC, a role can be defined as a job function and permission level that gives a user particular access rights with respect to a file and these rights can be formulated in high level or low level languages. The access rights are handled by assigning permissions in a very significant way because every operation holds some specific meaning within an application [16].

4.10 The Trace of the User's Behavior

ISSN: 2616-5325

The trace of user's behaviour helps in maintaining the security and privacy of data. A log is maintained about activities of a cloud user, the log can trace the changes made to data by the user as well as if someone behaves oddly, the trace will help CSP to take proper action accordingly [16].

4.11 Key Translation in browser

In this technique, the data is encrypted before uploading to cloud. The data owner retains the encryption and decryption keys. Therefore, cloud does not have any right to see the data and perform any operation on data. Thus data is secured against privacy violation. [28]

4.12 Hardware Anchored security

In this type of security mechanism, a special hardware component is used to store the keys in such a way that only certain programs can access those keys. A policy is agreed upon by cloud service consumer and cloud service provider on about how the data will be accessed and processed by the cloud applications. However, it is very challenging to implement and manage this security mechanism. [34]

4.13 Virtualization

Virtualization can enhance security in cloud. By using virtualization technique, single physical machine is logically partitioned into multiple virtual machines (VMs). Each VM is isolated and easily manageable. Data security and privacy is easy for each VM. Moreover, if any of the VMs gets failure, rest of the VMs continue to provide services to cloud users. [26]

4.14 Hadoop

Another one of the important security measures is Hadoop. It is Java-based framework for distributed processing of large datasets across large clusters of computers that deals with the storage of extremely large amount of data. Data is divided into segments and these segments are stored in clusters. It is very efficient and fault tolerant mechanism. [23]

4.15 HAIL (High-Availability and Integrity Layer)

HAIL is type of distributed cryptographic system. This technique allows a set of servers to prove to a client that a stored file is completely secure and retrievable. Some distinct mechanisms from the cryptographic and distributed system areas are strengthen by HAIL. This approach maintains the data integrity and availability across a set of servers. [20]

4.16 RAID (Redundant Array of Independent Disks)

RAID stores the same data in different places an efficient way through multiple hard disks. I/O operations can be completed efficiently by storing data in multiple hard disks, which in return improves the performance of the distributed systems. In cloud computing, RAID improves the confidentiality, integrity and availability of data. [20]

4.17 Multi-Clouds Databases

This mechanism is used to protect the user data on service layer. It ensures confidentiality, integrity and availability of data. Using this mechanism clouds are divided into multiple clouds. The reason is that if one cloud fails then the data can be recovers from other clouds [32].

4.18 Trusted Computing Technology

ISSN: 2616-5325

This mechanism is used to build the trust between user and consumer. Most of the time, users not satisfy to move on the clouds because of trust issue. To overcome this problem, authors proposed a trusted mechanism in which consumer give surety of data security. The agreement is sign between user and consumer. [34]

[39,40] has presented a framework Infrastructure-as-a-Service (IaaS) for security of data over cloud. The protocols allow trusted sharing of data and resistance against the threats defined in threat-model.

[41] Proposed the Trusted Cloud Computing Platform (TCCP) which puts all security, integrity and confidentiality of data over Cloud Service Provider. Other initiatives proposed are Private Virtual Infrastructure (PVI), and Private Cloud Management and Monitoring called PCMONS.

4.19 Secure Domain Name System

This mechanism provides a secure domain name system to the user in which user can access the resources from protected domains. Unauthorized user cannot access the domain of resources. [18]

Following table gives overview of some important studies in cloud computing security issues and techniques to deal with data security and privacy issues. (Table 01)

Table 01: Current security mechanisms in cloud computing

Reference, Year	Layer (Deployment/ Service)	Issues Discussed	Risks Involved	Employed Techniques	Strengths	Weaknesses
[11], 2013 [12], 2013 [8], 2013 [13], 2012 [46], 2013	Service Layers (SaaS, PaaS, IaaS)	Integrity (Unauthorized deletion, modification and insertion of data must be prevented), Confidentiality (protected data should be accessible by authorized users only), Authenticity (User identity must ensures using biometrics or some encrypted techniques)	Loss of data, Problem of security	Homomorphic Encryption, Attribute based encryption (ABE)	Preserve the confidentiality of user's data and its security.	It does not guarantee complete security.
[14], 2013	Service Layers (SaaS, PaaS, IaaS)	Confidentiality (Cloud based data is widely accessible by insecure protocols or APIs across public networks)	Inefficiency and safety of decrypted data	Fully Homomorphic Encryption	Magic solution of a big confidentiality problem and provides complete security.	It does not provide verifiable computation.
[5], 2012 [15], 2009	Deployment layer	Confidentiality (Securing users account from theft), Authenticity (Authenticate the identity of user) ,	Interactions between two parties based on trust.	Trusted Third Party	Provides strong authentication, authorization, data integrity and data confidentiality.	It is not directly applicable in an authentication and digital signature scheme,

