An Exhaustive Review on Security Issues in Cloud Computing

Shahin Fatima[1*] and Shish Ahmad[2]
[1] Department of Computer Science & Engineering
Integral University, Lucknow, India
[E-mail : cseshahinfatima@gmail.com]
[2] Department of Computer Science & Engineering
Integral University, Lucknow, India
[E-mail : shish@iul.ac.in]
*Corresponding author : Shahin Fatima

Received August 16, 2018; revised November 30, 2018; accepted December 28, 2018; published June 30, 2019

Abstract

The Cloud Computing is growing rapidly in the current IT industry. Cloud computing has become a buzzword in relation to Grid & Utility computing. It provides on demand services to customers and customers will pay for what they get. Various "Cloud Service Provider" such as Microsoft Azure, Google Web Services etc. enables the users to access the cloud in cost effective manner. However, security, privacy and integrity of data is a major concern. In this paper various security challenges have been identified and the survey briefs the comprehensive overview of various security issues in cloud computing. The classification of security issues in cloud computing have been studied. In this paper we have discussed security challenges in cloud computing and also list recommended methods available for addressing them in the literature.

Keywords: Cloud computing, privacy and security, cloud storage, access control, privacy protection, preventive measures.

1. Introduction

Cloud computing is the latest technology in the current era. Cloud computing provides a remarkable potential with latest range across IT, data storage and business. In cloud computing users can store the data on the remote servers and can access anywhere anytime. The "Cloud Service Provider" provides access to data to the users. The processing of data stored on the remote servers should be taken care of. Now-a-days security of data in cloud computing is a major concern. The data which is to be stored on remote data servers is at high risk and should be managed securely. Since multiple users can access data from remote servers, it's a big challenge in terms of data security. Therefore, proper security mechanisms should be employed to handle these challenges. **Fig. 1** shows that data security and privacy is the most important factor to be considered. According to definition of NIST (National Institute of Standard & Technology) "Cloud Computing is a model for easy, on demand access, resource pooling for delivering services to users by "Cloud Service Provider" [1]. Cloud computing follows the concept of pay as you go model [2]. The user can select any resources such as servers, operating system, memory etc. as per his demand and pay only for that resource. Cloud computing enables the users to access the resources efficiently using virtualization technique. Security is a biggest challenge in cloud computing for various organizations that rely completely on CSP to store its data. Trust factor is also very important in cloud computing. Users have a lot of query regarding which cloud service provider to choose in order to store its data. So maintaining trust by "Cloud Service Provider" is also a big concern.

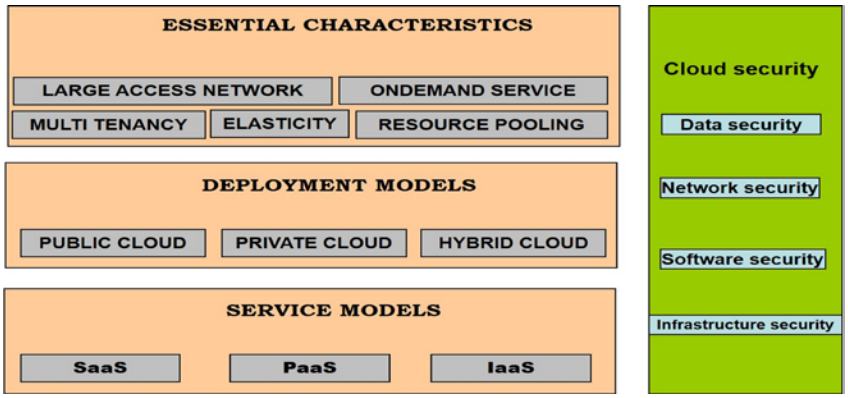

Fig. 1. Cloud Computing Service Framework

2. Cloud Computing Framework

Cloud computing uses various technologies to provide services to customers. According to National Institute of Standard & Technology [NIST]the definition of cloud is accepted [3] [4]. Cloud computing provides three step model of service a] Characteristics of cloud computing b] Deployment models c] Services offered. The paper is organized as follows. After the brief introduction about cloud computing Section II describes the cloud computing framework. Section III explores problems in cloud computing & their possible solutions from different author's perspective. Section IV deals with the classification of security challenges in cloud computing Section V deals with the various types of challenges faced by cloud computing. Finally, in Section VI we discuss about the conclusion, future work and references.

2.1 Characteristics of cloud computing

- **Resource Pooling**

In multitenant environment multiple users share resources provided by "Cloud Service Provider". The customers are much aware about the location of resources.

- **On demand service**

The customers can request the resources as per his demand from CSP and he has to 'pay for what he gets'. Various web services are used to interact with "Cloud Service Provider".

- **Elasticity**

Elasticity refers to scaling up and down of resources. In multitenancy multiple tenants share resources on pay as you go basis.

- **Large Network Access**

Large network is called ubiquitous network access in literature [4]. Services and data present on the cloud must be accessed by the customers using various mechanisms.

- **Multi tenancy**

Multi tenancy refers to using resources by multiple customers of various organizations. The customers are segregated in multi tenant environment for optimal use of resources by customers.

2.2 Deployment models of cloud

Various models of cloud computing are as follows: -

- **Private Cloud**
  Private cloud is owned by any organization or business and it is less secure . Example : Window Server 'Hyper-V'.

- **Public Cloud**
  Public cloud is open to all the users and organizations & the security risks is increased. Service Level Agreement [SLA] refers to license & trust between CSP &customer. In public cloud identifying location of resources is difficult & risks of data protection is higher. Example:- Google Doc

- **Hybrid Cloud**
  Hybrid cloud is the combination of public & private cloud. Hybrid cloud is more secure than public cloud for accessing data over the Internet. Example:- Cloud Bursting for load balancing.

2.3 Services of cloud computing

Cloud computing provide various services to the users & the user use it according to his need. Some services are as follows:

- **IaaS [Infrastructure as a Service]**
  IaaS is at the bottom level of the model. It deals with the hardware, network, server, data center, processor, memory etc. Some organizations don't want to buy a server because of its cost so they can rent a service from the "Cloud Service Provider" instead of purchasing it.

- **PaaS [Platform as a service]**
  PaaS is at the middle level of the model. It provides tools, framework & programs. Google App Engine provides an environment which support many programming languages. User can use these tools.
- **SaaS [Software as a Service]**
  SaaS is at the top layer of the model. In this type of service third party vendor manages the software and it is delivered to the user by web.

