JCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-6, Issue-12, Dec 2018 E-ISSN: 2347-2693

Comparative Analysis of Different Cryptographic Mechanisms of Data Security and Privacy in Cloud Environment

Manreet Sohal[1*], Sandeep Sharma[2]

[1,2]Dept. of Computer Engineering & Technology, Guru Nanak Dev University, Amritsar-143005, India

Corresponding Author: manreet.cetrsh@gndu.ac.in

Available online at: www.ijcseonline.org

Accepted: 06/Dec/2018, Published: 31/Dec/2018

***Abstract*—** Cloud computing is an internet-based service which provides a platform based upon the internet for performing computations. In other words, it is the hiring of services from the service providers. But, since data has to be stored at the third party location, the data owners are always concerned about the security of their data. There are a number of security issues related to cloud computing. In this paper, a comprehensive review of various security challenges faced by the cloud has been presented. The major focus of this paper is the security of the data stored on the cloud. We have provided a detailed discussion on various cryptographic algorithms that have been proposed in recent years to ensure data security. These algorithms have been compared and analyzed based upon various security parameters and their pros and cons have been highlighted. This analysis opens up a new space that can be used to develop a new algorithm which can overcome the shortcomings of the existing algorithms and can enhance the security of the existing systems.

***Keywords*—**Cloud Computing, Security, Privacy, Encryption, Decryption.

I. INTRODUCTION

In early 60's, the computers occupied large rooms and had high electricity consumptions, expensive electronic parts and very low processing powers. In due course of time, the smaller computers replaced them. By the end of the previous century, the distributed systems started evolving to provide greater efficiency [1]. In recent years, with the increase in requirements of data and online users, the conventional infrastructure has become costlier and difficult to handle. Conventional computing is not appropriate for anytime, anywhere access of data, for doing so, the data is required to be stored on an external storage system. Moreover, the traditional technology cannot handle the increasing number of online users on networking site, internet surfing, video conferencing etc [1]. This swift increase in global internet usage has moved us towards cloud computing for managing volume, variety and availability of data. In this modern era, cloud computing has become the hottest technical topic. It is thought as the future or the next generation paradigm of computing for allowing suitable, on- demand network access to the shared computing resources.

According to National Institute of Standards and Technology(NIST), cloud computing is defined as: "Model for enabling convenient, on-demand network access to a shared pool of configurable computing resources(e.g. networks, servers, storage, applications and services) that can be rapidly provisional and released with minimal management effort or service provider interaction"[2]. In this context, cloud computing moves up its users to the abstraction level where hardware and software infrastructure details are hidden from the users. This definition highlights three major key points; First NIST delineates the growth of technologies that hold up a ubiquitous, universal and relevant business model [2]. Second, it shows up the significance of network access systems to resources that are shared and that leads to interaction between Cloud Service Providers (CSP) and their clients. Third, the emphasis has been laid on the price model which permits the users to pay as per the resource consumption [2].

With cloud computing, scalable services are facilitated to be used up over the internet and the processing of users' data takes place on the remote machine [3, 4]. Virtualization, Service Oriented Computing, Utility Computing, Load Balancing, Multi-tenant Environment (sharable resources), Elasticity (increasing or decreasing users resources as per need), Scalability(tendency to range to thousands of systems), the ability of pay per use are some of the technologies responsible for the great success of cloud computing [5].

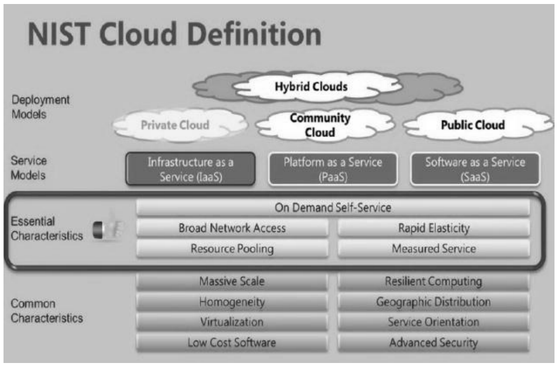

Figure1. Definition of cloud computing according to NIST [2]

There are three service models and five deployment models offered by cloud computing as shown in Fig. 1. These are discussed in detail in the following sections.

A. Cloud Service Models

The services provided by the clouds have been classified into three categories, namely: Software as Service (SaaS), Platform as Service (PaaS) and Infrastructure as Service (IaaS) [2]. These services are described as follows:

***1) SaaS**:* SaaS allows the customers to utilize the applications of Cloud Service Provider (CSP), running on cloud infrastructure through the internet. The applications can be accessed by making use of thin client interface. SaaS does not facilitate the development of software and an application. It only makes the software available that can be accessed via the internet. Thus, it is a model in which software is distributed through the web. The software is not owned by the customers, instead of that, customers pay for the software as per their usage [4, 6].

2) PaaS: This service provides a framework, where the applications owned by the customers can be managed and executed. The services offered by PaaS incorporates operating systems, platform layer resources, integrated development environment (IDE) etc. The control of the underlying cloud infrastructure is not provided to the customers, they have a control of only their applications that are shifted to the cloud [4, 6].

3) IaaS: This service provides hardware infrastructure such as network, storage, memory, processor and several other computing resources. The resources are offered as virtualized systems and can be accessed via the internet. The underlying resources are under the control of the CSP [4, 6].

B. Cloud Deployment Model

There are four cloud deployment models. These are as follows:-

1) Public Cloud: In this type of cloud, the cloud infrastructure is publically available and the organization selling cloud services i.e CSPs own it [3]. The customers share the resources and pay to the CSPs on the basis of what resources and services have been utilized by them. The physical infrastructure is off premises and controlled by CSP [6].

2) Private Cloud: Management of private cloud is done for a single organization and is available for that organization only. Its management may be done by the organization or by the third party and it may be present on premise or off premise [3]. The physical infrastructure of the cloud may or may not be owned by the organization. Private cloud's resources and services can be utilized by the single organization only. Any of the other customers cannot consume these resources [6].

3) Community cloud: This cloud's infrastructure is owned and shared by a group of organizations or customers forming the community [3]. The common interests of the community such as goal, policy, security requirements etc, are same. Any one of the organizations from the community or a third party may control this type of cloud.

4) Hybrid clouds: The cloud infrastructure is the combinations of two or more clouds (private, hybrid or community) [3].All of the clouds who are participating in the hybrid cloud formation maintain their unique properties but the proprietary and standardized technology is shared by them [6].