ISSN: 2616-5325

		Integrity (Prevent the alteration of information from unauthorized users)				because it requires honest secret dealer and honest secret recovery unit.
Reference, Year	Layer (Deployment/ Service)	Issues Discussed	Risks Involved	Employed Techniques	Strengths	Weaknesses
[25], 2016	Service Layer (SaaS)	Integrity (Protect data from unauthorized access), Authenticity (Ensures authenticity of proper entity or person)	Unauthorized access to secure area	Authentication and Certification in cloud computing	Provides identity management, Mutual authentication and Session key agreement.	1) Password verification is done by the local system. 2) If central server is hacked then entire server is hacked.
[21], 2014	Network Layer	Access Control (Data stored in the cloud is accessible by authorized users only), Authentication (Users identity should be proved to the cloud service provider)	1) Malicious insider 2) Attacker creates lot of traffic on cloud through emails	Intrusion Detection and Intrusion Prevention System	Provides detection and prevention of malicious activity in cloud.	IDS and IPS are cheaper to implement.
[25], 2016	Service Layer	Access Control (The requested data stored in the cloud is provided to authorized users only)	Unauthorized access	Access Control in Cloud Computing	It ensures that stored data is only accessible to authorized users.	Anybody can access the data from anywhere because it is based on the internet.
[24]	Service layer (SaaS)	Confidentiality (Unauthorized access cannot read the personal information of users), Integrity (Protection of information from unauthorized access) and Availability (Data should not be accessible on demand for unauthorized users)	Unauthorized user can access the secure information	Fragmentation-Redundancy-Scattering Technique	Provides fragmentation because if any intruder gets all the fragments, it is impossible to assemble then in correct order to get the actual information.	Unauthorized user can access the fragments due to the provision of weak maintenance.

ISSN: 2616-5325

[33], 2013	Service Layers	Data Security (Protection of personal information on cloud)	Data loss, unauthorized access and poor use of services	Multi-agent System	Provides confidentiality and integrity of data.	It does not ensure the complete data security.
[22] [16], 2010	Private Cloud and Service Layers	Authenticity (User identity must ensures using biometrics or some encrypted techniques)	Distributed Denial of Service Attacks	Role-Based Access Control	Provides authorization roles like permissions and assignment.	It does not ensure complete guarantee of authorized access.
[16], 2010	Service Layers	Authentication (must authenticate the identity of user)	Unauthorized Access	Trace of the Users Behavior	Provides verification methods, authentication, communication security and data protection.	Participants can do some malicious behaviour.
[28], 2013	Service Layer (SaaS)	Confidentiality (Protected data is accessible by authorized parties only.)	Risks of data security and privacy	Key Translation in Browser	Provides strong security and privacy guarantees.	Complete security does not ensure.
[34], 2013	Service Layers	Confidentiality (Poor authentication results in unauthorized access to users account on a cloud)	Unauthorized Access	Hardware Anchored Security	Binary attestation system used for confidentiality	Very difficult to implement
[26], 2012	Service Layers	Confidentiality (Only cloud user can access the resources based on authentication), Integrity (unauthorized access can modify, delete or add the data on cloud), Availability (Users data should not be accessible to unauthorized users like intruders)	Intrusions and DDOS attacks	Virtualization	Provides more secure and robust environment.	Maintenance of servers is difficult task and very complicated.