3. Security Solution provided in Literature

3.1 Generic Solutions to Privacy and security using secret sharing schemes

A new [K,L,n] threshold ramp scheme has been proposed in [5]. In this scheme if number of participants are k or more than k then it can recover the secret and if participants are less than k then it cannot extract information from secret. The scheme uses LaGrange interpolating polynomial for n shares and then recover the secret. This scheme is proposed to be better than Dekey technique which involves high computational cost to create n shares & then recover the secret to solve the problem. The proposed scheme can be implemented with Dekey on j-KM- "Cloud Service Provider". The technique has fast computation & also reduces storage space.

A multilevel threshold secret sharing scheme is proposed in [6] in order to improve the security in cloud environment. It includes creating replicas of shares and distributed it among different resource providers. The dummy shares are also used to identify if there is a presence of any malicious user. As the number of "Cloud Service Provider" increases the time to split the share decreases. In future various data replication techniques can be used to increase response time for finding data.

The secret sharing scheme is used in [7] to overcome the security issues in multi clouds. Secret sharing scheme is used to secure the data in multi clouds. In this technique the key used for encryption is divided into shares and stored on multiple clouds. The concept of multi cloud is used to increase data security and reduce the risk of data breach.

A multi secret sharing scheme have been proposed in [8] using computational security model for sharing the secrets among participants. The scheme has identified the drawbacks of existing multi secret sharing scheme and proposed a new computational security model. It also compared the existing method with the new method in no of shares & public values and the proposed scheme is found to be more efficient. The proposed method is much efficient and computationally secure.

A new scalable access policy called blocked linear secret sharing scheme [BLSSS] has been proposed in [9]. It has also proposed a cipher text policy attribute based encryption [SCP-ABE] scheme. This scheme uses BLSSS policy. The proposed method is better in terms of storage, computation cost and scalability. The SCP-ABE method has a proposed function update which generates incremental sets of policy updated cipher text.

Two cheating identification algorithms have been proposed in [10]. In the first algorithm m users who participate in secret reconstruction can identify cheaters. The rest n-m users involved in secret reconstruction can identify the cheaters. The symmetry property of bivariate polynomial & linearity of interpolated polynomial for cheater identification has been proposed

A multi secret sharing scheme based on Boolean XOR and asymmetric modulo is proposed in [11]. In the proposed method n shares are created from n secrets and for reconstruction threshold value is recurred. Three [n,n] MSSS has been proposed. The first

and second scheme uses Boolean XOR operation and third scheme is better in terms of security and time complexity.

Table 1. A Study on security and privacy issues using secret sharing scheme in cloud computing

Proposed Work	Focus	References
Multi secret sharing scheme	Security and privacy	[8],[11]
Blocked linear secret sharing scheme	Security and privacy	[9]
Threshold secret sharing	Security and privacy	[5], [6]
Secret sharing scheme	Security and privacy	[7], [10]

3.2 Generic Solutions to Privacy and security using visual cryptography

A new share creation scheme has been proposed in [12] made by [2,2] XOR visual cryptography. It has used AES algorithm to encrypt the shares. The shares generated by scheme and AES algorithm is called encapsulated shares. The proposed technique will give better security and also reduces the occurrence of fraud shares. The proposed technique is used to overcome the complex issue of share maintenance. The proposed scheme has identified how to encapsulate shares in visual cryptography. The scheme uses visual cryptography & encryption to ensure high security.

A secure portable document format is proposed in [13] using extended visual cryptography technique for efficient storage in order to reduce computational time and storage space. The proposed technique ensures data integrity and confidentiality. It has made use of visual cryptography to hide secret data in an image. The technique can hide large data with less effort, space and time complexity.

A new visual cryptography method has been proposed to encrypt or decrypt the data in [14], it takes less time and it can be applied in any field of cloud to improve its security. This technique can be used to improve authentication, access control and encryption of data. The proposed technique takes less execution time than other encryption approaches. In future the visual cryptography can be used in financial domains & other areas of cloud computing.

A new approach [3,4] image secret sharing scheme has been proposed in [15]. The approach made use of actual concept of cryptography over 2x2 blocks of data. Pseudo random sequence is used to re arrange the blocks in order to improve its level of security. In the given technique two pixels of each block is kept as it is and the remaining pixels are transformed to black. Running this process generates 4 shares in which any 3 shares are used to recalculate the original image. Bitwise OR operation is used to reconstruct the original image. In future it can be made [3,6] secret sharing scheme.

Table 2. A Study on security and privacy issues using visual cryptography

Proposed Work	Focus	References
Visual Cryptography	Security and privacy	[12], [13], [14]
Image secret sharing scheme	Security and privacy	[15]

3.3 Cloud specific solution to trust model

A technique to provide security has been proposed in [16] using trust model. The proposed technique calculates trust value and measures the security. The trust value consists of

various parameters which is important to measure the security of cloud services. In order to calculate security and validity of model cloud service alliance [CSA] is used. To verify the adequacy of this it has calculated trust value for conventional cloud services. The user can select a particular service effectively using trust model. Cloud service use trust model to integrate with cloud service managers. The cloud manager stores the trust value in its repository which is used by users to select particular service.

Table 3. A Study on security issues using trust model in cloud computing

Proposed Work	Focus	References
Trust Model	Trust Factor	[16]

3.4 Generic Solutions to Privacy and security using encryption techniques

An Intelligent Cryptography approach has been proposed in [17] through which the "Cloud Service Provider" cannot reach to data directly. In this approach the input file is divided and stored into distributed servers. The proposed model is called securely aware efficient distribution storage. The scheme made use of alternative data distribution, secure efficient data distribution & efficient data conflation algorithm. This approach is very effective in defeating multiple threats. In future the work can be extended to include secure data deduplication to increase data availability.

An approach match then decrypt has been proposed in [18]. In this technique an extra matching phase is also introduced before doing decryption phase. If the private key of attribute matches with access policies of cipher text without decryption, then the technique calculates special component in cipher text. The proposed technique reduces the compilation cost of attribute matching and it becomes less than one-time decryption operation. In order to ensure fast decryption special attributes are generated which allows aggregation of pairs during decryption. In future the work can be extended to develop full secure ABE schemes which supports fast decryption.