Besides having multiple advantages, there are many issues that act as a hindrance in the way of wide adoption of cloud computing [6]. This paper discusses about the various security issues present in cloud computing and various cryptography algorithms proposed in literature to provide data security. A comparative analysis of these algorithms has been done based upon their merit and demerits and based upon various security parameters.

The sectional Breakdown of this paper is as follows: Section 2 discusses about the various security issues faced by cloud environments, Section 3 discusses various cryptographic algorithms present in literature to ensure cloud data security, Section 4 provides comparative analysis of these algorithms and Finally, Section 5 concludes this paper.

II. SECURITY ISSUES IN CLOUD COMPUTING

As cloud computing encompasses several technologies like networks, databases, operating systems, load balancing, transaction management [3], virtualization, resource scheduling etc, there are many issues with this technology [3]. For example, in order to interconnect systems in the cloud, the interconnection needs to be established over a secure network. In addition to this, the virtualization approach leads to several security concerns such as it is required to securely map from virtual machines to physical machines. Encryption of data and enforcement of suitable policies of data sharing comprises data security. The security of memory management and resource allocation algorithms is required. For malware detection, data mining techniques are required to be applied [3]. According to the 2015 Cloud Adoption Practices & Priorities Survey Report presented by the Cloud Security Alliance (CSA), data security concerns is the topmost challenge faced by the cloud project (Fig. 2).

When using cloud computing at all levels i.e IaaS, PaaS and SaaS data security becomes very crucial. Cloud Security has to penetrate to the data level to gain the confidence of the enterprise that their data is safe in the cloud during its life cycle. Data lifecycle consists of six phases: Create, store, use, share, archive and destroy. Once data is created, without any restriction, it can move between these phases and may not go through all the phases. Security of data in cloud computing covers data in transit, data at rest, data processing, data lineage, data provenance, and data remanence [3].

At present times, the cyber warfare is debatably intricate challenge faced by multitenant and distributed environments. While transferring data to the cloud, the need of security should be the most essential concern. The European Network Information Security Agency (ENISA) catalogued various threats, suggestions and benefits for the cloud computing [8]. It also enlists the infection on confidential documents, loss of governance, malicious insiders and insecure incomplete data.

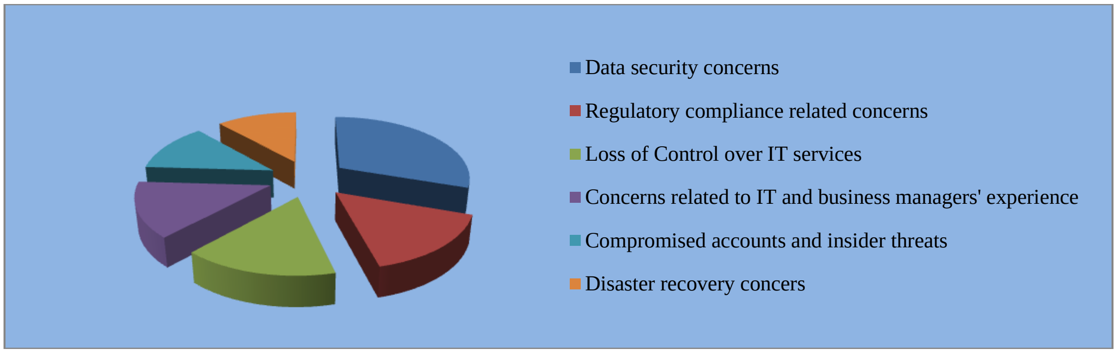

Figure 2. Top challenges faced by cloud projects [7]

Further, the 2015 shadow data report by Elastic [9] emphasize on the unauthorized sharing apps and inspects the type of data these apps are using, the most precarious exposures and the steps to be taken to alleviate these problems.
According to the survey conducted by the Cloud Security Alliance (CSA) in 2013[3, 6], there are nine major threats known as notorious nine, that impact the services of the cloud. These threats are described below:

1) Data Loss**:** This type of problem occurs quite often. The data may be lost due to several reasons such as accidental modification and deletion of data without having any backup, physical disasters like fire, earthquake etc, erasing of data from the cloud by malicious users, loss of encryption key of the data by the customers etc [3, 6].

2) Account Hijacking**:** It takes place when an attacker/criminal gains access to the personal information/credentials of the users. With the help of this stolen information, the attacker can access critical areas of the data and services of the cloud environments. He can also keep track of users' activities and can even redirect them to illegal sites and urls. He can also make user's accounts as a base to perform further attacks [3, 6].

3) Data Breaches: In order to lessen the effect of data breaches, the best way till now is encryption. But, the data in this case, will also be lost if the key is lost. If there is a mistake in the application of one client, the attacker can obtain access to not only that client's data but also to the data of all other clients, which is stored on that machine [3, 6].

4) Denial of Service (DOS) attacks: Denial of service (DOS)/ Distributed denial of service (DDOS) attacks are a try of making network's or machine's resources unavailable to the intended users. In such types of attacks, a large number of requests flood the services so that it becomes unavailable for the authorized users. An advanced version of DOS is DDOS in which attacks are transmitted from different dynamic networks which have been compromised, unlike the DOS attacks. DDOS attackers are tempted to a large extent by the services of the cloud. Therefore, their center of attention is primarily on private data centers [3, 6].

5) Malicious Insiders: A malicious insider is an inside threat such as an employee of an institution or business. It can also be an outsider who masquerades as an employee by acquiring fake credentials. The hacker gains access to the networks and computer systems of an enterprise and performs activities that are harmful to the enterprise [3, 6].

6) Cloud Services' Abuse: With the simple registration process anyone can immediately start using cloud services such as registration with any valid credit card etc. By making the adverse use of relative ambiguity behind such registration and usage models, the spammers, malicious code authors etc are able to perform malicious activities like cracking of passwords and keys, DDOS attacks, hosting malicious data, launch dynamic attack points etc [3, 6].

7) Lacking due Diligence: This case occurs when the organization starts using cloud services without fully understanding the cloud environment and risks related to it. This gives rise to operational and architectural issues and issues related to contracts over legal responsibility and transparency [3, 6].

8) Issue due to Sharing of Technology: By making use of the shared technology feature, the attacks can expand to a large extent in the cloud environment. All types of shared technology like disk partition, CPU caches etc are targeted under this type of threat [3, 6].

