Secure and Efficient Privacy Preserving Mechanism in Cloud Computing

Yogendra Singh Rajavat,
Assistant Professor
Prestige Institute of Management Dewas

Dr. Ashish Bansal,
Ex.Professor & Director, School of CS & IT Symboisis University of Applied Sciences,Indore

Sanjay Dubey,
Assistant Professor,
Prestige Institute of Management Dewas

ABSTRACT
Nowadays huge amount of digital data like image, videos and audios are generated which becomes critical task to store those data in disk or mobile phones. So now the people believe on storing their data online which keeps backup of our data or for using it real time, it gives us anywhere and anytime access. The cloud computing provides the platform to store data online. So, the rapid development of it many organizations or enterprises starts storing their outsource data to local cloud server. Though, exposed network and lack of trust cloud on cloud environment, they face huge security and privacy issues such as data disclosure, data loss and user privacy breach when outsourcing their data to a public cloud. To address these issues of cloud computing several solutions were proposed to enable data and privacy protection. This paper presents the survey of the privacy mechanism and also summarizes the literature work done by the various researchers to circumvent the security issues of cloud computing. We first present the services of the cloud computing and characteristics of the it. We then present the earlier work done by the various researchers to overcome the security issues of cloud computing and later then present the privacy mechanism to achieve secure, dependable and privacy-assured cloud data services including data finding, data sharing, data storage, computation and access.
Keywords: Data Security, Data Storage, Cloud Computing, Security, Data disclosure.

1. INTRODUCTION

The layout of the cloud and its data storing potential has massive benefits. Cloud allows to access tremendous resource by the authorized and authenticated cloud users where the resources are shared and outsourced in the cloud. It utilizes the remote resources on the internet. The cloud users can access the cloud at whatever time they require in a simple way with low expenses [11]. Cloud allows the authorized user to access the available resources and also get the rights to share the resources and outsource the resources in the cloud. If the user use the service in the cloud, it is not necessary to possess any software or hardware, the cloud service providers are in charge for installing and maintaining expense for both hardware and software. Even though cloud has many advantages it has some threats that hinder the implementation of the cloud services. Both the pros as well as cloud security challenges are included in these criteria [10]. Cloud computing has many problems, some of them are management of cloud user's identity, support for multi-tendency, requiring security applications, cloud user privacy conserving and achieving the authority over the life cycle of outsource data. Among these issues, conserving the privacy of cloud is reviewed in this paper. It is required to safeguard the cloud user's data and the identity and privacy of the users. The growth of the cloud computing is directly proportional to the responsibility of privacy conserving task [9]. When creating system with taking into consideration all these problems, attackers and the intruders could not be compromised and cannot do anything.

1.1 Background

The Cloud computing service models are divided into three categories as shown in Fig.1 Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) [12] [13].

1) SaaS: Itmakes use of Cloud computing infrastructure for the purpose of delivering one application to many users. It is also called as on demand service. As long as thecomputer has internet connection, SaaS is an application that can be accessed from anywhere in the world. This cloud hosted application is accessed without any additional hardware and software. It also provides security feature like SSL Encryption which is a cryptographic protocol. Examples: - Yahoo Mail, Hotmail, G-Mail.

2) IaaS: It is virtual delivery of computing resources in the form of storage services, hardware and networking. Optionally, it includes distribution of operating systems and virtualization technology to manage the resources. Companies rent these resources as needed, instead of buying and then installing the required resources in their own data center. Examples: - Google Apps, Microsoft Office.

3) PaaS: Cloud Providers deliver a computing platform and solution stack typically including operating system, Database, Web Server, and programming language execution environment. Examples: Windows Azure, AWS Elastic Beanstalk, Force.com, Apache Stratos, Google App Engine.[33]

Fig. 1: Cloud Computing Models

1.2 Cloud Computing Characteristics

Cloud computing systems satisfy many interesting characteristics that make them promising for future IT applications and services. The National Institute of Standard and Technology (NIST) [14] have defined five essential characteristics for cloud computing systems [15,16,17,18,19] and we describe them below:

- *On-demand self-service:* cloud services such as CUP time, Storage, network access, server time, web applications etc can be allocated automatically as required by the consumers without any human interaction.
- *Cost effectiveness:* Services provided by the cloud service providers are very cost effective if not free. The billing model is pay as per usage; there is no need to purchase the infrastructure and therefore lowers maintenance cost. • Broad Network Access (mobility): consumers can access cloud resources over the Internet all the time and from anywhere (i.e., ubiquitous) through different types of devices (e.g., mobile phones, laptops, and PDAs).
- *Resource Pooling:* physical and virtual computing resources are pooled into the cloud. These resources are not dependent on location in the sense that the customer has no control nor has knowledge over their location.
- *Rapid Elasticity:* computing resources can be rapidly and elastically provisioned and released based on the demand of the consumer. Consumers view these resources as if they are infinite and can be purchased in any quantity at any time.
- *Measured Services:* cloud resources and services are monitored, controlled and optimized by the CSPs through a pay-per-use business model. Consumers utilize these services in a way similar to utilizing electricity, water and gas. Other cloud computing characteristics are [20,21]:
- *Multitenancy:* a cloud provides services to multiple users at the same time. Those users share cloud resources at the network level, host level and application level, however, each user is isolated within his customized virtual application instance.
- *Scalability:* the infrastructure of cloud computing is very scalable. Cloud providers can add new nodes and servers to cloud with minor modifications to cloud infrastructure and software. • Reliability: is achieved in cloud computing by using multiple redundant sites. High reliability makes the cloud a perfect solution for disaster recovery and business critical tasks.
- Economies of scale: in order to take advantage of economies of scale, clouds are implemented to be as large as possible. Other considerations are also taken to reduce cost such as locating the cloud close to cheap power stations and in low cost real estate.
- *Customization:* a cloud is a reconfigurable environment that can be customized and adjusted in terms of infrastructure and applications based on user demand.
- Efficient resource utilization: delivering resources only for as long as they are needed allows for efficient utilization of these resources.
- *Virtualization:* Cloud computing makes user gets service anywhere, through any kind of terminal. The resources it required come from cloud instead of visible entity. You can complete all you want through net service using a laptop or a mobile phone. Users can attain or share it safely through an easy way, anytime, anywhere. Users can complete a task that can't be completed in a single computer.

2. RELATED WORK

Author's Name	Description	Years
Dharani, Lakshmi Priya, Nagajothi	Because the lifestyle of the people is changed and they are living in the digitalized world. Many banking applications are existing but still some of them having its own disadvantages. To provide more security and efficiency in transactions we are developing a banking application and also, they were proposing a privacy preserving biometric data in cloud computing. So that bank transactions are made simpler and safer using one individual's biometric data	2019
Imad El Ghoubach , Rachid Ben Abbou, FatihaMrabti	proposed an auditing scheme that provides to users an efficient and secure process to audit their outsourced data. The proposed scheme has a low computation overhead on the users and enables them to delegate the data verification process to a third party auditor while maintaining a low computational and communication overhead without jeopardizing the confidentiality of the stored data	2019
Yongkai Fan, Xiaodong Lin, Wei Liang, Gang Tan, Priyadarsi Nanda	Proposed a TEE (trusted execution environment) based secure deduplication scheme. In our scheme, each cloud user is assigned a privilege set; the deduplication can be performed if and only if the cloud users have the correct privilege. Moreover, their scheme augments the convergent encryption with users' privileges and relies on TEE to provide secure key management, which improves the ability of such cryptosystem to resist chosen plaintext attacks and chosen ciphertext attacks. A security analysis indicates that our scheme is secure enough to support data deduplication and to protect the confidentiality of sensitive data. Furthermore, we implement a prototype of our scheme and evaluate the performance of their prototype, experiments show that the overhead of their scheme is practical in realistic environments.	2019
Bharanidharan M,	Proposed a three-tier cross-domain architecture and an efficient and privacy-	2019

