IJCSE International Journal of Computer Sciences and Engineering Open Access

Survey Paper Vol.-6, Issue-10, Oct 2018 E-ISSN: 2347-2693

Cloud Computing Technologies for Privacy Data and Digital Security Authentication: A Literature Survey

Rakesh Prasad Sarang

SOS in Computer Science & Applications Jiwaji University, Gwalior (M.P.), 474001, India

Corresponding Author: sarang.nit@gmail.com, Tel.: +91-9926646335

Available online at: www.ijcseonline.org

Accepted:25/Oct/2018, Published: 30/Oct/2018

Abstract—Cloud computing is a model for enabling ubiquitous convenient, where the resources of a data center are shared using virtualization technology. Cloud computing is one of the dynamic provisioning technology. Cloud computing technology can be implemented in a wide variety of architectures under different services and deployment models. Privacy to the data stored in cloud server is a major challenging operation in cloud computing. The objective of this paper is to explore different methods for efficiently growing latest digital techniques. The main aim of this paper is to design and propose strong security system to the data stored in the cloud system. This paper presents a literature review we studied the background work of carried-out by the various approaches about the uses of cloud technology. We have proposed framework and different methods which provides, identification of high protection. The literature review presents previous studies related to the objectives of the present study. Further various features that make the proposed framework more suitable for analysis and evaluation of cloud computing. The privacy cloud algorithms are categorized into subgroups according to the high level security concerns in the cloud computing.

***Keywords*—**Cloud Computing, Privacy and Protection Technique, Digital Authentication for Data Security, Algorithms for Privacy

I. INTRODUCTION

The last decade of twenty-first century will be noted in the past time of mankind for the incredible growth of the internet and information technology. Every day shows the increasing popularity of the new technology and network. Cloud computing will provide availability of powerful computing technique, mobile, and sensing devices the internet is changing day to day working scenario. Accordingly, in this paper firstly, cloud computing emerges as a computing platform for the next generation of new internet computing technology. Cloud computing is a technology which provides services that make users access all the database resources and software through the internet from anywhere in the world, as long as they need. Cloud computing is a collection of new and old concepts in many research areas, such as distributed computing, grid computing, utility computing and service oriented architectures. In brief, cloud computing is the dynamic provisioning of IT capabilities (such as hardware, software deployment models, and service models) from over the network. Cloud computing technology can be implemented in a wide variety of architectures, under different services and deployment models. Cloud computing has the inherent ability to use shared computing resources with local servers handling various applications. This paper also supports the cloud computing users have the freedom to identify the location and the storage of their data. The device is so user-friendly that the users may start using the services anywhere and at anytime. The users have to access computing resources, such as Google Apps Engine and cloud based applications through using a browser and it can be organized on thousands of computers via internet [1].

In the present paper, our objective is to simplify the cloud techniques have several applications and components in different areas including clients', services, platform, infrastructure, data center and distributed servers. Through cloud computing, we can design and carry out the implementation of security applications. Cloud computing has been established as an important applicability research of areas such as IT, Google App, Google docs, hotmail, business, and Amazon. As a new field, cloud computing technology that improves our capability to optimize, time level and better support secure our server, system, and data storage. Since their introduction, number of researchers have involved in this field and proposed techniques and algorithms to reply the complex demand of information technology resources. Detail description of cloud computing is already discussed in the previous section of this paper. This paper is presenting a general review of cloud computing. With the main focus on privacy and security issues in cloud computing. We would also investigate challenges, implementing and the future of cloud computing. There are several problems that are designed by computer programs to solve and finding the best solution. In this section we shall discuss security and privacy challenges here which are also relevant to the general requirements for cloud suppliers such as provide reliable services. The cloud computing includes grand challenges and applications, such as Aerospace, Earth science, Life science, Bio medical, IT industries and E-commerce. In the cloud computing users directly share resources and operates the software and hardware. In the end of this paper, brief review reports on evaluation rules and privacy techniques of cloud computing are available in the literature, which is presented with implementation of structural design of each. The main objective of the proposed study is to discuss the algorithms software, security scenarios and analyze research technique in the field of cloud computing. As with other aspects basic requirements which lead to the evaluation of cloud computing includes server virtualization, storage virtualization and network virtualization [2,3]. Cloud computing has been defined by National Institute of Standards and Technology (NIST) as:

"Cloud computing is a model for enabling ubiquitous 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 provisioned and released with minimal management effort or service provider interaction" [4].

Out of various techniques of cloud computing such as distributed, parallel, grid, utility and service oriented is the most vital one due to its many services on pay – per use basis. Cloud computing technology can be used in several services such as telephony, gas, electricity, water, data storage, computation, and application-hosting. Privacy in cloud computing can be defined as the capability of an entity to manage all service models about itself to the cloud and how can access particular information. A cloud cannot be used for storing and processing data and applications if it is unsecured. The main problem regarding privacy in the cloud is how to secure data from being used by unauthorized users, how to stop attacks control next to privacy. This review of literature is a brief survey of cloud computing. It tries to analyze privacy, related research topics, analysis of data and evaluation of possible applications and future challenges. The study shall include introduction of layers, types of cloud computing, grid computing, services and new technologies.

This paper is organized as follows: Section 1 presents introduction to cloud computing, Section 2 presents evolution of cloud computing. The section 3 presents privacy and data protection. Section 4 presents literature of review. Section 5 presents privacy protection technique. Section 6 presents algorithms for privacy cloud computing. In section 7 we have presented migration of virtual cloud and features of cloud computing. And finally section 8 presents conclusion.

II. Evolution of Cloud Computing

In this section, we have defined the concept of cloud computing evolution. Evolution techniques can be used to introduce the solution cloud computing platforms. Evolutionary techniques are helpful in many applications and networks of large groups of resources service.

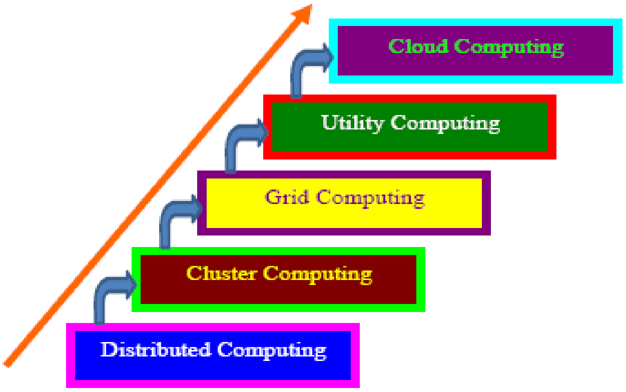

Figure 1 : Evolution of Cloud Computing

In figure 1 shows five phases of cloud computing paradigms. In the evolution of cloud computing provides an overview of the technologies. Cloud computing is a new technology which provides a delivery of computing resources through the internet. Cloud computing technique uses web applications and networks of large groups of server services. computing techniques have several applications and components in different areas including database storage, development models, networking, and deployment platforms, as well as big business processes. Cloud computing techniques perform different organization systems and resources (such as distributed, cluster, grid, and utility computing). We briefly review five core technology that played an important role in the realization of cloud computing. These are distributed computing, cluster computing, grid computing, utility computing and cloud computing. Evaluate these five computing paradigms, it looks like that cloud computing is the original mainframe computing paradigm. Some of the cloud computing techniques are as follow:

A. Distributed Computing

Distributed computing is a foundational model used for cloud computing. Since cloud structure are distributed systems. Distributed computing studies the models and system developments, the architecture, virtualization, service orientation, and web 2.0 used for building and managing distributed system. This is a core technology enabling the provisioning of cloud services from anywhere in the globe. A distributed system is one in which components located at networked computers communicate and coordinate their events only by passing e-mails. Distributed system has been defined by Tanenbaum as: *"A Distributed system is a collection of independent computers that appears to its users as a single coherent system"*.