A new fully homomorphic encryption algorithm has been proposed in [19] to ensure data security in cloud computing. This technique can be used to process encrypted data and it will lead to secure data transmission & data storage in cloud computing. This technique transfers the data between cloud and user safely. Various mechanisms are used to prevent online piracy and also prevent the violation of copyright digital content. IaaS users is responsible for data confidentiality and data integrity. PaaS and SaaS are equally responsible for data integrity and confidentiality

A new method has been proposed in [20] in which the keys are managed without any central authority and the security is updated dynamically. In the proposed method the privacy is enhanced by hiding the identities of the user. The efficiency of the method is also improved. In future the method can be built which combines the proposed scheme with hierarchical authority ABE.

An attribute based storage system has been proposed in [21]. In this method the public cloud is used for duplicate detection and storage management. The proposed method enables the users to access the policies without sharing decryption keys and achieves better data security. In the proposed method the private cloud is provided with a trapdoor key to transfer the cipher text over one access policy to other access policies. The validity of uploaded item is checked through private cloud.

A ORAM based data sharing scheme have been proposed in [22]. The proposed scheme makes use of shuffle correctness proof to prevent the data block from arbitrary modifications. The proposed scheme provides higher security and better efficiency. In future the work can be extended by reducing the involvement of data owner based on ORAM & new data sharing scheme.
A secure data sharing in clouds [SedaSC] method has been proposed in [23]. The proposed method uses a single key to encrypt the data file. This method ensures data integrity, confidentiality, data sharing and access control. The method makes use of two shares of key and each user will use only one share. The cryptographic server is used to store the other part of the key. The proposed method can be easily used in mobile cloud computing. In future the work can be extended to limit the level of trust in trusted third party.
A privacy preserving [P2Q] query is proposed in [24] for multidimensional big data to overcome the challenge of how to query encrypted data stored in untrusted heterogeneous environment. It has made use of Map Reduce for Hadoop distributed environment. The proposed scheme provides better data confidentiality & data owner's privacy.
A key update method is proposed in [25] to ensure security of data in cloud computing. It has provided the security model with zero knowledge data privacy for cloud computing. The proposed scheme is efficient and the performance is also improved.
A scheme for exchanging the data between users and mobile clouds is proposed in [26]. The proposed method makes use of high efficiency video coding. The proposed method supports real time processing and also saves power consumption. The method also makes use of AES [Advanced Encryption Scheme] for encryption. Using AES in proposed method decreases the processing time and also increases the data size. The proposed scheme supports encoding and decoding of HEVC standard.
A cipher text policy attribute based encryption scheme is proposed in [27]. By using user group, the issue of user revocation can be solved efficiently. The group manager will update the users private key anytime the user leaves the group. The proposed method has high computation cost & it can also tolerate collision attack by revoked users. Using the technique of outsource the computation cost is reduced.

Table 4. A Study on security and privacy issues using encryption techniques in cloud computing

Proposed Work	Focus	References
Intelligent Cryptography	Security and privacy	[17]
Homomorphic encryption	Security and privacy	[19]
Attribute based Encryption	Privacy	[18], [20], [27]
Data Sharing	Security and privacy	[22], [23], [26]
Attribute based Storage	Privacy and Storage Management	[21]
Privacy Preserving	Privacy	[24]
Key Update Method	Security	[25]

3.5 Measures for security specific to applications

A new technique has been proposed in [28] named cipher text policy attribute based cipher text [CP-ABSC]. It uses digital signature and encryption technique to provide authentication, confidentiality etc. A framework for secure sharing of personal health records in cloud has been developed. It also discussed about access control mechanisms and identified the best scenario for storing data on the cloud. The proposed scheme can access fine grained data in cloud computing. The authorized users can sign crypt and

design crypt the data of public health record. In future the work can be extended by using attribute revocation in attribute based signcryption.
An architecture for data sharing has been proposed in [29] which gives high level of security for sharing of patient data in cloud computing environment. It uses attribute based encryption and secret sharing cryptographic algorithm for dividing data into multiple clouds. Attribute based encryption is used for providing access to authorized data. The limitation of the proposed approach is that the point of failure can be ABE key authority can become decentralized if possible. The future work includes management tool for providing support for inter organizational access control policies.
A new algorithm has been proposed in [30] to compare the performance of secret sharing, information dispersal and proposed modified secret sharing algorithm for medical data sharing. The proposed algorithm is used to overcome the problems faced by existing algorithms. The technique can be used to share the data in secret way in dynamic database. It can also be used to secure data in multi cloud environment. In future the work can be extended to improve the performance and flexibility of the system.
A practical solution for preserving the privacy of medical data sharing in cloud computing has been proposed in [31]. It uses vertical partitioning method to classify the medical data with different privacy concerns. The proposed technique makes uses of vertical data partitioning, data merging, integrity checking & hybrid searching to search in plaintext and cipher text. In the given approach statistical analysis & cryptography is used in combination for better flexibility of medical data. It provides hybrid solution for privacy preserving technologies. In future the work can be extended to show hoe performance changes when multiple clients are accessing service simultaneously.
A good method is proposed in [32] of using personal information protection for eID cards. The information stored on the cards is prone to malicious users. With this method the information can be safely stored even when the eID cards is lost. By using these features of proposed method the eID cards can be used in e-passports & in various electronic identification cards of public officials.
A cipher text policy attribute based signcryption [CP-ABSC] scheme is proposed in [33] for cloud system for storing personal health record which gives access control, confidentiality and integrity of data. The proposed method uses smaller cipher text size and also require small pairing computations when compared with the other methods.

Table 5. A Study on security issues specific to applications in cloud computing

Proposed Work	Focus	References
Cipher text policy attribute based cipher text of health records	Security	[28]
Data sharing of Medical data	Security	[29], [30], [31], [33]
Protection of personal Information	Security	[32]

3.6 Measures for security specific to data protection and sharing

An IFC model have been presented in [34] and evaluated the architecture using Cam Flow. The data is controlled in IFC by using information centric MAC scheme which ensure no interference in security. It has made use of Cam Flow platform. The proposed work supports protection of different application from each other. It provides flexible data sharing and it also prevents the leakage of data.
An attribute based data sharing scheme is proposed in [35] to solve the issue of key & to improve the attribute expression in cloud computing. It has also the method of weighted

attribute to increase the expression of attribute so as to reduce the complexity of access policies. The scheme provides high efficiency & security and better performance of security analysis.

A NFV [Network Function Virtualization] is proposed in [36] to identify the security threats and provide measures to overcome those threats. NFV has the advantage of providing software based appliances and using proper cloud computing. In future the work can be extended to implement it using test bed so as to provide good security in NFV.