Karunakaran E	preserving big data de duplication is proposed in cloud storage (EPD). EPD achieves both data availability, resists brute-force attacks and privacy-preserving data. In addition, accountability is taken into consideration to offer better privacy assurances than existing schemes. The proposed data de-duplication outperforms existing competing schemes, in terms of computation, communication and storage overheads.	
L. Malina, J. Hajny, P. Dzurenda and V. Zeman	propose a novel privacy-preserving security solution for cloud services. Our solution is based on an efficient non-bilinear group signature scheme providing the anonymous access to cloud services and shared storage servers. The novel solution offers anonymous authentication for registered users. Thus, users' personal attributes (age, valid registration, successful payment) can be proven without revealing users' identity, and users can use cloud services without any threat of profiling their behavior. However, if a user breaks provider's rules, his access right is revoked. Their solution provides anonymous access, unlikability and the confidentiality of transmitted data. They implemented their solution as a proof of concept application and present the experimental results. Further, they analyze current privacy preserving solutions for cloud services and group signature schemes as basic parts of privacy enhancing solutions in cloud services. They compared the performance of our solution with the related solutions and schemes.	2015
B Nareshkumar, G. Ananthanath	In the meantime, the information owner loses the physical manipulate and ownership of information which activates sever a safety risks. Along these strains, inspecting management to test data respectability inside the cloud is fundamental. This issue has turned into a take a look at as the possession of information ought to be confirmed whilst keeping up the privacy. To address those troubles this work proposes at ease and efficient privacy preserving provable information possession (SEPDP). Further, we stretch out SEPDP to assist diverse owners, information elements and cluster affirmation. The maximum appealing component of this plan is that the evaluator can verify the ownership of facts with low computational overhead	2019
Yang et al.	Proposed all the computations and retrieval operations are handled by super stationary peers, while documents are stored in the cloud to achieve high efficiency and security of the index structure. They can also reduce the impact of vehicle dynamics on the information retrieval process in this way. In their system, the indexing efficiency is also improved by utilizing a hybrid indexing structure in which binary trees are nested in a B+ tree. Through security analysis and performance evaluation, they demonstrated that our proposal can achieve acceptable security and efficiency	2018
Yuwen Pu et al.	present two efficient data aggregation schemes to preserve private data of customers. In the first scheme, each IoT device slices its actual data randomly, keeps one piece to itself, and sends the remaining pieces to other devices which are in the same group via symmetric encryption. Then, each IoT device adds the received pieces and the held piece together to get an immediate result, which is sent to the aggregator after the computation. Moreover, homomorphic encryption and AES encryption are employed to guarantee secure communication. In the second scheme, the slicing strategy is also employed. Noise data are introduced to prevent the exchanged actual data of devices from disclosure when the devices blend data each other. AES encryption is also employed to guarantee secure communication between devices and aggregator, compared to homomorphic encryption, which has significantly less computational cost. Analysis shows that integrity and confidentiality of IoT devices' data can be guaranteed in our schemes. Both schemes can resist external attack, internal attack, colluding attack, and so on.	2019

3. PRIVACY IN CLOUD

3.1 Privacy

In general privacy refers the condition or state of hiding thepresence or view. There is a need to attain this state in the places where the confidential things are used such as data and files. In cloud data storage the privacy is need to attain for the data, user identity and on controls. Violation of privacy leads to major failure in the system. To maintain the data privacy, it is possible for a successful deployment and usage of any service.

3.2 Privacy issues in cloud

Data in the cloud data storage has maintained at several distributed locations. CSP is the responsible person to maintain all the data securely. If proper security mechanism is implemented the security is violated at the storage service. Data can be accessed only by the person who is authorized. It is possible in this cloud model a CSP can read the client data for his purpose. Some competitor companies of data owner can give some amount to the CSP and get the access for the data. Internal workers in the CSP organization may access the data and give it to the business

people for money. Government related data files like tender services, investigation documents, property checks may need by the industrialist. So the person contact the CSP and ask for the data. CSP can give it to the person on the basis of money or any other service. Identity of the famous person data like, Prime Minister, world famous sportsman, Actors personal data are accessed by the malicious persons to do such criminal activities. The access of a user is theft for performing some operation using their data. Some attackers are removing the data from the storage. Threats, malicious software are introduced to this storage for gettingaccess and gain knowledge about the data.