Distributed computing is a technique refers such as computing method, where a single task is decomposed into all the modules are completed on several computing devices over an established network. Developing applications and system software that control the cloud requires information across all these technologies. There are many kinds of new major challenges for engineers and developers such as pervasive networking technology, ubiquitous computing, social networks, e-commerce, and online gaming [5, 6, 7].

B. Cluster Computing

Cluster computing technique is an increasingly popular high performance and distributed computing solution. Cluster technology also provides an excellent platform for solving a range of parallel and distributed computing applications in both commercial and scientific areas. Clusters need to integrate fast interconnection technologies because is to support high-bandwidth and inter-processor communication connecting cluster nodes. Cluster machines are known as linked by a high-bandwidth network and controlled by specific software tools that manage them as a single computer system. The cluster techniques have several components and frameworks in different areas including distributed computing, multiple-standalone computers (PCs, Workstations), operating systems, high-performance interconnects, middleware, parallel programming environments, and applications [8,9].

In figure 2 show the architecture of a cluster computing will also have a cluster middleware which provides an interactive and easy to operate for the user. This cluster middleware is to connect high-speed network connection, which consists of several PC. The users will be running two applications sequent final application and parallel application.The main goal of cluster computing technique is to interconnection network technology that can be used in universities and all research laboratories. Because of a large amount of data that can be transmitted over the interconnect hardware from the source node to destination node in a fixed period of time. Cluster computing performed by a centralized resource manager and scheduling system.

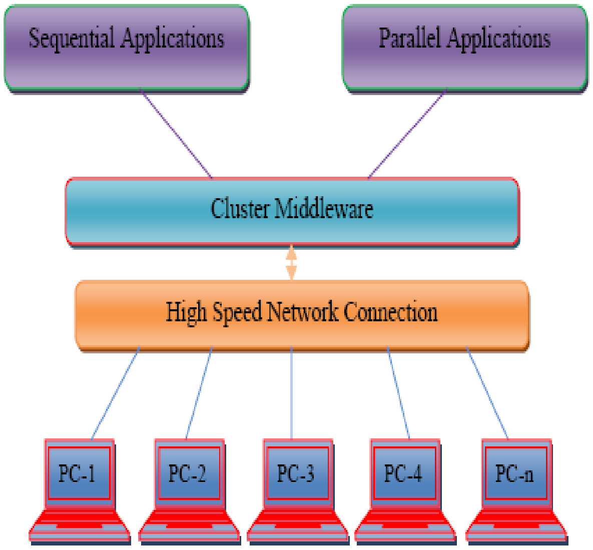

Figure 2: Architecture of Cluster Computing

C. Grid Computing

Grid computing has extended significantly in most recent ten years. There are a few pioneering schemes such as Globus, Condor, Legion and Unicore that provided grid solutions. Grid computing is the main technique that accesses to large computational power and sharing of computing application services. Grid computing has been defined by IBM as:

A grid is a collection of distributed computing resources over a local or wide area network that appears to an end-user or application as one large virtual computing system [10].

Grid computing is an advanced computing environment emergence of distributed processing. The grid techniques have several components and functional elements in different areas including resource management, security management, data management and services management. Grid computing techniques can be used to the deployment of computing applications and managed by many organizations. Grid techniques are helpful in many research fields like gas, oil fields, banking, and education. It can also provide remote access to distributed resources of the control system, and share of network resources such as data storage, databases, software, hardware and architectures. Grid computing is a new technology that composed asset sharing and critical thinking in powerful, multi-institutional virtual associations. One of the most versatile connection models of grid areas is shared are both customers and brokers [11].

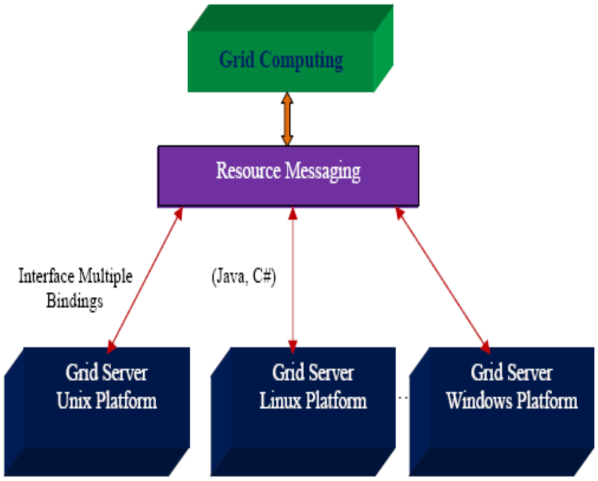
Grid Computing
Resource Messaging
Interface Multiple Bindings
(Java, C#)
Grid Server Unix Platform
Grid Server Linux Platform
Grid Server Windows Platform

Figure 3: Grid Computing

In figure 3 show the architecture of a grid computing will also have a resource messaging which provides different types of operating system platform, Such as Linux and windows. This resource messaging is the essential component of grid computing, which provides multiple interfaces and implementation such as Java, C# etc.

D. *Utility Computing*

Utility computing is a visualized to the next generation of information technology (IT) development, that represent how the computing needs of users can be fulfilled in the future IT industry. Utility computing is not specific to any kind of techniques, it should be applicable to various kinds of a real world where service providers maintain and supply utility services, such as electrical power, gas, and water to consumers. Utility techniques are using a computer system to both service providers and users.

There are many challenges that require being realizing in utility computing. The first challenge is that both service providers and users need to change and reorganize their current IT procedures and a user process. The second challenge managing the technological aspects of computing services delivery [12].

E. *Cloud Computing*

Cloud computing is a new concept of the modern world. Cloud computing combines all the services models and technologies together to deliver IT enterprise. Cloud computing emerges as a computing platform for the next generation of the new internet computing technology (ICT), that is cloud computing as a new technology modernization has been broadly accepted in the academic world. It means general-purpose, internet-based, moral pay-on-demand; researchers have a tendency to simplify the real situation for ICT.

III. Privacy and Data Protection

This section describes privacy which may also include authentication and prevention concerns to various legal and non legal norms of the cloud services. Privacy data protection is a primary human right. In this situation often understood as compliance with data protection regulations. It would be highly complex to provide the full privacy and personal data protection to issue proper implementation of cloud computing, such as database access security, server access security, internet access security, data privacy security and program access security. The globally accepted privacy principles give a useful framework, authority, purpose restriction, legitimacy, transparency, data security and data analysis participation.

Buyya et al. [13] presented 21st century vision of computing paradigms promising to convey the resources of cloud computing services. This vision of the computing paradigms has been proposed new advanced technologies such as multicore processors, networked computing environments and market-based resource management systems. Over the years, a market-based resource system is a 3rd generation Aneka enterprise Grid technology which is provided with an atmospheric of computing environment.