A new attribute based data sharing scheme is proposed in [37] for resource constrained environment in cloud computing. The computation task is eliminated in proposed scheme by using system public parameters besides of moving partial encryption computation offline. To generate immediate cipher text chameleon hash function is used. The proposed scheme is extremely suitable for resource constrained environment.

A fine grained HER access control scheme is proposed in [38]. In the proposed scheme the owner of HER is able to generate offline cipher text prior to knowledge of EHR data and policies. The proposed system is much appropriate for mobile cloud computing.

A quantum identity based authentication and key management approach is proposed in [39] for cloud server architecture. To provide security and privacy of data quantum cryptography is used which is based on the laws of quantum physics. It also made use of AVISHA tool to enhance security of the method. The proposed method is robust against all types of security threats. Long distance entanglement based QKD expression is also proposed.

A method for sharing the data inside the same group and providing high efficiency and security in the cloud is proposed in [40]. The proposed group data sharing method provides access to multiple users in the public cloud using key agreement method. The group members can communicate with each other using group signature & key is used to enable the members of the group to store their data.

CBIR method is proposed in [41] on encrypted images and prevent leaking of sensitive information to cloud server. The corresponding images are represented by extracting features. To improve the efficiency filters are constructed by locality sensitive hashing. It has made use of watermarking algorithm to identify illegal distributions. In future the work can be extended by using proper watermarking algorithm.

An attribute based data sharing system is proposed in [42] using hybrid combination of CP-ABE & symmetric encryption method. The proposed method provides better computation cost & it is secure in random Oracle model. The method is very much suitable for attribute based data sharing in mobile cloud computing. In future the work can be extended by using CCA2 secure CP-ABE scheme which provides constant computation cost.

A data protection method for cloud storage is proposed in [43] to overcome the challenge of how to protect the cryptographic keys. The proposed method provides following characteristics: -

a] The key used for encryption can be broken only if one of the two factors work.

b] Key separation and proxy re encryption methods can be used to revoke the key efficiently.

c] Attribute based encryption technique can be used to protect the data.

The proposed scheme is secure and efficient as per the performance evaluation.

Table 6. A Study on security issues specific to data protection and sharing in cloud computing

Proposed Work	Focus	References
IFC Model	Security	[34]
Network Function Virtualization	Security	[36]
Attribute based data sharing	Security	[35], [37], [40], [42]
Data protection method	Security	[43]
Authentication and Encryption	Security	[38], [39], [41]

3.7 Measures for security specific to untrusted server and image encryption

Many existing systems depend on the trusted server to collect the spatio-temporal crowd data [56] to disturb the collective statistics by using differential privacy mechanism in order to provide strong privacy. If the server gets hacked the privacy of users will be revealed. This paper studied the problem of real time crowd statistical data publishing for untrusted server. The paper proposed DADP framework which uses multiple agents between user and trusted server. The agent acts as intermediate between user and trusted server to send the information. In order to realize global event differential privacy authors proposed distributed budget allocation mechanism. Authors proposed DADP method for differential privacy for untrusted server and the method is robust.

The alternative to public key encryption is identity based encryption (IBE) [57] while the private key generation in user revocation can be the overhead computation. The authors proposed revocable IBE scheme for outsourcing computation into IBE. The method makes use of key generation operation and key update process. The technique uses hybrid private key for each user using AND gate to bound the identity and time component. The paper also discussed referred delegation model. The efficiency of proposed construction is shown by exhaustive experimental results.

A grouper framework [58] has been presented for developing mobile applications for untrusted cloud servers. The grouper framework makes use of secret sharing scheme to generate the shares and then uploading these shares to untrusted servers. These shares are deleted after certain period of time by self-destruction system of Grouper. The two applications are implemented using grouper framework and the experimental results shows that the performance of Grouper is acceptable for mobile applications.

A method for security feature of SIFT is proposed in [59]. The authors proposed privacy preserving SIFT to solve the problem of feature extraction in encrypted domain. The proposed privacy preserving SIFT is based on homomorphic encryption. The experimental result show that PPSIFT is secure against ciphertext only attack. The homomorphic encryption privacy preserving SIFT performs well when compared to original SIFT.

A scale invariant feature transform SIFT is proposed in [60] for privacy preserving computation over encrypted image data. The proposed method implemented a design for efficient and secure key characteristics. The key is splitted into two protocols for multiplication and comparison thereby distributed on two cloud servers. The experimental results show that the proposed method is more secure as compared to original SIFT.

Table 7. A Study on security specific to untrusted server and image encryption in cloud computing

Proposed Work	Focus	References
Distributed agent-based privacy-preserving framework	Privacy preservation for Untrusted Server	[56]
Identity-based Encryption	Security	[57]
Grouper framework without trusted central servers	Security	[58]
Privacy preserving SIFT	Image Feature Extraction with Privacy preservation	[59]
Securing SIFT	Image Feature Extraction with Privacy preservation	[60]

4. Classification of Security Challenges in Cloud Computing

When multiple users use the resources simultaneously on cloud, the data can be breached easily. So to protect the data on the cloud it is important to fulfil authentication, authorization, confidentiality requirement of data.

Following are some challenges faced by cloud computing: -

4.1 Security of Application Programming Interface [API]

Services and application to be provided to the user is an important requirement for cloud computing. The cloud applications are not bonded to any of its users. Multiple users can use the services simultaneously. The users and services on the cloud is bonded by API's. Security of API is important for data protection and prevention from malicious users.

4.2 Data Access

Users are given access to data according to SLA [Service Level Agreement]. This data is used by a particular user. In order to ensure safe data access various encryption techniques and key management methods are used.

4.3 VM Isolation

Virtual machines running on same hardware must be separated from each other. Although logical separation is already there between VM but still physical separation need to be there since resources are shared among servers and it can lead to data leakage.

4.4 Security and privacy

The security and privacy of data is an important issue in cloud computing. This issue is generally in cloud deployment models. Any information to be stored and retrieved from the cloud must follow certain security mechanisms.

4.5 Data recovery and backup

Due to multitenancy and elasticity the cloud users share resources on the cloud. In case of server failure, the data on the servers can be lost. So data recovery and backup is an important challenge in cloud computing. Replication is a technique to overcome this problem. As if one server fails then data can be recovered from other servers.