3.3 Privacy preservation

Privacy deals with accessibility and availability of sensitive information to the intended recipients. Outsourced data accessed and modified only by the users who are having appropriate access privileges. Consider an organization have prepared and outsource their data in cloud. The outsourced data contents are given to the local administrator to place in cloud. It is recommended to ensure that the administrator cannot view or modify the data contents. After file outsourcing, no one including service provider can view or modify the contents. If service provider or local administrator is trying to read the file contents, it must not be done. Privacy preservation deals with the kind of security in outsourced data. This could be ensured by using Cryptographic techniques.

4. PRIVACY PRESERVING SHCEME OF CLOUD COMPUTING

Data place the major role in the concerned cloud arena. Security issues are arising because of lack in providing secure storage service. Some researchers define and derive some models to preserve the privacy of cloud data storage. The models are as follows:

4.1 Three Layer Architecture

A. Three Layer Privacy

Now the cloud server is divided into three different layers for ensuring the security purpose and to avoid the location awareness. The three different privacy preserving layers are Cloud server, Fog server and Local server. A complete data is now partitioned and stored into three different layers. The ratio of the partition of data is major part of the data is stored in the cloud server, neither high nor low range of data is stored in the fog server and finally lower amount of local server. When the data required it can be combined into a single data using pattern matching method.[22]

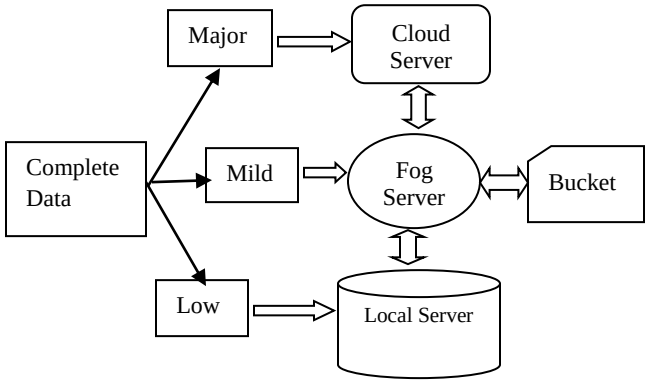

Fig. 2: Three-layer privacy preserving cloud storage architecture [22]

B. Encryption

While uploading the data in three layers, first it is encrypted using Hash Solomon algorithm of encryption. The original data is combined with appending bit and it is encrypted. Now the encrypted data is stored in three layers. When the user requires the complete data, it is decrypted first and combined with the other parts and given to the user as a complete original data.[22]

C. Fog Computing

Fog computing is familiar with cloud computing. It consists of low latency and increasing the geographical range of distribution. Fog computing can perform the data processing and limited storage capabilities. Fog computing consist of three-level architecture, the uppermost is a cloud computing layer, it can be used as storing data and computing data. The middle layer is the fog computing layer. Fog computing layer can perform critical data transmission to cloud server. And finally, the third layer is wireless sensor network layer. This layer's main job is to collect data and upload it to the fog server. In addition, the rate of transfer between the fog computing layer and other layers is faster than the rate between the cloud layer and the lower layer.[22]

4.2Data De-Duplication

In simplified terms, data de-duplication compares objects (usually files or blocks) and removes objects (copies) that already exist in the data set. The de-duplication process removes blocks that are not unique.[4] If you can de-duplicate what you store, you can better utilize your existing storage space, which can save money by using what you have more efficiently. If you store less, you also back up less, which again means less hardware and backup media. If you store less, you also send less data over the network in case of a disaster, which means you save money in hardware and network costs over time. Simply put, the process consists of four steps: (Fig.3)

- Divide the input data into blocks or “chunks.”
- Calculate a hash value for each block of data.
- Use these values to determine if another block of the same data has already been stored.
- Replace the duplicate data with a reference to the object already in the database.