Jansen [14] has proposed cloud hooks key issues, which are accepted to have long term importance in cloud computing security and privacy. Because of this key issues, identifies cloud based on documented problems and demonstrated faults. Moreover cloud hooks key techniques are not acceptable with the policies and cloud based systems. That follows best security related issues that are able to be believed have long-term significance for cloud computing. The proposed key issue in this section is data sensitivity and privacy of information have transmitted to outsourcing portions of the organizational computing environment.

Provos et al. [15] have proposed secure client side protection and secure website infrastructure both are required for protection against attacks. The proposed work identifies four types of content control. For each type, content control responsible for enabling web browser development: web server security, third party widgets, user contributed content and publicity. For many cloud computing services, web browser key element, web based malware infection and extensions which are available for their security problems. Moreover, the current state of malware web automatic update a small number of evaluations is based on users of existing vulnerabilities.

3.1 *Data Storage Protection IP Networks*

Data storage protections are classified into various kinds like: shared and non-shared, public or private, small zone or large zone systems and each of them have various security threats to deal with. Although considering the data storage protection, it is imperative to recognize private clouds. There is less vulnerability in a private cloud in comparison with open cloud. All the associations have a private arrange set up and consequently the system topology for a private cloud gets defined. Be that as it may, the trusted encryption plans and token system models should be changed to upgrade the security in an open cloud. Online data storage is becoming very popular now-a-days and it has been observed that enterprise storage will be networked in the coming years.

D.Tao et al. [16] designed and developed a new cloud platform based automated testing system for the mobile internet technique. By using automated testing resource of the cloud platform applied on large security of real-world applications. The cloud platform system works in three functional modules: In the first cloud platform functional by web front-end module, Django development framework. The second type cloud platform by testing environment module, support of virtual hosts and tools testing environment and third type cloud platform automated testing module, which perform testing tool interface packaging and the automated script control. The recent technological advancement, have the higher level of security policies with high performance.
Hebiya et al. [17] have proposed secure keyless algorithm (SKA) which are representing a new technique of data protection in cloud storage. In this algorithm the role of cloud server performs the user authentication and monitors are stored data in the remote server. The proposed technique is to find security vulnerabilities in cloud web applications. To think about SQL Injection (SQLI) and cross webpage scripting is an attack on the protection of customers of a specific web application. The proposed technique is to give cross site scripting method for storage server in cloud condition and to store the information utilizing secure keyless algorithm (SKA). It also perform authentication for the client at the time of cloud login. On the way if any unauthorized clients endeavor to get to the cloud storage it means the cloud review server is to reject that client by utilizing cross site scripting system.

Kaushik et al. [18] have proposed Keyless User Defined Optimal Security (KUDOS) algorithm. The proposed algorithm Keyless User Defined Optimal Security encryption is based on the concept of user customization. As the KUDOS algorithm is basically symmetric encryption process; the same key is used both to encrypt and decrypt the data. It also supports data dynamics where user can perform various operations on data like both stream cipher and block cipher to enhance by using binary bit level security. The significant advantage of KUDOS over other encryption algorithms is its capacity for customization. The client can control the chain counter as indicated by his needs; regardless of whether he needs it to be basic and faster than other or hard to split and secure.

3.2 *Identification of High Security*

The proposed study presents a general identification of cloud computing with the main focus on privacy and security evaluation concerns. The study encompasses identification of high security threats and their proposed solutions. The study shall glance into the new challenges in terms of implementing of analysis and remediation. The study shall generate some real datacenter attacks that can be detected from performance data in hypervisor operating systems. The proposed research areas include grid computing, network security, virtualization and evaluation.

Gholami et al. [19] proposed Apache Hadoop security as one of the deployment for big sensitive data infrastructures. It is analyzed that many organizations require proficient solutions to store big amount of data. Most of the Apache Hadoop security found to achieve better performance and handling big sensitive data in cloud computing environments. Therefore the preliminary data is generated from various sources such as high throughput instruments, sensors and connected devices. The main purpose, big data technologies can utilize cloud computing to provide significant benefits, such as the availability of automated tools to assemble, configure and virtualized resources on demand. Multi-tenancy authorization system (MTAS) model is proposed by Tang et al. [20]. It is well-known as role-based access control (RBAC) model. It uses a top collaborative access control properties such as centralized facilities, agility, homogeneity, and outsourcing cross tenant trust. They have introduced an authorization as a service (AaaS) approach using a formalized multi-tenancy authorization system, and provide system administrative approach. A similar work proposed another resource sharing approach known as data-centric clouds using database schema, but this approach is specialized to databases and cannot be directly applied to other types of services.

IV. LITERATURE OF REVIEW

A literature review is a method for gathering knowledge from the existing literature. The literature review in this paper is based on a review approach and is analyzed in the privacy and data protection.

4.1 Privacy Data Security in Cloud

In this section, some of the basic impression matters of the cloud in relation to privacy and security are presented. Cloud computing is based on the internet protocols viewpoint of information and electricity sharing, allowing access to one or more kind of heterogeneous and geographically separated resources. Sun Microsystems offers grid engine software that allows engineers at companies to pool the computer cycles on up to 80 workstations at a time. In grid computing, a large project is divided among multiple computers to make use of their resources.

Goyal et al. [21] proposed Veracity Aware Defiance Algorithm (VADA) for cloud environment which provides security and privacy. The proposed algorithm is novel and innovative data security which keeps network level and storage level security. The proposed algorithm in this section includes four parties during the communication for accessing and sensitive data stored in cloud, cloud service provider, data owner, user and trusted module. Because according to market research and analysis firm IDC there is 27% rise in usage of cloud services from 2008 to 2012. The performance of proposed algorithm is highly resourceful, safe and privacy aware for cloud environment.

A similar work proposed another algorithm [22] known as Optimal Keyless Algorithm for Security uses a new method of data and performs itself to create a protective shield. The proposed algorithm provides better and performance security at both character level as well as binary bit level. The quantity of rounds and the quantity of movements connected at binary bit level are made information dependent to increase the high security level, is a noteworthy advantage of the algorithm. The proposed framework with the motive to give most elevated security level with minimum execution time regarding encryption and decryption. So exploring the symmetric keyless cryptography follows the same technique of encryption algorithm but decryption algorithm in reverse order, i.e. this algorithm is keyless so no need of key generation and key administration exchange through an outsider.

4.2 Data Access Management Security

Mircea [23], has proposed authentication of clients and may use models based one or 2FA (password or fingerprint). Data security is a basic concern in our system. The data utilization requires the protection of information accessibility in the cloud and their utilization (perception, handling, and access) by the authorized people. Ensuring data security in the cloud requires the identification and investigation techniques that can be applied in every stage of data life cycle. The rights and authorizations related to people records, or areas permit the controlled and approved access to information utilization. The data security of basic controls must be to similarly concentrate on guaranteeing information sincerity. The utilization and safe exchange of system information can similarly be accomplished through gated, utilizing various procedures, for example, Multiprotocol Label Switching (MPLS), Virtual Private Systems (VPNs) and Virtual Local-Area Networks.

Dhanabakiyam et al. [24] have proposed a novel homomorphic verifying tag technique to verify the inner product evaluation on the dynamic data streams and then it extends to the matrix product verification**.** And also implement an extra proxy server for the data reliability. The proposed method for finding security data encryption is utilized for the basic information. The data encryption at various capacity can be carried on by utilizing at least one level, for example, equipment circle, record, application, and database recovery. Vijai et al. [25] have proposed a novel synergistic key administration convention in ciphertext agreement. The proposed methods improve protection of data and enhance the security for the system model. The data are outsourced to cloud after encryption key managing and utilization of easy or various keys, the data storage information that requires system encryption.