ISSN: 2616-5325

Reference, Year	Layer (Deployment/ Service)	Issues Discussed	Risks Involved	Employed Techniques	Strengths	Weaknesses
[23], 2015	Service Layers	Issue of big data	Large amount of data on clouds.	Hadoop	Provides efficiency	Hadoop does not provide the facility of encryption for data storage and it is not suitable for small data.
[20], 2013	SaaS	Integrity (Protecting data from unauthorized deletion, modification and addition), Confidentiality (Only authorized parties having ability to access protected data), Authenticity (User identity must ensures using biometrics or some encrypted techniques)	Data Privacy	High Availability and Integrity Layer (HAIL)	Provides integrity and availability.	It does not ensure strong encryption.
[20], 2013	SaaS	Integrity (Protection of information from unauthorized access), Confidentiality (Unauthorized access cannot read the personal information of users) and Availability (Data should not be accessible on demand for unauthorized users)	Data Privacy	Redundant Array of Independent Disks (RAID)	Provides integrity and availability.	Disks failures may significantly decrease throughput. The configuration may be too much if a small file transfer is the only requirement.
[32], 2011	Service Layer [SaaS (Business logic layer and Data processing layer)]	Confidentiality (Data is not secure due to unauthorized access), Integrity (Unauthorized access can modify or delete the data), Availability (Authenticity of users must be confirm)	Risk of data integrity and data confidentiality, loss of service availability	Multi-Clouds Databases	Provides data integrity and confidentiality.	May increase security risks in cloud computing.

ISSN: 2616-5325

[34], 2013	Service Layer	Authentication (must authenticate the identity of user), confidentiality (Only authorized parties having ability to access protected data) and integrity (Protection of information from unauthorized access)	Data Confidentiality, integrity	Trusted Computing Technology	Provides trusted approaches.	It is not directly applicable for users.
[18]	Service layer (IaaS)	Threats (Weak identity, credentials and access management), Facets	Deployment of Domain Name System	Secure Domain Name System	1) Provides Secure Domains to the user. 2) Give privacy from unauthorized access.	It does not ensure complete security of access management.

5. RECOMMENDATIONS FOR IMPROVED DATA SECURITY IN CLOUD

In this section, we are going to present some recommendations to make data secure over cloud.

- One of the important and foremost recommendations is to increase the trust among cloud service provider and cloud service consumers by ensuring that the valuable data of users is protected with efficient governance and monitoring. It means that security controls must exist which can increase the security and risk tolerance in cloud. Information which is allowed to be processed on cloud must be identified appropriately.

The cloud service provider's security management wing must have sufficient knowledge to detect, prevent and deal with security breaches on time.

- Third party audits should be performed periodically to check the cloud service provider's compliance with agreed policies and adherence to standards must be ensured. [42, 43]
- Data availability should be ensured by the cloud service provider. Effective measures should be taken to prevent data loss, unwanted data overwrite or destruction. Cloud service provider must have sufficient knowledge to recover data in case of data loss or destruction with adequate back up and replication policies. [44]
- All modifications in the cloud environment should be made and handled properly to maintain the integrity of data and to minimize the disruption and unauthorized changes or errors. Cloud service provider should keep valid and auditable proofs to show that no unauthorized changes occurred during specified period. [45]
- Multilevel user identification system can help to prevent unauthorized access to data over cloud.

REFERENCES

[1] Mell, Peter, and Tim Grance. "The NIST definition of cloud computing." (2011).

ISSN: 2616-5325

[2] Takabi, Hassan, James BD Joshi, and Gail-Joon Ahn. "Security and privacy challenges in cloud computing environments." *IEEE Security & Privacy* 8, no. 6 (2010): 24-31.

[3] Gorelik, Eugene. "Cloud computing models." PhD diss., Massachusetts Institute of Technology, 2013.

[4] Hwang, Kai, Sameer Kulkareni, and Yue Hu. "Cloud security with virtualized defense and reputation-based trust mangement." In *Dependable, Autonomic and Secure Computing, 2009. DASC'09. Eighth IEEE International Conference on*, pp. 717-722. IEEE, 2009.

[5] Zissis, Dimitrios, and Dimitrios Lekkas. "Addressing cloud computing security issues." *Future Generation computer systems* 28, no. 3 (2012): 583-592.

[6] Jensen, Meiko, Jorg Schwenk, Jens-Matthias Bohli, Nils Gruschka, and Luigi Lo Iacono. "Security prospects through cloud computing by adopting multiple clouds." In *Cloud Computing (CLOUD), 2011 IEEE International Conference on*, pp. 565-572. IEEE, 2011.