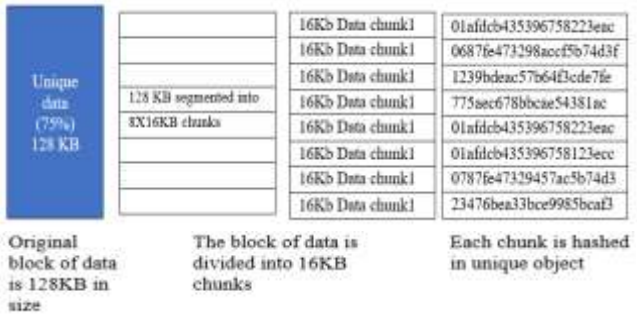

Fig. 3working of de-duplication [4]

Once the data is chunked, an index can be created from the results, and the duplicates can be found and eliminated. Only a single instance of every chunk is stored. The actual process of data de-duplication can be implemented in a number of different ways. You can eliminate duplicate data by simply comparing two files and making the decision to delete one that is older or no longer needed (Fig.4)

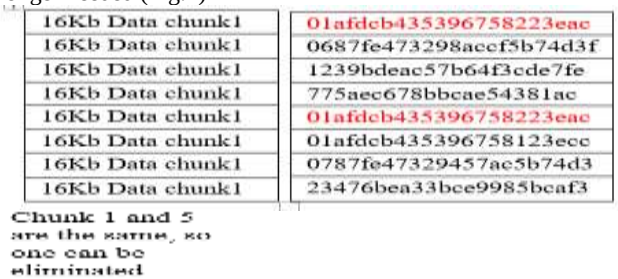

Fig. 4: Replacement of data [4]

4.3 Confidentiality-Assured Cloud Data Service

In public cloud environments, it is necessary to keep data secret while providing normal data utilization services. Encryption is a basic mechanism to enable data confidentiality. However, traditional encryption hampers the data utilization services (e.g., data search and data computation). Intuitively, all the outsourced data may be downloaded and decrypted locally to perform data search or data computation. However, this naive solution is obviously impractical for the reason of prohibitive communication overheads. To achieve confidentiality-assured and effective data services in the cloud, new cryptographic primitives and data encryption proposals have been presented. Specifically, Searchable Encryption (SE) and Homomorphic Encryption (HE) are proposed to offer secure search and computation services.[23]

4.4 Owner-Controlled Cloud Data Sharing

In untrusted cloud environments, a challenging problem is to enable fine-grained enforcements of data access and achieve secure data sharing among large-scale users. Obviously, since an owner does not trust the cloud, traditional access control mechanisms, normally depending on a trusted server, are not suitable for cloud data sharing. To address this challenge and enforce owner-controlled access control, data should be encrypted by the owner before outsourcing it to the cloud, and then the owner can perform fine-grained access control over the encrypted data by securely distributing keys. Based on this idea, access control based on encryption is proposed. Two typical mechanisms in this direction are access control based on selective encryption [24] and Attribute- Based Encryption (ABE) [25], respectively.

4.5 Public Key based Homomorphic Linear Authentication (HLA)

This scheme presents Privacy Preserving and Public Auditing for Data in Cloud Storage. Data Security is a major issue in Cloud computing that needs to be considered. The users store their data in file server without keeping local copy in the cloud where they cannot trust the clients and unreliable server. Hence, it is very important that the client should be able to verify the integrity of the data stored in remote server [26]. The users should be able to detect modification in any part of client's data, if server modifies; furthermore, the third-party auditor must also be able to detect it. This method allows verifying data integrity and its correctness on cloud using Third Party Auditor [27]. It achieves privacy preserving data security using public key-based HLA protocol with random masking. And hence, client can easily trust the service provided by cloud, as TPA works on behalf of cloud user. The data will be kept private against the third-party auditor, even while verifying the integrity of the client's data [28] [29][30].