4.3 Web Based Application Security

Viswanadham et al. [26, 27] have proposed as a virtualization technology that permits us to create web pages and allows the clients to interact in a virtual machine. Web based security aspects defined as a virtualization technique. Web 2.0, is a key technology towards empowering the utilization of software as a Service (SaaS), the clients from assignments like support and establishment of software. During cloud computing services, clients access any business applications online from web browser, whereas software and data are stored on the servers. Web security service is one of the critical issues in implementing cloud computing environment. To develop a complete security evaluation and management structure is a part of cloud computing services. For satisfying the security demands and deploying the framework of the cloud computing environment it is highly required. Web of applications, the bulk of user data and applications will reside in the network cloud. Web applications are a critical part of Internet infrastructure and are used for banking, email, financial management, online shopping, auctions, social networking, and the like. Corporations such as Amazon, Google, Microsoft, and Yahoo expend considerable effort to keep up with the growing demand for communication.

Kumar et al. [28] presents SQL injection prevention techniques, which are used for security of data in a web application. Many web applications have interfaces where a user can input data to interact with the application’s underlying database. However, this technique supports various SQL injections which will cover a wide range of SQL injection attacks. The efficiency of combination of these prevention techniques may lead to a more secure and reliable database system.

4.4 Data on Open Stack Storage Security

Albaroodi et al. [29] have proposed security performing object storage developments and presenting additional support for virtualization technology. With open stack storage security, presents policies can give a more noteworthy comprehension of how are allowing long dreamed vision of cloud computing. Here one file encrypted with data encryption standard algorithm in which keys are created sequence one by one to the cloud system. The cloud system data is not moved from the virtual computing machine, while the application is running.

Nagar [30] has also proposed a specific component in swift storage of open stack is considered to be protected. Whereas additional components like nova, compute, glance and dashboard need to be superior. Many kinds of security and module attributes handles, such as addresses secure information, vulnerabilities, keystone module authentication, web service security and web applications. Open stack have some features of the proposed modules. The primary feature is the validation of a client before getting to the whole display in the open stack swift model that have only tokens character for each of client. Last and major feature of this storage security is the requirement of authorization and user-level authentication.

4.5 Digital Authentication for Data Security

Sivasakthi [31] has proposed client authentication to secure information of encryption technique with computerized signature in cloud computing. How to verify digital signature communication comes integral from the maintained sender. One of the secure frameworks ensured the data stored in the cloud server. Only single key distributed cryptography is utilized, because these key is shared services by remotely host. If the key is released messages are endangered, so this is called symmetric. This algorithm is an authentication search module form ϴ(x) = (p-1)*(q-1), where ϴ(x) encryption key and (p-1)*(q-1) encryption and decryption process algorithm. This process continues till no data privacy's are secured over cloud server. During the process of keystone can provide a strong authentication key machine that uses third party. This algorithm stores each client of key sizes of 128, 192 and 256 bits.

Singh et al. [32] proposed algorithm implemented throughout simulator tool EnDeCloud Reports for enhancing software resource data security in cloud environment. During the study of proposed algorithm on various parameters is discussed with respect to accessible cryptography algorithms. To use EnDeCloud Reports the information owner to authenticate the data users. The proposed algorithm used in EnDeCloudReports is an attempt to secure raw data files holding hardware resource utilization information of any cloud in an organization. After this data in ASCII value passed through 10 rounds for first 10 words and then so on starting from round 0 to 9, where round id is substituted before and after every word. It requires securing prioritized data files holding software hardware resource utilized information of any cloud in an organization. The data placement algorithm will tell us how to place the files efficiently to the containers in object storage. But most of the proposed algorithms encountered several problems such as lack of robustness and significant amount of time taken in encryption/decryption of data exist in on server in cloud.

4.6 Data Centric Algorithms Security

Sarita [33] provided a comparison between four most universal and easily used symmetric key algorithms: DES, 3DES, AES and Blowfish. A comparison has been completed on the source of different parameters for example: block size, number of rounds, key size, encryption and decryption time, scalability, security rate, throughput time and power consumption. It provides resources like infrastructure, platform, software, networks, servers, storage and applications. In the real life software online business applications (e-business, e-commerce), web-mails (Gmail, rediff), social networking sites such as Face book, twitter and LinkedIn and online data storage are available.
.

Panda [34] has proposed a new cryptography algorithm through an integrated method to improve data security and privacy with three types of computing resources. For each type consume significant, such as CPU time, memory, and battery power. It is one of the best methods to execute a public key cryptosystem whose security is based on the complexity of factoring big prime numbers. The proposed methods of this section take public key cryptosystems for key exchange digital signatures of blocks of data. It is also used for the authentication of a digital data and made it available in the public domain. A digital signature needs a public secrete key system to use the private and public key of the sender and receiver user.

V. PRIVACY PROTECTION TECHNIQUE

Chuang et al. [35] have proposed a technique on privacy and data protection, in which they developed a full encryption method. This method allows data to be processed without being decrypted. Privacy is a dynamic idea, and how to evaluate the quality of various encryption algorithms. In this section, we depict a Cloud Data Protection System (CDPS) that incorporates the point by point EPPS and its basic ideas. The Effective Privacy Protection Scheme (EPPS) is proposed to give the proper security insurance which is fulfilling the user demand protection necessity and looking after framework execution at the same time. In figure 4 show the privacy architecture of CDPS, the choosing security system in the best half decides a creation of encryption algorithm and the division numbers to secure clients' data. The base half is information assurance stream that data will be secured by executing system choosing security creation. The system contains four main important components - Privacy analysis, Quantification models, Data protection procedure, and Data division.

- ➢ Privacy requirement of user's data is to provide privacy for the most appropriate security on demand and update frequency of key which is used to encrypt data. Various types of data stored in the cloud storage like email, video and image.

- The quantification models are including the protection and speed phases. To make this quantification model the users' trust to believe that provider cannot disclose their data to attackers. Thus we want to propose clock rotations megabyte per second when performing each encryption algorithm in a specific mechanism.
- The data division is an important model that is used to build data more secure. The analysis result and quantification data are used by data protection procedure.
- The data protection procedure is the kernel system of Cloud Data Protection System (CDPS) and its major aim is to obtain the work of encryption algorithm. The major aim of Data Protection Procedure is obtaining the best work of encryption algorithm and number of division by objective function and constraint.