9) Insecure APIs: An attack may begin at the network level with flood attacks like DNS attacks, ICMP attacks etc and can then shift to the application layer with attacks like Dos attacks, cross-site script attacks etc. Once the system is infected, data is the next target of the attacker. The security of the basic APIs determines the security and availability of cloud services. These interfaces are developed to provide protection, right from the access control and authentication to the activity supervision and encryption, against both accidental and malicious attacks [3, 6].

In 2016, CSA came up with a new list of threats called the Treacherous Twelve (shown in Fig. 3) in which it added 3 new threats that affect cloud services. These new threats have been explained below:

***10)Insufficient Identity, Credential and Access Management*:** Insufficient Identity, Credential and Access Management permits unauthorized data access and potentially cataclysmic harm to the end user and organizations [11]. Under this threat, the attackers masquerade as legitimate operators, developers and users to read, alter and delete the data and to sneak into the data in transit and liberates malicious software as if it has been originated from a legitimate source.

***11)System Vulnerabilities**:* These are the susceptible bugs at program levels that make the system vulnerable to attacks. Taking advantages of these bugs the attackers can penetrate into a system and can steal the data, upset the operations and can take over the control of the system [11]. If these vulnerabilities are present in the operating system, it places data and entire services at considerable risks.

12)Advanced Persistent Threats (APTs): These are the cyber attack that penetrates into the systems to set up a bridgehead in the IT infrastructure of the bull-eyed [11] companies from which the data has to be stolen [11]. APTs follow their objectives cautiously over longer periods of time, frequently making adaptations to the suitable measures that have been taken to defend them. Once API's set them at proper positions, they can progress creatively through networks of data centers and can intermingle with the usual network traffic to accomplish their goals.

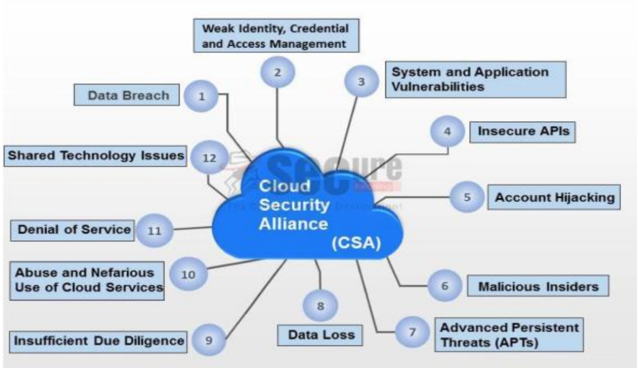
Weak Identity, Credential and Access Management
2
System and Application Vulnerabilities
3
Data Breach
1
4
Insecure APIs
Shared Technology Issues
12
Cloud Security Alliance (CSA)
5
Account Hijacking
Denial of Service
11
Abuse and Nefarious Use of Cloud Services
10
6
Malicious Insiders
8
Data Loss
7
Advanced Persistent Threats (APTs)
Insufficient Due Diligence
9

Figure 3. Twelve major cloud security threats according to CSA [11]

Further, the CSA have laid emphasis on security in the following domains:

- *Governance and Enterprise Risk* Management [3]: It focuses on recognizing and implementing the appropriate organizational structure, process, and controls to retain effectual governance of information security and risk management. The function of the organization in guarantying information security is also highlighted in this domain [3].

- *Information Management and Data* Security [3]: Due to the migration of organizations and companies towards cloud computing, the traditional methods of information security are checked by cloud-based architectures. Features of clouds like elasticity, multi-tenancy, new architectures, abstracted controls etc require the implementation of new data security strategies and technical architectures [3].

- *Disaster Recovery, Continuity of Business and Traditional Security* [3]: The major aim of this domain is to make the roles of traditional security clear to the cloud users. Traditional security includes measures to ensure the safety and existence of data and personnel against theft, sabotage, spying etc [3].

- *Incident Response (IR)* [3]: It is the foundation of information security. This domain tends to search for the gaps related to IR, created by distinct features of cloud computing. It may be used by security professionals for creating response plans and carrying out other activities during the preparation stage of IR lifecycle [3].

- *Application* Security [3]: This domain concentrates on fields like secure Software Development Life Cycle (SDLC), application security architecture in clouds, cloud encryption in an application based on cloud, malicious software avoidance, authentication, compliance and risk management of applications etc [3].

- *Encryption and Key Management* [3]:This domain emphasizes on encryption of data transmitted to the cloud. It also involves the concerns about the encryption for transmitting unsecured data outside the organization. This domain also emphasizes on cloud database encryption for the purpose of hiding it from database privileged users. The value of encrypted data is negligible unless a proper key management is taken into account. Therefore this domain also takes care of protecting the key and storage [3].

- *Entitlement, Identity, and Access Management* [3]: This domain emphasizes on using different sources of identity and attributes related to them in cloud applications [3].

- *Security as Service (Secaas)* [3]: It is different from normal cloud security. It is cloud-based model for offering security solutions. Security offerings provided by the cloud can be evaluated by cloud consumers [3].

This paper emphasizes on Information Management and data security, and Encryption and Key Management domains of cloud security. In the following sections various encryption techniques have been discussed and their contribution towards information and data security has been analyzed and compared.

A. Security Requirements of Cloud Deployment and Service Models

In Table 1. Six major security requirements of different types of clouds have been described. It is clear from the table itself that in order to avoid unauthorized access to the valuable information, authorization requirements are obligatory. Hybrid clouds are more secure than public and private clouds. Therefore, security requirements for hybrid clouds are less. Integrity is the most wanted security requirement among all the deployment models i.e finding of the correctness of data whether it is corrupted or not. Further, it is indicated that most of the requirements lie in SaaS model which leads to concerns about the service and web-based access of applications in SaaS [12].

Table 1. Requirements of cloud deployment and service models

Security Requirements	**Public Cloud**			**Private Cloud**			**Hybrid Cloud**		
	SaaS	**PaaS**	**IaaS**	**SaaS**	**PaaS**	**IaaS**	**SaaS**	**PaaS**	**IaaS**
Identification and authentication	Y	N	Y	Y	N	Y	Y	N	N
Authorization	Y	Y	Y	Y	N	N	Y	N	N
Confidentiality	Y	N	N	Y	Y	N	Y	N	N
Integrity	Y	N	Y	Y	Y	N	Y	Y	Y
Non-repudiation	Y	N	N	Y	N	N	N	N	N
Availability	N	Y	Y	Y	Y	Y	N	N	N

III. CRYPTOGRAPHIC SECURITY TECHNIQUES AVAILABLE IN LITERATURE

In this section we have discussed various cryptographic algorithms that exist in literature in the field of cloud computing security. The selection criteria adopted for choosing the techniques for reviewing is based upon the year of publication (2014-2018) and number of citations. We have tried to incorporate the most recent and quality work done in this field. Since, there are rapid changes in the technology, so we have tried to pick up the latest papers. These papers have been discussed below and we have named them as $T_{1,}$ $T_{2......}$ T_{20} for ease of reference while using in comparison tables.