4.6 Cryptographic Techniques for Data Security in Cloud Computing

Cryptographic technique presents data integrity verification in Cloud Storage without using Trusted TPA (TTPA). TTPA is an independent component which is trusted by both cloud users and service provider. Even though TTPA is reliable, there exist few issues such as leakage of data, scalability, accountability, performance overhead, dynamic data support etc [31]. In cryptographic algorithm, there are two types of key: symmetric key and asymmetric key for encryption and decryption of data. Data security and integrity verification is achieved using Hash Function. Algorithms such as RSA and DES are used for encrypting and decrypting data and then hash code is generated using hash function. Data owner encrypts the file, generates signature using hash function and uploads to cloud. Whenever the owner wants to modify data, a request is sent to service provider. Service provider generates hash code data for encrypted file, decrypts it and sends it to data user [31] [32]. Hash functions such as MD5, SHA1, SHA2 and SHA3 are used for data correction and integrity verification. [30]

4.7 Privacy-Preserving Public Auditing for Secure Cloud Storage

Using Cloud Storage, users can remotely store their data and enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in Cloud Computing a formidable task, especially for users with constrained computing resources. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a third-party auditor (TPA) to check the integrity of outsourced data and be worry-free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user. In this paper, we propose a secure cloud storage system supporting privacy-preserving public auditing. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient.

5. CONCLUSION

Due to the availability of huge data over internet or online security and privacy becomes the critical issues for the cloud computing. For providing security and privacy to our digital data several state-of-the-art securities solutions have been anticipated for protecting the outsourced data and user privacy. In this survey, we review these solutions in the literature and also discuss the privacy mechanism that provide data confidentiality, integrity, access control and preservability for cloud services. In this survey, we find that most of the privacy scheme achieving a trade-off between security and functionality while some improves the performance of the cloud services and also reduces the computation time but they increase the bandwidth cost, storage overhead and complexity so as to enhance their practability. So, in future work we need to design such hybrid privacy mechanism which will provide more security and privacy to our data over cloud together with reducing the storage overhead, computation time and bandwidth cost.

Reference

[1]. Dharani, Lakshmi Priya, Nagajothi (2019). A Novel Privacy Preserving Biometric Identification Scheme in Cloud Computing. International Journal of Innovative Research in Science, Engineering and Technology, Vol. 8, Issue 2, February 2019, pp 1399-1404.

[2]. Imad El Ghoubach , Rachid Ben Abbou, FatihaMrabti, (2019). A secure and efficient remote data auditing scheme for cloud storage. Journal of King Saud University – Computer and Information Sciences xxx (xxxx) xxx.

[3]. Yongkai Fan, Xiaodong Lin, Wei Liang, Gang Tan, Priyadarsi Nanda, (2019). A secure privacy preserving deduplication scheme for cloud computing. Future Generation Computer Systems 101 (2019) 127–135.

[4]. Bharanidharan M, Karunakaran E, (2019). An Efficient Privacy-Preserving Data De-Duplication in Cloud. International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 8 pp. 1798-1804.

[5]. L. Malina, J. Hajny, P. Dzurenda and V. Zeman, (2015). Privacy-preserving security solution for cloud services. Journal of Applied Research and Technology, Vol.13,20-31.

[6]. B Nareshkumar, G. Ananthanath, (2019). Secure and Efficient Privacy Preserving Provable Data Possession in Cloud Storage. International Journal for Scientific Research & Development| Vol. 7, Issue 01, 2019, 857-861.

[7]. Kai Fan, Xin Wang, Katsuya Suto, Hui Li, and Yintang Yang, (2018). Secure and Efficient Privacy-Preserving Ciphertext Retrieval in Connected Vehicular Cloud Computing. IEEE Network • May/June 2018, 52-57.

[8]. Yuwen Pu et al., (2019). Two Secure Privacy-Preserving Data Aggregation Schemes for IoT. HindawiWireless Communications and Mobile Computing Volume 2019,1-11.

[9]. Security and Privacy in Cloud Computing, IEEE Communications Surveys & Tutorials, vol PP(99), 1–17.

[10]. Takabi H, (2010). Beyond lightning: A survey on security challenges in cloud computing, Computers & Electrical Engineering, vol 39(1), 47–54.

[11]. Xiao Z, and Xiao Y. Security and Privacy Challenges in Cloud Computing Environments. IEEE Security & Privacy, vol 8(6), 24–31.

[12]. Pradeep Kumar Tiwari1 and Dr. Bharat Mishra, (2012). Cloud Computing Security Issues, Challenges and Solution. International Journal of Emerging Technology and Advanced Engineering, Vol 2, Issue 8.