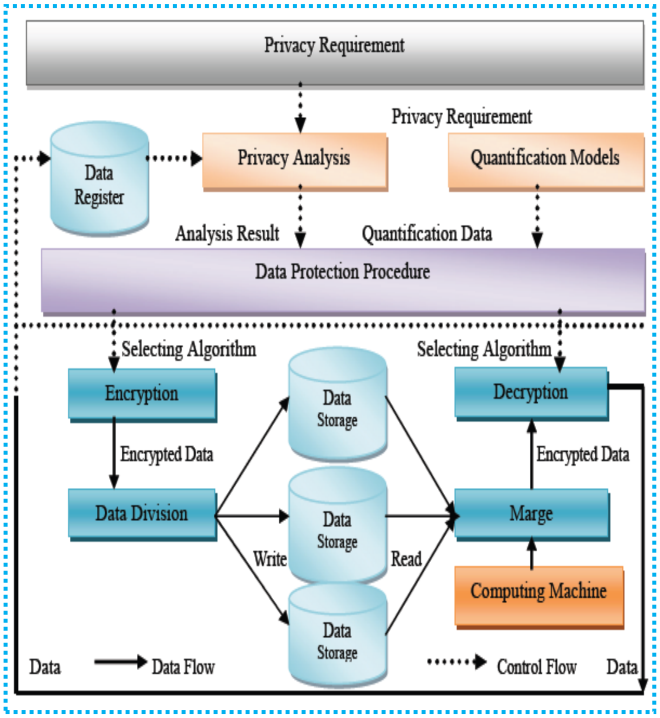

Figure 4: Privacy CDPS Architecture

5.1 Analysis Requirement for Privacy Technique

There are many privacy requirements of cloud computing that proposed basic execution time of an encryption algorithm and number of data division is stored in the cloud. Data stored in the cloud storage are various types, like email, video, image etc. The privacy level requirement is defined by users. Users can configure the privacy level according to their data concerning, how much sensitive information is and the level of security they want. Privacy requirement techniques are at more than three levels:

- **Privacy Level One:** At this level no sensitive information is present in the cloud. Clients want to use the weak encryption work to attain more performance for using cloud services.
- **Privacy Level Two:** At this level data includes some sensitive data. If the data uses the weak encryption for security, clients will concern about that the sensitive information that can be easily disclosed. However, clients also want the performance of required cloud services to be fast.
- **Privacy Level Three:** At this level the information can controls all important information. In this protection of the data security, clients prefer to give up routine to ensure the confidentiality.

5.2 M-PIN Server 2FA Authentication Technique

Nagar et al. [36] proposed M-pin authentication server techniques that maintain 2FA where, the client is verified through cryptography. This technique uses the security in such a way that the hacker or attacker cannot get into it and compromise its integrity. This security key technique works in two phases. During the first phase which is issued by an appropriated distributed trusted authority (D-TA) hub within the M-pin managed cloud services. The second phase of the secrecy is issued by the client hosted D-TA utilizes a zero-learning verification confirmation, strong, elliptic curve based cryptography. So this approach 2FA verification innovation enables undertakings to ensure client certifications and to reduce the quantity of affairs identified with unauthorized access and accreditations in the IT environment. Here this section is the investigation of security issues and difficulties for the cloud computing in authentication level and proposed a computing technique to secure private information, and essential data about the client. An M-pin PINPAD user identification acquires the end client's pin and it is joined M-pin client security key. The M-pin PINPAD used in ATM server's administration domain can get to the M-pin token put away in the client's program.
Kapoor [37] has proposed a new integrated cryptographic algorithm included MD5 scheme to improve data security. MD5 algorithm generates a 128 bit output as a message digest of plaintext. Proposed a new integrated cryptographic algorithm uses four major securities such as authentication, confidentiality, integrity of data and non-repudiation, when a given data is sent from sender to receiver.

5.3 Key Rotation for Data Security in Cloud System

Prakash et al. [38] have proposed an Attribute Based Encryption (ABE) and verifiable data decryption technique to provide data privacy in cloud based method. Key rotation is an important measure for both encrypted and decrypted based algorithm on the user requested elements of the outsourced. It can help to access the outsourced encrypted file from the cloud service provider. The key is an essential component which describes the criteria for choose key character for cover the block character of a record. If a selected block character outer the range of key size, then modulus of block character location to key size is executed to fetch a key.

Priyanka and Dasgupta [39, 40] proposed Genetic Algorithm (GA) optimization technique is used to gain the growth points one which give up parallel response model. For this purpose, one can minimize the error between the response of the model and that of designed closed loop method. Optimization technique can be used to obtain better support and response growth point of model.

A similar work proposed another algorithm using a novel load balancing approach. The load balancing approach has been simulated by using cloud Analyst simulator. It is analyzed that Genetic Algorithms for cloud computing to find a global optimum processors for job in a cloud.

5.4 *Privacy preserving Biometric Identification Technique*

Changhee et al. [41] have proposed privacy biometric identification, which is one of the major techniques to identify an individual client. The proposed biometric identification of this section, such as fingerprint, iris, and retina, share the very important factors of universality. Thus recently several studies, privacy preserving identification method which is used an asymmetric homomorphic encryption algorithm to encrypt data, so that only key owners can access their actual fingerprints data.

Pseudo Random Number Generator (PRNG) technique is proposed by John [42]. Adoption issues of cloud computing are divided into several categories here such as availability, security, performance, compliance, private cloud, integration and environment in premises of cloud. Cloud security issues have recently gained a lot of attention from research community, with much of the focus on securing the OS and VM on which the services are deployed. Sometimes it happens that without awareness of company's detail user record their data; companies may send user's sensitive information to other companies for the economic reason, by transformation of data, a cyber criminal may steal the user email and bank's detail etc. The awareness is also increased because of the need for designing a privacy mechanism for both companies and government organization. So design techniques are required to protect the privacy in cloud computing, must get together and they must be maintained despite the changes of data.

VI. Algorithms for Privacy Cloud Computing

A lot of research has been done in the field of cloud computing with respect to its challenges and privacy. The proposed work intends to improve the privacy of cloud computing. It is also aimed to find out the preferred issue that makes them high level security concerns in cloud computing, such as data integrity, application deployment and privacy of sensitive information.

Nowadays, some researchers focus on cloud data storage security in cloud computing, mobile computing, grid computing, web hosting and privacy. This research work involves the optimization of the issues associated with these clouds, using a simple optimizing privacy technology known as open stack platform method to solve these privacy problems in cloud computing. Some noticeable work related to this area of research is given as follows:

6.1 *RSA: Algorithm Implementation in Cloud Computing*

Saravanan [43], has used Ron Rivest, Adi Shamir and Leonard Adleman (RSA) algorithm. The method is providing privacy by implementing RSA algorithm using cloud SQL to the data that will be stored in the third party. RSA algorithm performs three steps through the Key Generation algorithm, known as the encryption exponent or public key exponent, then finding two distinct prime numbers, all the values are relative, and public key and private key must be kept secret. Using second encryption algorithm, sender transmits the public key to the recipient for the process of encryption data. And third Decryption algorithm, known as the decryption exponent or private key exponent, the recipient uses a private key to decrypt the plaintext from the message received.
Encryption: Plaintext: $M<n$ Cipher text: $C=M^e$ (Mod n)
Decryption: Cipher text: C Plaintext: $M=C^d$ (Mod n)
There are two promoter exponents' e and d, where e is a public key and d is private key. And also where, M is the plaintext, C the cipher text and n is the very large number, created during the key generation process.

6.2 *DES Algorithm*

Singh et al. [44, 45] have proposed data security system executed into cloud storage. Data Encryption Standard (DES) algorithm was described in 1970 by triples DES (3DES). 3DES runs are exactly three times slower than DES, but is much more secure and support if used properly, it means performs 3 iterations of DES encryption on each block. Data privacy systems implemented into cloud computing using DES algorithm is available. This Cipher chain block system is used to secure data for customers and server. The privacy architecture of the system is designed by using DES Cipher chain block, which eliminates the fraud that occurs today with stolen data. DES executes an original transformation on the entire 64 bit block of data. In encryption site, DES takes a 64-bit plaintext and creates a 64-bit cipher chain block, in decryption site, it takes a 64-bit cipher chain block and creates a 64-bit plaintext, and same 56-bit cipher key is used for both encryption and decryption algorithm.