[7] Zhou, Minqi, Rong Zhang, Wei Xie, Weining Qian, and Aoying Zhou. "Security and privacy in cloud computing: A survey." In *Semantics Knowledge and Grid (SKG), 2010 Sixth International Conference on*, pp. 105-112. IEEE, 2010.

[8] Xiao, Zhifeng, and Yang Xiao. "Security and privacy in cloud computing." *IEEE Communications Surveys & Tutorials* 15, no. 2 (2013): 843-859.

[9] Ghebghoub, Y., S. Oukid, and O. Boussaid. "A Survey on Security Issues and the Existing Solutions in Cloud Computing." *International Journal of Computer and Electrical Engineering* 5, no. 6 (2013): 587.

[10] Foster, Ian, Yong Zhao, Ioan Raicu, and Shiyong Lu. "Cloud computing and grid computing 360-degree compared." In *Grid Computing Environments Workshop, 2008. GCE'08*, pp. 1-10. Ieee, 2008.

[11] Hashizume, Keiko, David G. Rosado, Eduardo Fernández-Medina, and Eduardo B. Fernandez. "An analysis of security issues for cloud computing." *Journal of Internet Services and Applications* 4, no. 1 (2013): 5.

[12] Ghebghoub, Y., S. Oukid, and O. Boussaid. "A Survey on Security Issues and the Existing Solutions in Cloud Computing." *International Journal of Computer and Electrical Engineering* 5, no. 6 (2013): 587.

[13] Hamlen, Kevin, Murat Kantarcioglu, Latifur Khan, and Bhavani Thuraisingham. "Security issues for cloud computing." *Optimizing Information Security and Advancing Privacy Assurance: New Technologies: New Technologies* 150 (2012).

[14] Ryan, Mark D. "Cloud computing security: The scientific challenge, and a survey of solutions." *Journal of Systems and Software* 86, no. 9 (2013): 2263-2268.

Hwang, Kai, Sameer Kulkareni, and Yue Hu. "Cloud security with virtualized defense and reputation-based trust mangement." In *Dependable, Autonomic and Secure Computing, 2009. DASC'09. Eighth IEEE International Conference on*, pp. 717-722. IEEE, 2009.

[15] Shen, Zhidong, and Qiang Tong. "The security of cloud computing system enabled by trusted computing technology." In *Signal Processing Systems (ICSPS), 2010 2nd International Conference on*, vol. 2, pp. V2-11. IEEE, 2010.

[16] Jensen, Meiko, Jorg Schwenk, Jens-Matthias Bohli, Nils Gruschka, and Luigi Lo Iacono. "Security prospects through cloud computing by adopting multiple clouds." In *Cloud Computing (CLOUD), 2011 IEEE International Conference on*, pp. 565-572. IEEE, 2011.

[17] Chandramouli, Ramaswamy, and Scott Rose. "Secure domain name system (DNS) deployment guide." *NIST Special Publication* 800 (2006): 81-2.

ISSN: 2616-5325

[18] Li, Jin, Jingwei Li, Xiaofeng Chen, Chunfu Jia, and Wenjing Lou. "Identity-based encryption with outsourced revocation in cloud computing." *Ieee Transactions on computers* 64, no. 2 (2015): 425-437.

[19] Juels, Ari, and Alina Oprea. "New approaches to security and availability for cloud data." *Communications of the ACM* 56, no. 2 (2013): 64-73.

[20] Rahman, Masudur, and Wah Man Cheung. "A novel cloud computing security model to detect and prevent DoS and DDoS attack." *International Journal of Advanced Computer Science and Applications (IJACSA)* 5, no. 6 (2014).

[21] Rani, Meena, and Cherry Assistant Professo. "Role Based Access Mechanism in Cloud Computing: Survey."

[22] Hashem, Ibrahim Abaker Targio, Ibrar Yaqoob, Nor Badrul Anuar, Salimah Mokhtar, Abdullah Gani, and Samee Ullah Khan. "The rise of "big data" on cloud computing: Review and open research issues." *Information Systems* 47 (2015): 98-115.

[23] El Mrabti, Almokhtar Ait, Najim Ammari, Anas Abou El Kalam, Abdellah Ait Ouahman, and Mina De Montfort. "New mechanism for Cloud Computing Storage Security." *International Journal of Advanced Computer Science & Applications* 1, no. 7: 526-539.