[13]. Subashini S and Kavitha V, (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and computer Applications.

[14]. NIST, http://www.nist.gov/itl/cloud/index.cfm

[15]. GTSI Group, "Cloud Computing - Building a Framework for Successful Transition," White Paper, GTSI Corporation, 2009.

[16]. T. Dillon, C. Wu and E. Chang, (2010). Cloud Computing: Issues and Challenges. 24th IEEE International Conference on Advanced Information Networking and Applications.

[17]. P. Mell and T. Grance, (2011). The NIST Definition of Cloud Computing. Recommendation of NIST, Special Publication 800- 145, http://csrc.nist.gov/publications/nistpubs/800-145/SP800- 45.pdf

[18]. Z. Wang, (2011). Security and Privacy Issues Within Cloud Computing. IEEE Int. conference on computational and information sciences, Chengdu, China.

[19]. Ahmed Youssef and Manal Alageel, (2011). Security Issues in Cloud Computing. In the GSTF International Journal on Computing , Vol.1 No. 3, 2011.

[20]. Dimitrios Zissis and DimitriosLekkas, (2012). Addressing cloud computing security issues. Future generation Computer Systems 28, pp. 583-592.

[21]. Rajnish Choubey, Rajshree Dubey and Joy Bhattacharjee, (2011). A Survey on Cloud Computing Security, Challenges and Threats. International Journal on Computer Science and Engineering (IJCSE), vol. 3, No. 3.

[22]. M. Preetha, G. Pravinkumar, S. Sabarinathan, (2019). Three-Layer Privacy Preserving Cloud Storage Scheme based on Computational Intelligence in Fog Computing. International Journal for Research in Applied Science & Engineering Technology (IJRASET) Volume 7 Issue III, ISSN: 2321-9653.

[23]. JUN TANG et al., (2016). Ensuring Security and Privacy Preservation for Cloud Data Services. ACM Computing Surveys, Vol. 49, No. 1, pp 1-39.

[24]. Sabrina De Capitani Di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, and PierangelaSamarati, (2010). Encryption policies for regulating access to outsourced data. ACM Transactions on Database Systems (TODS) 35, 2, 12.

[25]. Amit Sahai and Brent Waters, (2005). Fuzzy identity-based encryption. In Advances in Cryptology (EUROCRYPT' 05). Springer, 457–473.

[26]. M.Priya, E. Anitha and V.Murugalakshmi, "Privacy Preserving Public Auditing for Data in Cloud Storage", International Journal of Innovative Research in Computer and Communication Engineering, Vol 2, Issue 1, 2014.

[27]. K Govinda, V. Gurunathprasad and H. Sathishkumar, "Third Party Auditing for Secure Data Storage in Cloud Through Digital Signature Using RSA", International Journal of Advanced science and Technical Research, Vol 4, 4 August 2012.

[28]. Maha TEBAA, Said EL HAJJI and Abdellatif EL GHAZI "Homomorphic Encryption Applied to the Cloud Computing Security", Proceedings of the World Congress on Engineering, 2012.

[29]. Abhishek Mohta, Lalit Kumar Awasti, (2012). Cloud Data Security while using Third Party Auditor. International Journal of Scientific & Engineering Research, Vol 3, Issue 6,1-4.

[30]. Pooja HP, NagarathnaN,(2015). Privacy in Preserving Issues and their Solutions in cloud Computing - A Survey. (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (2) , 1588-1592

[31]. Rana M Pir, (2014). Data Integrity Verification in Cloud Storage without using Trusted Third Party Auditor. IJEDR, Vol 2, Issue 1.

[32]. K. Raen, C. Wang, Q. Wang, (2012). Security Challenges for the Public Cloud. Published by IEEE Computer Society, Jan/Feb 2012.

[33]. Harsh Pratap Singh, Dr Jitendra Sheetlani, Rashmi Singh, (2018). Cloud Computing Security Issues, Challenges and Solutions. International Journal of Innovation in Engineering Research and Management, Vol.5, issue-01. ISSN 2348-4918