6.3 *AES: Advanced Encryption Standard Algorithm*

Mahajan et al. [46] proposed (AES) algorithm for new security as well as is much faster than other algorithms amazing speed. This algorithm is the main powerful modern encryption known against it, in which the attacker seeks to test every one of the characters, merges to open the encryption. Because both software and hardware usage are even faster. It has variable key length of 128, 192, or 256 bits; default 256. It encodes in sequence squares of 128 bits in 10, 12 what's more, 14 round contingent upon the key size. AES encryption is a fast and flexible algorithm for whole cloud storage exists in main memory. It can be actualized on different stages especially in small implement. It is analyzed carefully tried for some security applications.

6.4 DSA: Digital Signature Algorithm

In order to improve the performance of DSA federal information processing standard for computerized signatures, it was proposed by the National Institute of Standards and Technology (NIST) in August 1991 for use in their Digital Signature Standard (DSS) and received as Federal Information Processing Standard (FIPS) 186 of year 1993. Now a day’s digital signature is used to verify the cloud server systems. Different methods for signature can be used. This increases the computational time but helps to maintain the security code. Digital watermark can also be used as a technique for a unique identification number. Four modifications to the underlying determination have been discharged: FIPS 186-1 out of 1996, FIPS 186-2 out of 2000, FIPS 186-3 out of 2009, and FIPS 186-4 out of 2013. The performances of DSA become designed as an encryption algorithm to assure privacy and security of data is also preferred faster key technology. It is critical to the point that abusing any one of those three prerequisites can uncover the whole private key to an attacker. Utilizing to a similar regard twice (even while keeping k secrecy), consume an anticipated regard. This algorithm releasing even a pair of bits of k in each of a few marks is sufficient to break [47].

6.5 SKA: Secure Keyless Algorithm

Hebiya [48] has proposed a secure key-less algorithm for useful storage of data in cloud storage server. Secure Key-less algorithm (SKA) algorithm represents the functionality of encryption process, without any key and applies the different type of logical process as well as shift functions to the cloud data. To analyze the new way of data protection method to enhance the security against cross site scripting (XSS) attacks in cloud storage. This secure key-less algorithm (SKA) is to provide the better performance outcome with existing systems and effective data storage in the cloud.

6.6 TBDS: Token Based Data Security Algorithm

Seth et al. [49] proposed a new technique to develop data security during data transmission. A relationship between the cloud client and cloud service source leads to getting a combined exploit for performing data in cloud computing. Giving information security amid online information transmission between the cloud customer and cloud specialist run in a reasonable way. This Token Based Data Security (TBDS) algorithm is a calculation that makes different information will be gotten to by the validated client without impedance of deposit. When the cloud client (CC) will send ask for the cloud space from cloud specialist organization then the customer must need to enlist first, and make another record for getting to any administration on cloud. After, recruitment the cloud client will move to second resources, to state his/her own enrollment. When cloud client progresses toward becoming individual from cloud and cloud service provider are auto-created unique Token_ID for future messages. When cloud retailer sends ask for information exchange then it in the first place confirms the transfer Token_ID for particular kind of cloud benefit, and if the allocated Token_ID will coordinate, at that point information will be exchanged or gotten starting with one end then onto the next end.

6.7 Privacy Manager Algorithm for Cloud

Rao [50] has proposed privacy manager algorithm, that counters challenges faced by privacy in cloud computing. A privacy manager helps in storing the consumer private data in the cloud server, securing it by using the technique of strict privacy. That is this technique is obfuscation privacy law. Privacy manager software on the client system helps users to protect their data when accessing cloud services. And also it may be deployed in a private local cloud network, to protect information relating to multiple social gathering. The basic architecture of privacy manager client is shown in figure 5 Privacy manager provides an obfuscation service, which is reducing the amount of sensitive information in the cloud.

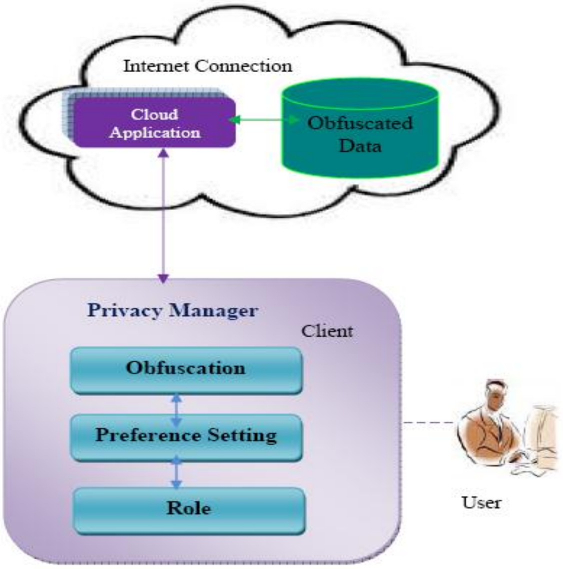

Figure 5: Privacy Manager Client

VII. PROVISIONING AND MIGRATION OF VIRTUAL CLOUD

In this section, we will have an overview on the provision and its migration major potential status of virtual cloud. Virtual cloud environment are easier than in traditional computing. Here, we describe the taxonomy of provisioning virtual cloud server. In the first position, you have to choose a server and second, you have to load the software programs. Third, you have to customize and arrange the virtual machine and last, the cloud virtual server is prepared to begin with its recently loaded software. It may also be a migration virtual cloud, it is process of moving a virtual machine from one host cloud server to storage location. There are various examples of migration techniques, real time, anatomy, Xen Hypervisor, and Web server. In the literature, some virtualization software services are given below:

VM Management Using Open Nebula

Buyya et al. [51] proposed virtual solution model the structure of a multi-machine virtual software service. Open nebula is an open source and flexible tool that uses existing data center's environments to build any type of cloud deployment. Open Nebula can be primarily used as a virtualization tool to manage your virtual infrastructure, which is usually referred to as private cloud. The Open Nebula tools are compared with different parameters such as hybrid cloud to combine local infrastructure with public cloud-based infrastructure, enabling highly scalable hosting environments. This tool is supporting several research outlines in advance reservation of capacity, probabilistic admission control, placement optimization, resource models for the efficient management of groups of virtual machines, elasticity support.

Cloud Platform Virtualization

Cloud computing commonly relies on a virtualization platform. Clients give their own particular virtual machines and the cloud supplier runs them regularly without information of the OS or their configurations. Cloud providers offering security as a service based on virtual machine introspection assure the finest of both scenarios, it centralizes visitor protection into a security. VM which supports Linux and windows operating systems and can be easily extended to support new operating systems. A mobile device can get resources from an external source such as cloud platform. However, an access to these platforms isn't generally ensured to be accessible and is expensive to access them; virtual cloud platform using mobile phones are imported solution in privacy [52].

Environments of Virtual Machine

Jansen [53, 54] has proposed virtual machine environment key issues, which are recognized to long-term significance in cloud computing security. The issues have been organized into several categories: trust, architecture, identity management, software separation, data protection and availability. Since security and privacy issues are important to cloud computing, as related to outsourcing portions of the organizational computing environment. It points out areas of concern with public clouds that require special attention and provides the necessary background to make informed security decisions. Although the emergence of cloud computing is recently made, insights into the critical aspects of security. The basis experiences of early adopters and also researchers are still analyzing and experimenting. Here this section is a description of some known hardened browser environments from research organization.