T_1:- "Data security and integrity in cloud computing based on RSA partial homomorphic and MD5 cryptography" [13]. In this technique, before uploading; the data is encrypted using RSA Partial Homomorphic algorithm. Then associated with the file, public and private key pair is generated. Once the file is uploaded, the data owner receives information like date and time when the file is uploaded and the hash value of the file. After uploading to the cloud servers, for security and verification purposes hash value is calculated by the CSP using MD5 hashing scheme and is sent to the data owner for verifying [13]. For verifying their data, data owners can request for verification option. Then at that time the hash value of the data on the cloud is calculated and is sent to the data owner. If it matches with the old hash value already present with data owner no modification has been done to the data. The output is obtained in the form of a report. The users receive files in an encrypted format and they can only decrypt it using private keys. During decryption, an access file is also uploaded which has information regarding authorized users. It provides two-fold access control mechanism one through authentication and other through private keys [13].

T_2:- "Enhancing Distributed Data Storage Security for Cloud Computing Using TPA and AES Algorithm" [14]. In this paper, file distribution across various servers has been discussed. The hash value of each block is calculated using SHA-1 scheme [14]. This scheme generates a fixed hash value of size 20 bytes. Therefore, it is faster as compared to other techniques like token generation etc. Data is encrypted using Advanced Encryption Standard (AES). It is a symmetric block cipher which uses the same key for encryption as well as decryption. In this technique, AES uses 128-bit key size instead of 192 and 256 bit because computation complexity of this size is less as compared to other key sizes. A third-party auditor is used for auditing the outsourced data and ensures its security. Then, the Correctness verification & error localization algorithm is run to find out if any changes are made to the file and by which server. All parts of the file are obtained from different servers and then a backup file is fetched from the backup server. The hash value of each file part is compared with the backup file. If the value is different, changes have been made to that part of the file and the misbehaving server can be found. Then, Error recovery algorithm is executed, once the corrupted file part is found, it is replaced by original file part from the backup server [14]. The results have shown that the presented system is greatly efficient against server collusion attacks and against modification of data by malicious users. Performance evaluation has proved that the proposed approach is highly secure and efficient.

T_3:- "Enhanced Attribute Based Encryption for Cloud Computing" [15]. In this paper, an enhanced ABE is used for the real-time systems. It uses digital signatures and hash functions. Access structure used in this approach provides controlled access to the genuine users. This access is provided on the basis of certain roles and attributes. Dual authentication is used with the digital signature and the public key. When the user requests for a particular file, based on the public key and access structure, a decision is made whether to allow or restrict the user. If the user is allowed then the master secret key is generated. Based on the private key of the user and the secret key generated, a digital signature is formed. Once secret key is generated by the CSP, an id is created. This id needs to match with the id of the user's private key. Finally, the decryption is performed and the plain text is provided to the user based upon the access privileges. It has been proved that the access time of the proposed scheme has been reduced and it is highly cost effective [15].

T_4:- "Enabled/disabled predicate encryption in clouds" [16]. In this paper, a timed-release (enabled) services and data self-destruction (disabled) schemes have been provided [16]. The readable/unreadable time for the file to be sent is set by the sender. The receiver can only decrypt and read the file after readable time. After unreadable time, the structure of the file gets destructed. Furthermore, the length of the encrypted message is independent of the order of the group. The undecryptable search has also been provided in this algorithm [16]. The authors have claimed that the proposed model is appropriate for encrypted data search on cloud.

T_5:- "An efficient certificateless encryption for secure data sharing in public clouds" [17].In this technique, data is encrypted by the data owner using symmetric encryption algorithm. Based upon the access control policies and the symmetric data encryption, keys are encrypted using public keys generated by key generator center residing in cloud i.e. using mcl-PKE [17]. Then, the data is uploaded on the cloud. Key generation center in this approach is present in public cloud. Therefore, the key management task of the organizations is simplified. The complete private key of the users in conventional CL-PKE includes a user-generated secret key and a partial private key produced by key generator. But, in this approach partial private key lies with a semi-trusted Security Mediator (SEM) [17]. Therefore, the user's request for accessing the data goes via SEM which

checks prior to decryption, whether the user is revoked or not. This security mediator acts like a point of policy enforcement and in addition to that, offers immediate revocation of malicious users. If a number of users have been authorized for accessing the same data, the data encryption key is encrypted only one time by the data owner but, additional information is provided to the cloud so that authorized users would be able to decrypt the data using their private keys. If authorization is successful, a semi-trusted Security mediator (SEM) in cloud partially decrypts the data for the user and sends this data to the user. A user can fully decrypt it by using his/her private key and an intermediate key provided by SEM.

T_6:- "Identity-based encryption with outsourced equality test in cloud computing" [18]. It combines the concepts of Public Key Encryption with Equality Test (PKEET) and Identity based Encryption (IBE) to obtain Identity Based Encryption with Equality Test (IBEET) to take the benefits of both [18]. It provides support for the cloud service authorization for carrying out equality test on ciphertexts through a trapdoor. The receiver calculates the trapdoor based on the secret value of identity. Using this trapdoor, he can delegate the ability to check equality of its ciphertext with others' ciphertext, to the cloud server without requiring a central authority as a delegator. Therefore, it can be considered as the PKEET variant with user level authorization. In this approach, IBE with keyword search is extended to obtain the feature of equality test. The equality test is performed on the ciphertext of different users as well as that of the same user, without the ciphertexts being decrypted by the cloud server. It contains decryption algorithm along with encryption algorithm. Therefore, it can be used alone unlike Public key encryption with keyword search and identity based encryption with keyword search which require another encryption for the message due to lack of decryption algorithm for the keyword [18].