4.6 Confidentiality

Confidentiality ensures protection of data from malicious users. The user must be satisfied that his data stored on the cloud is protected against all vulnerabilities and attacks.

4.7 Integrity

Integrity ensures that whatever data is stored on the cloud is not modified or changed. In order to ensure integrity users are advised not to store their passwords and personal data. Only authorized person can modify the data. To follow integrity every transaction on the cloud should follow ACID properties of transaction.

4.8 Availability

Availability ensures that whenever data is required by the user it should be available for user. In several organizations availability is considered a major issue as it totally depends on the agreement between Cloud Service Provider and user.

4.9 Data Breaches

Since large amount of data is stored on the cloud and multiple users access the data stored on cloud, there is a possibility that the malicious user enters the cloud and in that case the cloud is at high risk. So it's an important challenge in field of cloud computing. Example:- weak passwords etc.

4.10 Identity Management

In order to protect data from unauthorized access it is very important to keep track of identity of each and every customer. However, cloud also deals with different authentication and authorization frameworks with same resources simultaneously. The pay as you go feature allows the users to enter and leave cloud frequently. These characteristics enables the need of proper identity mechanisms of user to update the control policies.

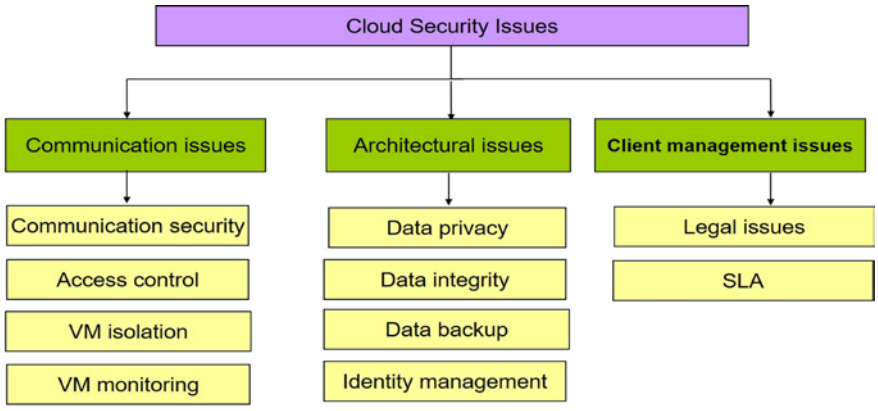

Fig. 2. Classification of Cloud Security Issues

4.11 Service level Agreements [SLA]

SLA is a licensed agreement with terms and conditions to be fulfilled between user and CSP. Continuous monitoring of the agreement is also an important issue because the user cannot fully rely on the statistics provided by cloud service provider. When such conflict occurs between CSP and user then identification of responsibility is also an important issue.

4.12 Legal Issues

Legal issues arise due to conflicting legal jurisdictions and when cloud service provider share resources in different geographical locations because sometimes different data may be present in different location with different digital laws.

4.13 Spectre and Meltdown

Spectre and Meltdown affects modern processors. The malicious hardware enable sthe program to carry off the data processed by the system. Meltdown and spectre can get the secrets of the memory of programs such as passwords in password manager etc.

4.14 DoS Attacks

In denial of service attacks the malicious traffic disable the machine thereby preventing the user from accessing the service. With the use of cryptocurrency the DoS attacks occur more frequently. Example:- botnet floods the targeted system with traffic.

5. Cloud Computing Issues and Study in Literature

5.1 Data Security

In multitenant environment when there are multiple organizations and multiple users the data can be misused or mishandled. To ensure trust of the user, proper security mechanisms should be incorporated to prevent data loss.

5.2 Key Management

Key Management is an important issue in cloud security. If the key used for encryption gets compromised, then stored data might be lost. The key used for encryption/ decryption should be secure to prevent unauthorized access of data. Key size should be large enough to prevent it from breaking.

5.3 Cloud Data Storage

Cloud computing offers a way to store large amount of data. Due to its simplicity multiple organizations are storing their bulk data onto the cloud. Proper confidentiality, integrity, privacy of data should be maintained to prevent loss of data of any individual.

5.4 Data Privacy

To prevent data from unauthorized access privacy should be maintained. The data should ensure authentication & authorization. Proper authentication methods used can ensure data for privacy.

5.5 Anomaly Detection

When talking about data security anomaly detection plays a major role for developing an environment to detect unusual activities in the cloud network. Different anomaly detection mechanisms are used worldwide to incorporate security measures for data on the cloud.

5.6 Vendor Lock-In

Vendor Lock-In is a period of time alotted by cloud service provider to the user using the service. If the user is not satisfied by the services of cloud service provider then he cannot move to another service provider until the lock in period expires. Therefore in cloud computing switching of services is very complex.

Table 8. Summary of cloud computing issues and respective studies in literature

Category	Issues	Recommended Solutions	References
Key Management	Compromised Key, outsider attack, Data Loss	Secret Sharing Schemes, Visual Cryptography, dummy shares, replica keys	[5], [6], [7], [8],[9],[10].[11],[12], [13], [14], [15], [32], [45]
Data Security	Weak key management and cryptographic algorithms, Confidentiality, Access Control, Trust Management	Attribute based encryption, ant colony optimization, Data Classification, trust based mechanism, fuzzy logic, cipher text encryption, genetic algorithm	[9], [11], [17], [18], [19], [20],[21], [23], [26],[27], [28], [29], [30], [31], [34],[37], [41], [45], [46], [47], [56], [57].
Data Privacy	Authentication, Data protection, eavesdropping	Privacy preservation record linkage, trust based mechanism, Multifactor authentication, dynamic programming, role based multitenancy access control, ant colony optimization	[16], [17], [18], [19], [20], [21], [22],[23] [24], [25], [27], [31], [33], [35], [36],[38], [39], [44], [46],[58], [59], [60].
Anomaly Detection	Intruder detection, Compromised Data, DoS Attacks	Naïve Bayes, Decision tree, Dampster Shafer Theory, SNORT, Backpropagation Neural Network, Fuzzy Clustering	[48], [49], 50], [51], [52], [53], [54], [55]
Cloud Data Storage & Sharing	Unavailability of data, access control, storage optimization, Data Loss, Leakage, data security, data breach	Deduplication, Intelligent cryptography for big data storage, Secure Cloud Storage, Probabilistic methods for data classification, compression, attribute based sharing	[21], [22], [26], [27], [36], [37], [38], [40], [42], [43], [44], [45]
Vendor Lock-In	Lack of Interoperability, technical incompatibilities, cost, complexity, lack of portability, Legal Constraints	Standardization of API , Fragmentation., horizontal and vertical integration.	[61], [62],[63],[64], [65]

6. Conclusion and Future Work

Cloud Computing is a latest trend in IT industry. It has many benefits for companies and organizations. Security is a major challenge in cloud because data on the cloud is more prone to attacks. Various researches have showed security challenges, vulnerabilities & attacks in cloud computing. The research paper provides detailed survey for various security challenges in cloud. We have analyzed various characteristics of cloud and the threats related to that. Concurrently many counter measures are also proposed in literature to overcome threats. The tabular analysis reviewed many papers and identified the focus and approach used in existing techniques. Although many methods are given by researchers to ensure security of data in cloud but still there are loopholes. In future work proper key management techniques can be used to distribute keys over different cloud service provider so as to improve the security of data in cloud computing.