[24] Jakimoski, Kire. "Security Techniques for Data Protection in Cloud Computing." *International Journal of Grid and Distributed Computing* 9, no. 1 (2016): 49-56.

[25] Duan, Qiang, Yuhong Yan, and Athanasios V. Vasilakos. "A survey on service-oriented network virtualization toward convergence of networking and cloud computing." *IEEE Transactions on Network and Service Management* 9, no. 4 (2012): 373-392.

[26] John Bethencourt, John, Amit Sahai, and Brent Waters. "Ciphertext-policy attribute-based encryption." In *Security and Privacy, 2007. SP'07. IEEE Symposium on*, pp. 321-334. IEEE, 2007.

[27] Arapinis, Myrto, Sergiu Bursuc, and Mark Ryan. "Privacy-supporting cloud computing by in-browser key translation." *Journal of Computer Security* 21, no. 6 (2013): 847-880.

[28] Ziyad, S., and S. Rehman. "Critical Review of Authentication Mechanisms in Cloud Computing." *International Journal of Computer Science Issues (IJCSI)* 11, no. 3 (2014): 145.

[29] Ziyad, S., and S. Rehman. "Critical Review of Authentication Mechanisms in Cloud Computing." *International Journal of Computer Science Issues (IJCSI)* 11, no. 3 (2014): 145.

[30] Xi, Kai, Yan Tang, and Jiankun Hu. "Correlation keystroke verification scheme for user access control in cloud computing environment." *The Computer Journal* (2011): bxr064.

[31] Jensen, Meiko, Jorg Schwenk, Jens-Matthias Bohli, Nils Gruschka, and Luigi Lo Iacono. "Security prospects through cloud computing by adopting multiple clouds." In *Cloud Computing (CLOUD), 2011 IEEE International Conference on*, pp. 565-572. IEEE, 2011.

[32] de la Prieta, Fernando, María Navarro, Jose A. García, Roberto González, and Sara Rodríguez. "Multi-agent System for Controlling a Cloud Computing Environment." In *Portuguese Conference on Artificial Intelligence*, pp. 13-20. Springer Berlin Heidelberg, 2013.

[33] Ryan, Mark D. "Cloud computing security: The scientific challenge, and a survey of solutions." *Journal of Systems and Software* 86, no. 9 (2013): 2263-2268.

[34] Santos, Nuno, Krishna P. Gummadi, and Rodrigo Rodrigues. "Towards Trusted Cloud Computing." *HotCloud* 9, no. 9 (2009): 3.

[35] Ouedraogo, Moussa, Severine Mignon, Herve Cholez, Steven Furnell, and Eric Dubois. "Security transparency: the next frontier for security research in the cloud." *Journal of Cloud Computing* 4, no. 1 (2015): 12.

ISSN: 2616-5325

[36] Michalas, Antonis, and Rafael Dowsley. "Towards trusted ehealth services in the cloud." In *Utility and Cloud Computing (UCC), 2015 IEEE/ACM 8th International Conference on*, pp. 618-623. IEEE, 2015.

[37] Hashizume, Keiko, David G. Rosado, Eduardo Fernández-Medina, and Eduardo B. Fernandez. "An analysis of security issues for cloud computing." *Journal of Internet Services and Applications* 4, no. 1 (2013): 5.

[38] Lombardi, Flavio, and Roberto Di Pietro. "Secure virtualization for cloud computing." *Journal of Network and Computer Applications* 34, no. 4 (2011): 1113-1122.

[39] Michalas, Antonis. "Sharing in the Rain: Secure and Efficient Data Sharing for the Cloud." In *2016 International Conference for Internet Technology And Secured Transactions*, pp. 589-595. 2016.

[40] Robertson, B.: Top Five Cloud Computing Adoption Inhibitors, cited 1 December(2009)

[41] M. Vael. (2010, 24 July 2010). Cloud Computing: An insight in the Governance & Security aspects.

[42] Cloud Security Alliance. (2009, 20 May 2010). Security Guidance for Critical Areas of Focus in Cloud Computing.

[43] Third Brigade. (2008, 21 July 2009). Cloud Computing Security: Making Virtual Machines Cloud-Ready.

[44] Li, Ming, Shucheng Yu, Yao Zheng, Kui Ren, and Wenjing Lou. "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption." *IEEE transactions on parallel and distributed systems* 24, no. 1 (2013): 131-143.