T_7:- "A pairing-free certificate-based proxy re-encryption scheme for secure data sharing in public clouds" [19].In this paper, a certificate based proxy re-encryption has been used. Proxy re-encryption provides secure sharing of data by enabling the data owner to pass on the decryption rights of the encrypted data without directly interacting with them. In this approach, a semi-trusted third party known as proxy is engaged by the data owner (delegator) for changing the ciphertext encrypted under the public key of the data owner into a new ciphertext of the same data encrypted under the public key of the delegator without having any knowledge about the actual data [19]. In this approach, further, a certificate based encryption is used in which a public/private key pair is generated by the user and the public key is sent to a trusted central authority for the generation of certificate. For decryption purposes, this certificate and private key of the user is used. No other user is concerned about this certificate therefore, it is kept public. Therefore, certificate management problem is eliminated. It has been proved that this approach provides chosen cipher text security under Diffie Hellman assumption in random oracle model [19]. It provides secure data sharing among authorized users without any direct interaction. It is computationally efficient as it doesn't use bilinear pairing. It is based upon hash-enhanced Elgamal PKE and Schnorr's signature scheme [19]. It has been proved that it highly efficient in comparison to other models and can be used for those devices that require lesser computations and are power constrained.

T_8:- "Privacy-preserving data utilization in hybrid clouds" [20]. In this paper, practical hybrid architecture has been proposed. A private cloud has been introduced to act as an interface between users and the public cloud. It provides fine grained access control and keyword search over encrypted data. Public cloud provides outsourcing of data and controls the outside access to the stored data. The data owners are responsible for defining and enforcing access policy on their own files by encrypting them. Private cloud generates trapdoors for efficient keyword search. Two phased encryption has been used, symmetric encryption like AES has been used for files and ABE has been used for encryption keys [20]. The authors have further exhibited the methods to outsource the cryptographic mechanism of access control and have proved the computation costs at data user side have been reduced.

T_9:- "A hybrid cloud approach for secure authorized deduplication" [21]. In this approach the concept of differential data deduplication has been used to save the storage space on public cloud. File is stored on public cloud just once and multiple users with same copies of files are provided with the pointers to the same file based upon the privileges. First of all, the user's identification is checked by the private cloud, if it passes the user requests private cloud for key tokens for the files they want to access. The private cloud manages all the private privilege keys for the authorized users and generates file tokens. The public cloud performs data Deduplication checks based on the file and file token submitted by the user. To provide Deduplication, instead of encrypting the file with each user's key, enhanced convergent key encryption is used [21]. The authors have implemented the prototype of their proposed model and carried out experiments that prove that their model involve minimal overhead as compared to other convergent encryption techniques.

T_{10}:- "*A novel security private cloud solution based on eCryptfs"* [22]. It is a strong encrypted file system for an enterprise. Transparency, dynamic, efficient and safe encryption feature has been provided for the applications. In

this paper, file encryption system for a secure cloud has been provided based on ecryptfs. In this approach, the private cloud of the enterprise is combined with overall architecture of the system and the file storage security is analyzed. Ecryptfs, basically deal with encryption and decryption of data [22]. The underlying file system manages the storage of data. Ecryptfs act like "filter" between virtual file system layer and low level physical file system layer. Firstly symmetric key encryption is used to encrypt the file contents and then, file encryption key (FEK) is generated [22]. Then, FEK is protected using password supplied by the user, public key encryption algorithm like RSA and trusted platform module for public key. First of all, using hash functions the user password is processed, and then a symmetric key algorithm encrypts the FEK. There may be multiple EFEKs (Encrypted File Encryption keys) as number of authorized users is allowed to access the same encrypted file [22].

T_{11}:- *"Secure and Efficient Data Collaboration with the hierarchical attribute-based encryption"* [23].This technique offers a fine-grained access control of ciphertext and provides a secure way of performing data write operations on the ciphertext by using ABE and Attribute based signature (ABS) [23]. In this scheme, there is no key management burden on the attribute authority instead a full delegation method has been used which is based upon hierarchical ABE. Further, the scheme also supports partial decryption and partial signing construction [23].

T_{12}:- *"Efficient and Secure identity based encryption scheme with equality test"* [24]. This is an identity based encryption with equality test technique which uses bilinear pairing. It lowers the requirement of using HashToPoint functions which are time consuming. It is highly secure against Chosen Identity & Chosen Ciphertext attacks in random oracle model [24]. The performance evaluation demonstrates that the scheme is highly efficient and has low communication as well as computational costs.

T_{13}:- *"Cryptography-based secure data storage and sharing using HEVC and public clouds"* [25]. This technique is used for exchanging data between mobile users and media clouds by hiding the data under high efficiency video calling (HEVC) [25] intra-encoded video streams in unsliced mode. In this scheme an enhanced version of AES has been used which outperforms AES-256 in terms of processing time and memory requirements. It is suitable for real time applications. The experimental results prove that this technique is highly secure and robust under power-saving constraints and for use in real time processing.

T_{14}:- *"Intelligent cryptography approach for secure distributed big data storage in cloud computing"* [26]. This approach prevents the cloud service providers from gaining access to the partial data. In this approach, the files are split up and are stored separately in different cloud servers. Further, one more approach, called as Security-Aware Efficient Distributed Storage (SA-EDS) [26] mode has also been proposed, which checks whether the data should be split up or not for decreasing operation time. Three algorithms namely, Alternative Data Distribution (AD2), Secure Efficient Data Distribution (SED2) Algorithm and Efficient Data Conflation have been proposed to support (SA-EDS)[26]. The experimental results show that it is highly secure against cloud service provider attacks and has a low computation time.

T_{15}:- *"Homomorphic Encryption for Security of Cloud Data"* [27]. In this approach, client side data encryption has been used. Fully homomorphic encryption technique [27] has been used for storing data on the cloud in encrypted format. This approach offers high confidentiality, since data is never rendered as plaintext at any stage. Further, it also prevents against collusion attacks from cloud service providers.

T_{16}:- *"Pairing-based CP-ABE with Constant Size Ciphertext and Secret keys for Cloud Environments*" [28]. In this paper a novel pairing based Ciphertext Policy Attribute Based Encryption (CP-ABE) [28] for resource-constrained mobile devices has been proposed to prevent data from unauthorized access. In order to work for these devices, the proposed approach provides ciphertexts and secret keys of constant size. The authors claim that it is the first technique to offer constant size ciphertext and secret key. The security proofs of the proposed scheme claim that it is secure against chosen ciphertext attacks in a selectively secure model and more efficient than other ABE schemes when used in real world scenarios [28].

T_{17}:- *"An efficient and Secure Privacy preserving approach for outsourced data of resource constrained mobile devices in cloud computing"* [29]. In this paper, a new keyword searchable encryption scheme for resource constrained mobile devices has been proposed. For the encryption of the data, this scheme uses a probabilistic key encryption [29] and for retrieving the files from the cloud, it calls upon ranked keyword search over encrypted data. With this keyword search the system usability is improved as it allows the ranking on the basis of relevance score obtained from search results and instead of sending all the files, it sends only the top most relevant files. This scheme ensures high data privacy and low computation overheads. The experimental results show that the proposed scheme is highly secure and efficient.