References

[1] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Future Generation Computer Systems*, Vol. 28, no. 3 pp. 583- 592, 2012. Article (CrossRef Link).

[2] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of network and computer applications*, Vol. 34, no. 1, pp. 1-11, 2011. Article (CrossRef Link).

[3] P. Mell and T. Grance, "The NIST definition of cloud computing," *NIST special publication*, 800, No.145, pp.7, 2011. Article (CrossRef Link).

[4] D. Fernandes, L. Soares, J.V.Gomes, M.M. Freire, and P. Inácio, "Security issues in cloud environments: a survey," *International Journal of Information Security*, Vol. 13, No. 2, pp. 113-170, 2014. Article (CrossRef Link).

[5] P. Dharani and M.A. Berlin, "Survey on Secret Sharing Scheme with Deduplication in Cloud Computing," in *Proc. of IEEE 9th International Conference on Intelligent Systems and Control [ISCO]*, pp. 1-5. IEEE, Coimbatore, 2015. Article (CrossRef Link).

[6] D. Pal, P.K. Khethavath, P. Johnson and TT. Chen, "Multilevel Threshold Secret Sharing in Distributed Cloud," *Springer International Publishing*, pp. 13–23. Switzerland, 2015. Article (CrossRef Link).

[7] M. Muhil, U.H. Krishna, R.K. Kumar and E.A.M Anita, "Securing Multi-Cloud using Secret Sharing Algorithm," *Procedia Computer Science*, vol. 50, pp. pp. 421 – 426, 2015. Article (CrossRef Link).

[8] R. Ghasemi, A. Saifi, and M.H. Dehkordi, "Efficient multi secret sharing scheme using new proposed computational security model," *Wiley Library*, 2017. Article (CrossRef Link).

[9] J. Wang, C. Huang, N. Xiong, and J. Wang, "Blocked linear secret sharing scheme for scalable attribute based encryption in manageable cloud storage system," *Information Sciences ELSEVIER*, vol. 424, pp. 1–26, 2018. Article (CrossRef Link).

[10] Y. Liu, C. Yang, Y. Wang, L. Zhua, and W. Ji, "Cheating identifiable secret sharing scheme using symmetric bivariate polynomial," *Information Sciences ELSEVIER*, vol. 453, pp.21–29, 2018. Article (CrossRef Link).

[11] M. Deshmukh, N. Nain and M. Ahmed, "Efficient and secure multi secret sharing schemes based on boolean XOR and arithmetic modulo," *Multimedia Tools and Applications*, vol. 77, no. 1, pp. 89-107, 2018. Article (CrossRef Link).

[12] K. Shankar and P. Eswaran, "Sharing a Secret Image with Encapsulated Shares in Visual Cryptography," in *Proc. of 4th International Conference on Eco-friendly Computing and Communication Systems, ICECCS Procedia Computer Science ELSEVIER*, pp. 462 – 468, 2015. Article (CrossRef Link).

[13] K. Brindha and N. Jeyanthi, "Securing Portable Document Format File Using Extended Visual Cryptography to Protect Cloud Data Storage," *International Journal of Network Security*, Vol.19, No.5, pp.684-693, 2017. Article (CrossRef Link).

[14] Jaya, "Securing Cloud Data and Cheque Truncation System with Visual Cryptography," *International Journal of Computer Applications*, Vol. 70, No. 2, 2013. Article (CrossRef Link).

[15] R. Roy, S. Bandyopadhyay, S. Kandar and B. Chandra Dhara, "A Novel 3-4 Image Secret Sharing Scheme," in *Proc. of International Conference on Advances in Computing, Communications and Informatics [ICACCI]*, pp. 2072 – 2075, 2015. Article (CrossRef Link).

[16] R. Shaikh and M. Sasikumar, "Trust Model for Measuring Security Strength of Cloud Computing Service," ELSEVIER *International Conference on Advanced Computing Technologies and Applications [ICACTA] Procedia Computer Science* 45, pp. 380 – 389, 2015. Article (CrossRef Link).

[17] L. Yibin, K. Gai, L. Qiu, M. Qiu and H. Zhao, "Intelligent cryptography approach for secure distributed big data storage in cloud computing," *Information Sciences ELSEVIER*, vol. 387, pp. 103-115, 2017. Article (CrossRef Link).