In figure 6 we controlled cloud computing privacy as shown below. It contains three main phases: privacy categories, privacy service models and privacy scope. There are many privacy requirements of cloud computing where data is stored. Here privacy scope very important dimension is the cloud that contains an implementation of the various algorithms for the different task of cloud computing such as privacy area, risks, and threats.

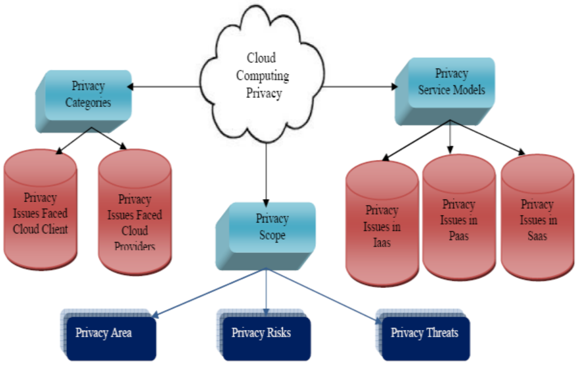

Figure 6: View of Cloud Computing Privacy

Virtual Machine in Cloud Computing

Virtual machine is also a significant research area in the field of cloud virtualization, such as VMware, Xen and KVM is virtualization. Virtual machines could be supplied by the same underlying host machine in an Infrastructure as a Service (IaaS). There is various migration techniques are used to achieve cloud virtualization. A one-migration technique is used by Xen known as live migration VM which is useful in power consumption and energy saving from the data center. Further it is extended to call as green cloud, which the latest aspect of cloud networking [55, 56].

Salient Features of Cloud Computing

There are various features that make proposed framework more suitable for analysis and evaluation of cloud computing. Some of them are given below:

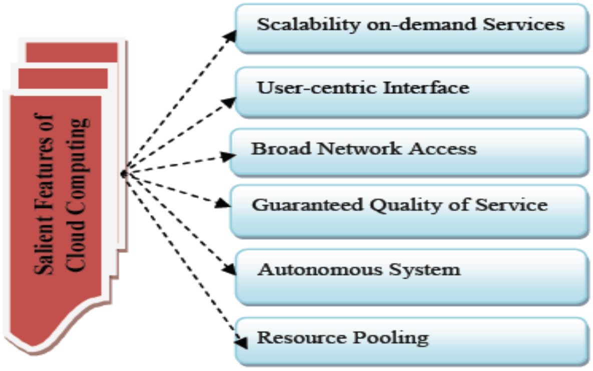
Salient Features of Cloud Computing
Scalability on-demand Services
User-centric Interface
Broad Network Access
Guaranteed Quality of Service
Autonomous System
Resource Pooling

Figure 7 : Features of Cloud Computing

- Scalability on-demand Services

One of the critical issues in cloud computing provides resources and services for users on demand. The resources are scalable over several data centers. Computing resources include processing power, storage, virtual machine etc.

- User-centric Interface

User cloud centric interfaces are location independent and can be accessed by well established interfaces, such as web services and internet browsers. The administration got must be modifiable by the customer association without reaching the facilitating supplier.

- Broad Network Access

The broad network access previously mentioned resources can be accessed over a network using heterogeneous devices, such as laptop, Desktop, Smartphone, Tablet device. Broad system gets to is normally expert by utilizing the inherent web program for the gadget, as it is one of the most pervasive customers accessible.

- Guaranteed Quality of Service

Cloud computed can guarantee QoS for users in terms of hardware, CPU performance, bandwidth, and memory capacity.

- Autonomous System

The cloud computing systems are autonomous systems managed transparently by users. However software and data inside clouds can be automatically reconfigured and consolidated to a simple platform depending on user need.

- Resource Pooling

Resource pooling is the concepts that are shared by multiple users. It means cloud service providers pool their resources multiple organizations can share the cloud infrastructure. This is referred as multi-tenancy where for example a physical server may host several virtual machines belonging to different users [57].

VIII. CONCLUSION

In this review paper, we have summarized the research papers related with the study to search a list of aspects. To use of these privacy techniques the work is to provide security to the stored data in the cloud storage. We conclude that workload both secret key and authorized user to get secure systems maintained the high security code. We focus on high level privacy and security to the data which is secured in cloud server system. The future work will focus on more privacy for cloud storage by using different cloud techniques to improve potency based on a digital signature processing algorithm.

REFERENCES

[1] Ranchal et al., “Protection of Identity Information in Cloud Computing without Trusted Third Party”, 2010 29th IEEE International Symposium on Reliable Distributed Systems, pp. 368-372, 2010.

[2] Z. Xin et al., “Research on Cloud Computing Data Security Model Based on Multi-dimension”,International Symposium on Information Technology in Medicine and Education, IEEE, pp. 897-900, 2012.

[3] Rao, Srinivasa and V Nageswara Rao, “Cloud Computing: an Overview”, Computing, pp71-76, 2009.

[4] Mell, Peter and Timothy Grance, “The NIST Definition of Cloud Computing”, National Institute of Standards and Technology, 2011.

[5] Mitra, A., & Kundu, A., “Cost optimized set of Primes Generation with Cellular Automata for Stress Testing in Distributed Computing”, International Conference on Computational Intelligence: Modeling Techniques and Applications (CIMTA) Procedia Technology, 10, Elsevier, pp 365-372, 2013.

[6] A.S. Tanenbaum and M. Van Steen., “Distributed systems: principles and paradigm”, prentice Hall PTR, Upper Saddle River, NJ, USA, 2001.

[7] C.S.R.Prabhu, “Grid and Cluster Computing”, 2012.

[8] Yeo, C. S., Buyya, R., Pourreza, H., Eskicioglu, R., Graham, P., & Sommers, F. “Cluster Computing: High-Performance, High-Availability, and High-Throughput Processing on a Network of Computer. Communication”, 1-24.

[9] R, Buyya, “High-Performance Cluster Computing: Architecture and system”, prentice Hall PTR, NJ, 1999.

[10] William Maples, “ High Performance Computing, Grid Computing”

[11] Zhang, M. A. Z. Y. D. P., “Adoptability of grid computing technology in power systems analysis, operations and control”, Engineering and Technology, 2009.

[12] Yeo, C. S., Buyya, R., Assunção, M. D. D., Yu, J., Sulistio, A., Venugopal, S., et al.,”Utility Computing on Global Grids Benefits of Utility Computing”. Group, 1-26.

[13] R. Buyya et al., “ Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities”,2008.

[14] A. Jansen,” Cloud Hooks: Security and Privacy Issues in Cloud Computing”, Proceedings of the 44th Hawaii International Conference on System Sciences, pp 1-10, 2011.

[15] N. Provos, “The Ghost In The Browser Analysis of Web-based Malware”, USENIX Association, 2007.

[16] D.Tao, " Cloud Platform Based Automated Security Testing System for Mobile Internet", Tsinghua Science and Technology, Vol. 20, Number 6,pp. 537-544, 2015.