T_{18}:- *"A General Framework to design Secure Cloud Storage Protocol using Homomorphic Encryption Scheme"*

[30]. In this paper, the authors have designed G-SCS i.e Generic Way to Secure Cloud Storage scheme [30]. The proposed scheme can be used in real time applications as it supports data dynamics, randomized and deterministic auditing and third party auditing. The experimental results claim that the proposed scheme is highly secure and efficient. It outperforms the existing works in terms of storage, communication and computation costs [30].

T_{19}:- "Fuzzy encryption in cloud computation: efficient verifiable outsourced attribute-based encryption" [31].It is a new CP-ABE technique which uses blinding algorithm [31] to reduce the number of exponential operations involved in the encryption process. Further, the proposed scheme is a CP-ABE scheme with checkabilty and constant-sized ciphertext. With the help of Green's outsourcing security model [31], the authors have proved that this scheme is a secure against replay-able chosen ciphertext attacks. Further the experimental results illustrate that the proposed scheme is efficient in terms of computation overheads, communication costs and encryption time.

T_{20}:- "Enhance the Data Security in cloud computing by Text Steganography" [32]. It is a new linguistic approach of text Steganography which increases data security [32]. In this approach a random cover media is used to hide the data after encrypting it with substitution. This approach uses Indian script as encoding method and capital alphabet shape encoding method which is difficult to break. The experimental results show that this approach has very low time overheads [32].

IV. COMPARATIVE ANALYSIS

In this section, the cryptographic techniques discussed in the previous section have been analyzed and compared over various aspects. Table 2. Highlights the type of encryption algorithm used in each technique and the year in which the technique was proposed.

Table 2. Types of encryption scheme used in various techniques

Technique	Year of publication	Encryption algorithm Used
T_1	Ora et al.(2015)	RSA and Homomorphic Encryption
T_2	Shimbre et al. (2015)	AES
T_3	Kumar et al. (2015)	ABE
T_4	Huang et al. (2015)	Predicate Encryption
T_5	Seo et al. (2014)	Mediated Certificateless Public Key Encryption
T_6	Ma (2016)	Identity-based Encryption
T_7	Lu et al. (2015)	Proxy re-encryption
T_8	Li et al. (2014)	Attribute based Encryption and Searchable Encryption
T_9	Li et al. (2015)	Convergent Key Symmetric Encryption
T_{10}	Zia (2013)	RSA and A Symmetric Key Encryption
T_{11}	Huang et al. (2017)	ABE
T_{12}	Wu et al. (2017)	Identity-based Encryption
T_{13}	Usman et al. (2017)	AES
T_{14}	Li et al. (2017)	Probability Public Key Encryption Algorithm
T_{15}	Potey (2016)	Homomorphic Encryption
T_{16}	Odelu et al. (2017)	Ciphertext Policy based ABE
T_{17}	Pasupuleti et. al (2016)	Probabilistic Public Key Encryption
T_{18}	Zhang et. al (2017)	Homomorphic Encryption
T_{19}	Li et. al (2017)	Ciphertext policy-based Encryption
T_{20}	Sanghi et. al (2018)	Text Steganography

Table 3. Compares each technique by the type of cloud in which it has been used. This table highlights whether the given technique is used in public, private or hybrid cloud. Each type of cloud has its own security requirements, with hybrid cloud being the most secure one and the public is the least secure. In Table 4. the pros and cons of different cryptographic techniques have been highlighted.

Table 3. Types of clouds for which cryptographic technique has been designed

Technique used	Types of Cloud		
	Public	Private	Hybrid
T_1	✓	×	×
T_2	✓	×	×
T_3	✓	×	×
T_4	✓	×	×
T_5	✓	×	×
T_6	✓	×	×
T_7	✓	×	×
T_8	×	×	✓
T_9	×	×	✓
T_{10}	×	✓	×
T_{11}	✓	×	×
T_{12}	✓	×	×
T_{13}	✓	×	×
T_{14}	✓	×	×
T_{15}	✓	×	×
T_{16}	✓	×	×
T_{17}	✓	×	×
T_{18}	✓	×	×
T_{19}	✓	×	×
T_{20}	×	✓	×

Table 4. Comparison of the Different Techniques based upon their Merits and Demerits

Technique	Advantages	Disadvantages
T_1	• It provides data confidentiality, integrity and access control.	• The Private keys are sent to the users thorough emails, therefore there is chance of leakage of these keys on the network communication channels if they are not secure.
T_2	• It is greatly efficient against malicious data modification attacks and server colluding attacks. • It provides faster error localization, faster recovery, security and integrity.	• No comparison with the existing work has been provided
T_3	• It is difficult for hackers to break in as it goes through multiple steps. • It is easy and inexpensive as compared to other encryption techniques. • It is secure as the data which is encrypted consists of attributes and not data.	• Decryption is expensive at it is performed on the servers itself.
T_4	• It uses asymmetric encryption and is flexible in practice. • After the unreadable time both the secret key and cipher text gets destroyed, therefore it provides higher security. • With this scheme the attacker cannot derive the full cipher text and cannot perform cryptanalysis using any type of attack	• The computation cost of encryption scheme is high as compared to other approaches due to time release and data self destruction properties.
T_5	• Confidentiality of data and keys is maintained as cloud cannot fully decrypt the data. • Computation overhead is less as pairing operations are not used this technique. • Solves the problem of key escrow in identity based encryption and certificate revocation in public key cryptography.	• The partial keys generated by the Key Generator Centers have to be transmitted over the network.
T_6	• It provides for cloud server authorization to conduct a equality test. • It provides one way chose ciphertext security against a chosen identity attack (OW-ID-CCA) • Suitable for those with minimal resources for computations like mobile phones • Does not requires central delegator.	• Computation complexity for decryption is expensive due to bilinear pairing. • Key size and trapdoor length is larger as compared to IBEKS.
T_7	• Reduced Computation cost • Solves the problems of Key escrow problem of Identity based encryption and certificate revocation problem in PKE • Solves the key distribution problem as certificates are made public • Provides security against chosen ciphertext attacks	• Security proofs have been provided for only random oracle model and not the standard model.
T_8	• Provides user authentication using message	• High computation complexity due to bilinear maps