[18] Y. Zhang, X. Chen, J. Li, D. Wong, H. Li and I. You, "Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing," *Information Sciences ELSEVIER*, vol. 379, pp. 42-61, 2016. Article (CrossRef Link).
[19] F. Zhao, C. Li and C. Lio, "A cloud computing security solution based on fully homomorphic encryption," in *Proc. of 16th International Conference on Advanced Communication Technology IEEE, Pyeongchang, South Korea*, pp. 485 – 488. 2014. Article (CrossRef Link).
[20] J. Yang, J. Li and Y. Niu, "A Hybrid Solution for Privacy Preserving Medical Data Sharing in the Cloud Environment," *Future Generation Computer Systems ELSEVIER*, Vol. 43-44, no. C, pp 74-86, 2015. Article (CrossRef Link).
[21] H. Cui, R.H. Deng, Y. Li and G. Wu, "Attribute-Based Storage Supporting Secure Deduplication of Encrypted Data in Cloud," *IEEE Transactions on Big Data*, 2016. Article (CrossRef Link).
[22] D. Yuan, X. Song, Q. Xu, M. Zhao, X. Wei, H. Wang and H. Jiang, "An ORAM-based privacy preserving data sharing scheme for cloud storage," *Journal of Information Security and Applications ELSEVIER*, vol. 39, pp 1–9, 2018. Article (CrossRef Link).
[23] M. Ali, R. Dhamotharan, E. Khan, S.U. Khan, A.V. Vasilakos, K. Li and A.Y. Zomaya, "SeDaSC: Secure Data Sharing in Clouds," *IEEE SYSTEMS JOURNAL*, VOL. 11, NO. 2, pp. 395-404, 2017. Article (CrossRef Link).
[24] R. Jiang, R. Lu and C.K. Raymond, "Achieving high performance and privacy-preserving query over encrypted multidimensional big metering data," *Future Generation Computer Systems ELSEVEIR*, VOL. 78, pp. 392-401, 2016. Article (CrossRef Link).
[25] Y. Li, Y. Yu, B. Yang, G. Min and H. Wu, "Privacy preserving cloud data auditing with efficient key update," *Future Generation Computer Systems, ELSEVIER*, VOL. 78, pp. 789-798, 2018. Article (CrossRef Link).
[26] M. Usman, M.A. Jan and X. He, "Cryptography-Based Secure Data Storage and Sharing Using HEVCand Public Clouds," *Information Sciences, ELSEVIER*, VOL. 387, pp. 90-102, 2017. Article (CrossRef Link).
[27] S. KS and HR. Divakar, "Flexible and Fine-Grained Attribute-Based Data Storage in Cloud," *IJESC*, VOL. 7, no. 9, 2017. Article (CrossRef Link).
[28] J. Liu, X. Huanga and L.K. Joseph, "Secure sharing of Personal Health Records in cloud computing: Ciphertext-Policy Attribute-Based Signcryption," *Future Generation Computer Systems ELSEVIER*, vol. 52, pp.67–76, 2015. Article (CrossRef Link).
[29] B. Fabian, T. Ermakova and P. Junghanns, "Collaborative and secure sharing of healthcare data in multi-clouds," *Information Systems, ELSEVIER*, vol. 48, pp.132-150, 2014. Article (CrossRef Link).
[30] K.A, Muthukumar and M. Nandhini, "Modified Secret Sharing Algorithm for Secured Medical Data Sharing in Cloud Environment," in *Proc. of Second International Conference on Science Technology Engineering and Management [ICONSTEM] IEEE* Madras, pp. 67 – 71, 2016. Article (CrossRef Link).
[31] Ji. Yang, J. Li and Y. Niu, "A Hybrid Solution for Privacy Preserving Medical Data Sharing in the Cloud Environment," *Future Generation Computer Systems ELSEVIER*, Vol. 43–44, pp. 74-86, 2015. Article (CrossRef Link).
[32] N. Park and D. Lee, "Electronic identity information hiding methods using a secret sharing scheme in multimedia-centric internet of things environment," *Springer-Verlag London*, vol. 22, no. 1, pp. 3-10, 2017. Article (CrossRef Link).
[33] Y.S. Rao, "A secure and efficient Ciphertext-Policy Attribute-Based Signcryption for Personal Health Records sharing in cloud computing," *Future Generation Computer Systems ELSEVIER*, vol. 67, pp. 133-151, 2016. Article (CrossRef Link).
[34] T. Pasquier, J. Bacon and D. Eyers, "Data-Centric Access Control for Cloud Computing," in *Proc. of ACM SACMAT '16 Proceedings of the 21st ACM on Symposium on Access Control Models and Technologies*., pp. 81-88, 2016. Article (CrossRef Link).
[35] S. Wang, K. Liang, J.K. Liu, J. Yu, J. Chen and W. Xie, "Attribute-Based Data Sharing Scheme Revisited in Cloud Computing," *IEEE Transactions on Information Forensics and Security*, Vol. 11, Issue. 8, 2016. Article (CrossRef Link).

[36] M.D. Firoozjaei, J. Jeong, H. Koa and H. Kim, "Security challenges with network functions virtualization," *Future Generation Computer Systems, ELSEVIER*, vol. 67, pp. 315-324, 2017. Article (CrossRef Link).
[37] J. Li, Y. Zhang, X. Chen and Y. Xiang, "Secure attribute-based data sharing for resource- limited users in cloud computing," *Computers & Security, ELSEVIER*, vol. 72, pp. 1-12, 2018. Article (CrossRef Link).
[38] Y. Liu, Y. Zhang, J. Ling and Z. Liu, "Secure and fine-grained access control on e-healthcare records in mobile cloud computing," *Future Generation Computer Systems, ELSEVIER*, vol. 78, pp. 1020-1026, 2018. Article (CrossRef Link).
[39] G. Sharma and S. Kalra, "Identity based secure authentication scheme based on quantum key distribution for cloud computing," *Peer-to-Peer Networking and Applications*, vol. 11, no. 2, pp. 220-234, 2018. Article (CrossRef Link).
[40] J. Shen, T. Zhou, X. Chen, J. Li and W. Susilo, "Anonymous and Traceable Group Data Sharing in Cloud Computing," *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, VOL. 13, NO. 4, pp. 912-925, 2018. Article (CrossRef Link).
[41] Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun and K. Ren, "A Privacy-preserving and Copy-deterrence Content-based Image Retrieval Scheme in Cloud Computing," *IEEE TRANSCATION ON INFORMATION FORENSIC AND SECURITY*, vol. 11, no. 11, pp. 2594-2608, 2016. Article (CrossRef Link).
[42] Y. Zhanga, D. Zheng, X. Chenc, J. Li and H. Li, "Efficient attribute-based data sharing in mobile clouds," *Pervasive and Mobile Computing, ELSEVIER*, vol. 28, pp. 135-149, 2016. Article (CrossRef Link).
[43] C. Zuo, J. Shao, J.K. Liu, G. Wei and Y. Ling, "Fine-Grained Two-Factor Protection Mechanism for Data Sharing in Cloud Storage," *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, vol. 13, no. 1, pp. 186-196, 2017. Article (CrossRef Link).
[44] J. Ru, J. Grundy, Y. Yang, J. Keung and L. Hao, "Providing Fairer Resource Allocation for Multi-Tenant Cloud-based Systems," in *Proc. of IEEE 7th International Conference on Cloud Computing Technology and Science IEEE, Canada*, pp. 306-313, 2015. Article (CrossRef Link).
[45] A. KANAI, N. KIKUCHI, S. TANIMOTO and H. SATO, "Data Management Approach for Multiple Clouds using Secret Sharing Scheme," in *Proc. of International Conference on Network-Based Information Systems, IEEE, Salerno, Italy*, pp. 432 – 437, 2014. Article (CrossRef Link).
[46] Z. Xia, X. Wang, X. Sun and Q. Wang, "A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data," *IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS IEEE*, VOL. 27, NO. 2, pp. 340-352, 2016. Article (CrossRef Link).
[47] L. Tawalbeh,, N. Darwazeh, R. Al-Qassas and F. AlDosari, "A Secure Cloud Computing Model based on Data Classification," in *Proc. of First International Workshop on Mobile Cloud Computing Systems, Management, and Security [MCSMS-2015] Procedia Computer Science*, vol. 52, pp.1153 – 1158, 2015. Article (CrossRef Link).
[48] K. Arjunan and C. Modi, "An Enhanced Intrusion Detection Framework for Securing Net-work Layer of Cloud Computing," *ISEA Asia Security and Privacy [ISEASP] Surat India, IEEE*, pp. 1 – 10, 2017. Article (CrossRef Link).
[49] K. Kumar and V. Mohan, "Performance Enhancement of Intrusion Detection using Neuro - Fuzzy Intelligent System," *Indian Journal of Computer Science and Engineering [IJCSE]*, Vol. 5, No.5, pp. 186-189, 2014. Article (CrossRef Link).
[50] J. JABEZ and B. MUTHUKUMAR, "Intrusion Detection System [IDS]: Anomaly Detection using Outlier Detection Approach," in *Proc. of International Conference on Intelligent Computing, Communication & Convergence [ICCC], Procedia Computer Science ELSEVIER*, vol. 48, pp. 338 – 346, 2015. Article (CrossRef Link).
[51] B. Khadka, C. Withana, A. Alsadoon and A. Elchouemi, "Distributed Denial of Service attack on Cloud: Detection and Prevention," in *Proc. of International Conference and Workshop on Computing and Communication [IEMCON]*, pp. 1 – 6, 2015. Article (CrossRef Link).