[17] Hebiya et al., "Secure Data Storage Framework using Anti-XSS in cloud", International Journal of Innovative Research in Science, Engineering and Technology, Vol.4, Issue 11, pp. 11429- 11436, 2015.

[18] Kaushik et al., "Keyless User Defined Optimal Security Encryption", International Journal of Computer and Electrical Engineering, Vol.4, No.2, pp. 99-103,2012.

[19] Gholami et al., "Big Data Security and Privacy Issues in the Cloud", International Journal of Network Security & Its Applications, Vol.8, No.1, pp.59-79, 2016.

[20] Tang et al., "Multi-Tenancy Authorization Models for Collaborative Cloud Services", International Conference on Collaboration Technologies and Systems, IEEE Xplore: pp.132-138, 2013.

[21] Goyal et al., "Veracity Aware Defense Algorithm (VADA) for Cloud computing environment", pp. 57-68.

[22] K. Malviya et al., "On Security Issues in Web Applications through Cross Site Scripting (XSS)", 20th Asia-Pacific Software Engineering Conference, pp.583-588,2013.

[23] Mircea, "Addressing Data Security in the Cloud",International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol.6, No.6,pp.798-805, 2012.

[24] K. Dhanabakiyam,V. Divya,"Enhanced Protection Over Data Streams under Multiple Keys in Cloud", International Journal of Advance Research, Ideas and Innovations in Technology, Vol. 4, Issue 2,pp.439-442,2018.

[25] Vijai et al., "An Efficient Framework Security Model of Sharing Data for Privacy Protection and Performance-Based Outsource Data Sharing on Cloud",International Journal of Advance Research, Ideas and Innovations in Technology, Vol.4, Issue 2,pp.297-304,2018.

[26] Viswanadham et al., "Security Issues in Cloud Computing and Associated Mitigation Techniques",Advances in Information Science and Computer Engineering,pp. 528-540.

[27] D.Bein, "The Impact of Cloud Computing on Web 2.0", Economy Informatics, vol. 9, no.1,pp.9-12, 2009.

[28] J. Kumar et al., "Analysis of Security Vulnerabilities for web Based
Application", Fourth International Conference on Advances in Recent Technologies in Communication and Computing, pp.233-236,2012.

[29] H.Albaroodi et al.,"A Proposed Framework for Outsourcing and Secure Encrypted Data on OpenStack Object Storage (Swift)", Journal of Computer Science, 11 (3), 590-597, 2015.

[30] N.Nagar and U.Suman,"Architectural Comparison and Implementation of Cloud Tools and Technologies",International Journal of Future Computer and Communication, Vol. 3, No. 3,pp.153-160, 2014.

[31] T. Sivasakthi and N. Prabakaran, "Applying Digital Signature with Encryption Algorithm of User Authentication for Data Security in Cloud Computing", International Journal of Innovative Research in Computer and Communication Engineering,Vol. 2, Issue 2, pp. 3102-3107, 2014.

[32] S.Singh et al.,"Analysis of EnDeCloudReports for Encrypting and Decrypting Data in Cloud", International Journal of Computer Applications, Vol. 136 – No.12,pp.12-16, 2016.

[33] K. Sarita, J. Thakur,"Data Centric Security Algorithms In Cloud Computing - A Review", International Journal for Research in Applied Science & Engineering Technology, Vol.5 Issue X,pp.1155-1160, 2017.

[34] M.Panda, "Performance Analysis of Encryption Algorithms for Security", International conference on Signal Processing, Communication, Power and Embedded System,2016.

[35] Chuang et al., "An Effective Privacy Protection Scheme for Cloud Computing", pp.260-265,ICACT,2011.

[36] N. Nagar and U. Suman,"Two Factor Authentication using M-pin Server for Secure Cloud Computing Environment", International Journal of Cloud Applications and Computing, 4(4), pp. 42-54,2014.

[37] V. Kapoor, "A New Cryptography Algorithm with an Integrated Scheme to Improve Data Security", Int. J. Sci. Res. In Network Security and Communication, Vol.1 Issue 2,pp.39-46, 2013.

[38] Prakash et al., "Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud System", International Journal of Engineering and Computer Science, Vol.3 Issue 4, pp. 5215-5223, 2014.

[39] Priyanka et al., "A New Approach for Design of Model Matching Controllers for Time Delay Systems by Using GA Technique",Journal of Engineering Research and Applications, Vol. 5, Issue 1, pp.89-99 ,2015.

[40] K. Dasgupta et al., "A Genetic Algorithm (GA) based Load Balancing Strategy for Cloud Computing",International Conference on Computational Intelligence: Modeling Techniques and Applications, pp. 340 – 347, 2013.

[41] Changhee H., J. Hur,"Efficient and privacy-preserving biometric identification in cloud", The Korean Institute of Communications Information Sciences, Publishing Services Elsevier, pp.135-139,2016.

[42] John et al.,"Cryptanalytic Attacks on Pseudorandom Number Generators", pp. 1-22.

[43] N. Saravanan et al., "An Implementation of RSA Algorithm in Google Cloud using Cloud SQL",Research Journal of Applied Sciences, Engineering and Technology 4(19), pp.3574-3579, 2012.

[44] G.Singh, supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security",International Journal of Computer Application, Vol. 67– No.19,pp.33-38, 2013.

[45] Karthik S. et al.,"Data Encryption and Decryption by Using Triple DES and Performance Analysis of Crypto System",International Journal of Scientific Engineering and Research,Vol. 2 Issue 11, pp.24-31, 2014.

[46] P.Mahajan et al., "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network, Web & Security,Vol.13 Issue 15 Version 1.0, pp.15-22, 2013.

[47] R. Kaur ,S. Kinger, "Analysis of Security Algorithms in Cloud Computing",International Journal of Application or Innovation in Engineering & Management, Vol.3, Issue 3,pp. 171-176, 2014.

[48] Hebiya et al., "Secure Data Storage Framework using Anti-XSS in cloud",International Journal of Innovative Research in Science,Engineering and Technology, Vol.4, Issue 11, pp.11429-11436, 2015.

[49] R. K. Seth, et al., "TBDS- A New Data Security Algorithm in Cloud Computing", International Journal of Computer Science and Information Technologies, Vol. 5 (3) , pp., 2703-2706, 2014.

[50] D.Rao et al., "A Design of Cloud Privacy Manager Algorithm", International Journal of Computer Science and Network Security, Vol.12, No.7,pp.36-41, 2012.

[51] Buyya et al., "Cloud Computing Principles and Paradigms".

[52] Mihai et al., "Cloud Security Is Not (Just) Virtualization Security", CCSW-09, 2009.

[53] A. Jansen, "Cloud Hooks: Security and Privacy Issues in Cloud Computing", Proceedings of the 44th Hawaii International Conference on System Sciences, pp 1-10, 2011.

[54] Dale L, "Virtualization Technologies in Information Systems Education", Journal of Information Systems Education, Vol.20 (3), PP.339-348.

[55] M. A. Vouk,"Cloud Computing – Issues, Research and Implementations", Journal of Computing and Information Technology - CIT 16, 4, pp.235–246, 2012.

[56] M.Komu et al., "Secure Networking for Virtual Machines in the Cloud", IEEE International Conference on Cluster Computing Workshops,pp. 88-96, 2012.

[57] B. Furht and A. Escalante, "Handbook of cloud computing", Springer New York Dordrecht Heidelberg London, ISBN 978-1-4419-6523-3, 2010.