	authentication code, thus preventing replay attacks by revoked users. • More efficient searching using symbol based trie. • Reduced computation overhead at users side • Higher confidentiality	
T₉	• Differential authorization • Authorized duplicate checks • Unforgeability and Indistinguishabiltiy of duplicate check tokens • Data confidentiality • Minimal overhead as compared to other convergent key encryption algorithms	• If the adversary colludes with the private cloud, it will lead to confidentiality of the file reduced to convergent encryption as encryption key becomes deterministic
T₁₀	• High security • Rich allocation strategies • Reduced operating costs • Higher speed	• No performance analysis with the existing techniques have been done
T₁₁	• Offers authorization and fine-grained access control • No key management burden • Offers Partial Decryption that reduces computation overhead on users • Cost effective	• High computation complexity due to the usage of bilinear pairing.
T₁₂	• High efficiency • Low Communication and computational costs • Secure against OW-ID-CA attacks • Low Ciphertext size	• It suffers from key escrow problem • Not secure against Collusion attacks
T₁₃	• High security and robustness • Secure against collusion attacks • Suitable for real time applications • Low processing time and memory requirements	• The size of the encrypted audio stream gets increased
T₁₄	• High security and efficiency • Secure against cloud provider attacks • Low computational time	• Lacks data availability
T₁₅	• High data confidentiality • Secure against collusion attacks	• Reduction in ciphertext size is required
T₁₆	• Provides authorization and access control • First ABE scheme to support constant sized ciphertexts and keys • Suitable for resource constrained devices and real world scenarios • Secure against chosen ciphertext attacks	• High computation complexity due to bilinear maps. • Not secure against collusion attacks. • Efficiency needs to be improved.
T₁₇	• Ensures high data privacy, confidentiality and integrity • Low computation overheads • High efficiency • Suitable for resource-constrained devices	• No supports for dynamic data operations.
T₁₈	• High security and efficiency • Supports data dynamics, third party auditing , randomized and deterministic auditing • Low storage, communications and computation costs • Suitable for real time applications	• Higher storage costs at cloud side
T₁₉	• Secure against replay-able chosen ciphertext attacks and collusion attacks • Low computation overheads • Low communication costs and encryption time	• Low computation efficiency due to bilinear maps.
T₂₀	• Very difficult to break • Very low time overheads.	• Memory requirements are large.

In Table 5., various cryptographic techniques have been compared on the basis of six major parameters that are required for the security and privacy of the data stored on the cloud.

Table 5. Comparison of Different Techniques based upon Various Parameters

Technique used	**Security Parameters**							
	Access control	**Authorization & Authentication**	**Cost effective**	**Complexity**	**Collusion attacks proof**	**Data confidentiality**	**Integrity**	**Processing Speed**
T_1	✓	✗	✗	✗	✗	✓	✓	✗
T_2	✓	✗	✗	✗	✓	✓	✓	✓
T_3	✓	✓	✓	✗	✗	✓	✗	✓
T_4	✓	✗	✗	✓	✓	✓	✗	✗
T_5	✓	✗	✓	✗	✗	✓	✗	✓
T_6	✗	✓	✗	✓	✓	✗	✗	✓
T_7	✗	✓	✓	✗	✗	✓	✗	✓
T_8	✓	✗	✓	✗	✗	✓	✗	✗
T_9	✓	✓	✓	✗	✗	✓	✗	✗
T_{10}	✗	✗	✓	✗	✗	✓	✓	✓
T_{11}	✓	✓	✓	✓	✗	✗	✗	✓
T_{12}	✗	✗	✓	✓	✗	✗	✗	✓
T_{13}	✗	✗	✓	✗	✓	✗	✓	✓
T_{14}	✗	✗	✓	✗	✓	✗	✗	✓
T_{15}	✗	✗	✗	✗	✓	✓	✓	✓
T_{16}	✓	✓	✓	✓	✗	✓	✗	✗
T_{17}	✗	✗	✓	✗	✗	✓	✓	✓
T_{18}	✗	✗	✓	✗	✗	✗	✓	✓
T_{19}	✗	✗	✓	✓	✓	✗	✗	✓
T_{20}	✗	✗	✓	✗	✗	✓	✓	✓

V. CONCLUSIONS

Security in clouds provide secure channel for establishing trust between the customers and the cloud service providers. This paper has tried to highlight the major security challenges that are acting as stumbling blocks in the way of cloud computing. In this paper, the work of different researchers in field of data security has been analyzed. Various enhanced cryptographic techniques in different types of clouds have been discussed and their pros and cons have been highlighted. Since, the range of cloud security is very vast and every other day a new threat is emerging, still a lot of work has to be done to make the cloud data fully secure and to gain the trust of the users towards adopting clouds without any fears. Therefore, we have tried to highlight the crucial issues that need to be worked upon. The findings of this paper can be used for the future research to overcome the shortcomings of the present techniques and to build up new algorithms to enhance the security of the existing ones.

REFERENCES

[1] Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, "A survey on security issues and solutions at different layers of Cloud computing", The Journal of Supercomputing, Vol. 63, Issue. 2, pp. 561-592, 2013.

[2] National Institute of Standards and Technology, Information Technology Laboratory, "The NIST Definition of Cloud Computing," https://www.nist.gov/sites/default/files/documents/itl/cloud/cloud-def-v15.pdf.

[3] T.V. Sathyanarayana, L.M.I. Sheela, "Data security in cloud computing", in Proceedings of IEEE International Conference on Green Computing, Communication and Conservation of Energy (ICGCE), India, pp. 822-827, 2013.

[4] A.M. Khan, S. Ahmad, M. Haroon, "A Comparative Study of Trends in Security in Cloud Computing ", in Proceedings of the 5th IEEE International Conference on Communication Systems and Network Technologies (CSNT), India,pp. 586-590, 2015.

[5] P. Sirohi, A. Agarwal, "Cloud computing data storage security framework relating to data integrity, privacy and trust", in Proceedings of the Ist IEEE International Conference on Next Generation Computing Technologies (NGCT), India, pp. 115-118, 2015.

[6] Ennajjar, Y. Tabii, A. Benkaddour, "Security in cloud computing approaches and solutions" in Proceedings of the 3rd IEEE International Colloquium Information Science and Technology (CIST), Morocco, pp. 57-61, 2014.

[7] Cloud Security Alliance, "Cloud Adoption Practices & Priorities Survey Report"https://downloads.cloudsecurityalliance.org/initiatives/surveys/capp/Cloud_Adoption_Practices_Priorities_Survey_Final.pdf.