[52] K. Angelos, M. Watson, N. Shirazi, A. Mauthe and D. Hutchison, "Malware Analysis in Cloud Computing: Network and System Characteristics," in *Proc. of Globecom-2013 Workshop- Cloud Computing systems, networks and applications*, pp. 482 – 487, 2013. Article (CrossRef Link).
[53] P. Ghosh, C. Debnath, D. Metia and R. Dutta, "An Efficient Hybrid Multilevel Intrusion Detection System in Cloud Environment," *IOSR Journal of Computer Engineering [IOSR-JCE]*, Vol. 16, no. 4, Ver. VII pp. 16-26, 2014. Article (CrossRef Link).
[54] W. Lin, S. Ke and C. Tsai, "CANN: An intrusion detection system based on combining cluster centers and nearest neighbours," *Knowledge-Based Systems*, vol. 78, pp. 13–21, 2015. Article (CrossRef Link).
[55] R.W. Ahmad, A. Gani, S.A. Hamid, M. Shiraz, A. Yousafzai and F. Xia, "A survey on virtual machine migration and server consolidation frameworks for cloud data centers," *ELSEVIER Journal of Network and Computer Applications*, Vol. 52. pp.11–25, 2015. Article (CrossRef Link).
[56] Z. Wang, X. Pang, Y. Chen, H. Shao, Q. Wang, L. Wu, H. Chen and H. Qi, "Privacy-preserving Crowd-sourced Statistical Data Publishing with an Untrusted Server," *IEEE TRANSACTIONS ON MOBILE COMPUTING*, vol. 18, no. 6, pp. 1356-1367, 2018. Article (CrossRef Link).
[57] J. Li, J. Li, X. Chen, C. Jia and W. Lou, "Identity-based Encryption with Outsourced Revocation in Cloud Computing," *IEEE TRANSACTIONS ON COMPUTERS*, Vol. 64, Issue. 2, pp. 425-437, 2015. Article (CrossRef Link).
[58] M. Li and Y. Shinjo, "Grouper: A Framework for Developing Mobile Applications using a Secret Sharing Scheme and Untrusted Servers," in *Proc. of the 2017 VI International Conference on Network, Communication and Computing*. pp. 125-134, 2017. Article (CrossRef Link).
[59] C. Y. Hsu, C. S. Lu, and S. C. Pei, "Image Feature Extraction in Encrypted Domain with Privacy-Preserving SIFT," IEEE *Transactions On Image Processing*, Vol. 21, No. 11, pp. 4593-4607, 2012. Article (CrossRef Link).
[60] S. Hu, Q. Wang, J. Wang, Z. Qin, and K. Ren, "Securing SIFT: Privacy-preserving Outsourcing Computation of Feature Extractions over Encrypted Image Data," *IEEE Transactions on Image Processing*, Vol. 25, no. 7, pp. 3411-3425, 2016. Article (CrossRef Link).
[61] J. O. Martins, R. Sahandi and F. Tian, "Critical Review of Vendor Lock-in and Its Impact on Adoption of Cloud Computing," in *Proc. of IEEE International Conference on Information Society (i-Society 2014)*, 2014. Article (CrossRef Link).
[62] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," *Communications of the ACM*, vol. 53, no. 4, pp. 50-58, 2010. Article (CrossRef Link).
[63] P. F. Hsu, S. Ray and Y. Li-Hsieh, "Examining cloud computing adoption intention, pricing mechanism,and deployment model," *International Journal of Information Management ELSEVIER*, Vol. 34, no. 4, pp. 474-488, 2014. Article (CrossRef Link).
[64] M. A. Morsy, J. Grundy and I. Müller, "An Analysis of the Cloud Computing Security Problem," *ArXiv*, 2010. Article (CrossRef Link).
[65] T. Kurze, M. Klemsy, D. Bermbachy, A. Lenkz, S. Taiy and M. Kunze, "Cloud Federation," in *Proc. of The Second International Conference on Cloud Computing, GRIDs, and Virtualization*, CLOUD COMPUTING 2011. Article (CrossRef Link).

Shahin Fatima is a Phd Scholar from Integral University, Lucknow, India. Her areas of interest include cryptography, cloud computing, computer networks, Wireless Sensor Networks, Database Management System.

Prof. (Dr.) Shish Ahmad is a Associate Professor at Integral University, Lucknow, India. His areas of interest include Computer Networks, Cryptography, Database Management System, Wireless Sensor Networks, Cloud Computing.