[8] J. Somorovsky,M. Heiderich, M. Jensen, J. Schwenk, N. Gruschka, L.Iacono, "All your clouds are belong to us: security analysis of cloud management interfaces," in Proceedings of the 3rd ACM workshop CCW,pp.3–14, 2011.

[9] G. Zhaolong, S. Yamaguchi, B.B. Gupta, "Analysis of various security issues and challenges in cloud computing environment: a survey" in Handbook of research on modern cryptographic solutions for computer and cyber security. IGI Global Publisher., pp. 393-419, 2016.

[10] Cloud Security Alliance, "The Notorious Nine Cloud Computing Top Threats in 2013" https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf.

[11] Cloud Security Alliance, "The Treacherous Twelve,"https://downloads.cloudsecurityalliance.org/assets/research/top-threats/treacherous-12-top-threats.pdf.

[12] D.A.B. Fernandes, L.F.B Soares, J.V. Gomes, M.M Freire, P.R. Inacio, “Security issues in cloud environments: a survey”, International Journal of Information Security, Vol. 13, Issue 2, pp. 113-170, 2014.

[13] P. Ora, P.R. Pal, “Data security and integrity in cloud computing based on RSA partial homomorphic and MD5 cryptography”, in Proceedings of IEEE International Conference on Computer, Communication and Control (CC4), India, pp. 1-6, 2015.

[14] N. Shimbre, P. Deshpande, “Enhancing Distributed Data Storage Security for Cloud Computing Using TPA and AES Algorithm”, in Proceedings of IEEE International Conference on Computing Communication Control and Automation (ICCUBEA), India, pp. 35-39, 2015.

[15] N.S. Kumar, G.R. Lakshmi, B. Balamurugan, “Enhanced Attribute Based Encryption for Cloud Computing”, Procedia Computer Science, Vol. 46, pp. 689-696, 2015.

[16] S.Y. Huang, C.I. Fan, Y.F. Tseng, “Enabled/disabled predicate encryption in clouds”, Future Generation Computer Systems, Vol. 62, pp. 148-160, 2016.

[17] S.H. Seo, M. Nabeel, X. Ding, “An efficient certificateless encryption for secure data sharing in public clouds”, IEEE Tansactions on Knowledge and Data Engineering, Vol. 26, Issue. 9, pp. 2107-2119, 2014.

[18] S. Ma, “Identity-based encryption with outsourced equality test in cloud computing”, Information Sciences, Vol. 328,pp. 389-402, 2016.

[19] Y. Lu, J. Li, “A pairing-free certificate-based proxy re-encryption scheme for secure data sharing in public clouds”, Future Generation Computer Systems, Vol. 62, pp. 140-147, 2016.

[20] J. Li, J. Li, X. Chen, Z. Liu, C. Jia, “Privacy-preserving data utilization in hybrid clouds”, Future Generation Computer Systems, Vol. 30, pp. 98-106, 2014.

[21] J. Li, Y.K. Li, X. Chen, P.P.C Lee, W. Lou, “A hybrid cloud approach for secure authorized deduplication”, IEEE Transactions on Parallel and Distributed Systems, Vol. 26, Issue. 5, pp. 1206-1216, 2015.

[22] Z.P. Jia, X. Tian, “A novel security private cloud solution based on eCryptfs”, in Proceedings of the 6th IEEE International Conference on Information Management, Innovation Management and Industrial Engineering (ICIII), China, pp. 38-41, 2013.

[23] Q. Huang,Y. Yang, M. Shen, “Secure and efficient data collaboration with hierarchical attribute-based encryption in cloud computing”, Future Generation Computer Systems,Vol.72, pp. 239-249, 2017.

[24] L. Wu, Y. Zhang, K.K.r. Choo, D. He, “Efficient and secure identity-based encryption scheme with equality test in cloud computing", Future Generation Computer Systems, Vol. 73, pp. 22-31, 2017.

[25] M. Usman, M.A. Jan, X. He, “Cryptography-based secure data storage and sharing using HEVC and public clouds”, Information Sciences, Vol. 387, pp. 90-102, 2017.

[26] L. Yibin, K. Gai, L. Qiu, M. Qiu, H. Zhao, “Intelligent cryptography approach for secure distributed big data storage in cloud computing”, Information Sciences, Vol. 387, pp. 103-115,2017.

[27] C.A. Dhote, “Homomorphic encryption for security of cloud data”, Procedia Computer Science, Vol. 79, pp. 175-181, 2016.

[28] Odelu, A.K. Das, Y.S. Rao, S. Kumari, M.K. Khan, K.K. Choo, “Pairing-based CP-ABE with constant-size ciphertexts and secret keys for cloud environment”, Computer Standards & Interfaces, Vol. 54, pp. 3-9, 2017.

[29] S.K. Pasupuleti, S. Ramalingam, R. Buyya, “An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing”, Journal of Network and Computer Application, Vol. 64, pp. 12-22, 2016.

[30] J. Zhang, Y. Yang, Y. Chen, J.Chen, Q. Zhang, “A general framework to design secure cloud storage protocol using homomorphic encryption scheme”, Computer Networks, Vol.129, pp.37-50, 2017.

[31] J. Li, X. Li, L. Wang, D. He, H.Ahmad, X. Niu, “Fuzzy encryption in cloud computation: efficient verifiable outsourced attribute-based encryption”, Soft Computing, Vol. 22, Issue 3, pp. 707-714, 2018.

[32] A. Sanghi, S. Chaudhary, M. Dave, “Enhance the Data Security in Cloud Computing by Text Steganography,”, Smart Trends in Systems, Security and Sustainability, ser. Lecture Notes in Networks and Systems, Singapore: Springer, Vol. 18, 2018.

Author Profile

Manreet Sohal (born June 10, 1992) is research scholar, pursuing PhD at Department of Computer Engineering & Technology, Guru Nanak Dev University Amritsar. She has passed out her M.Tech (CSE) and B.Tech (CSE) from Guru Nanak Dev University. Her main area of interest is Cloud Computing.

Sandeep Sharma graduated with B.E (Computer) degree from the University of Pune, received the M.E(Computer) from Thapar University Patiala and received his PhD degree from Guru Nanak Dev University Amritsar. He is a Professor and The Head of Department of Computer Engineering and Technology at Guru Nanak Dev University, Amritsar. He is a Chief Security Information Officer as well as Nodal Officer of Digital India Week. He is the Network as well as mail Administrator of the Guru Nanak Dev University .He has many research publications in the areas of parallel processing, wireless sensor networks and Cloud computing