International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 3 | ISSN : 2456-3307

A Study on Cloud Computing Securities and Algorithms

M. Subhashini [1], Dr. P. Srivaramangai[2]

[1]Research Scholar, Department of Computer Science, Marudupandiyar College(Affiliated to Bharathidasan University), Thanjavur, Tamilnadu, India

[2]Associate Professor, Department of Computer Science, Marudupandiyar College(Affiliated to Bharathidasan University), Thanjavur, Tamilnadu, India

ABSTRACT

Cloud computing is that describe about a digital era of an Internet-based computing and after that step evolution of the internet access. It has received important attention in current years, however security protection issue is one of the main inhibitor for reducing the development of cloud computing. In this Cloud computing technology there are a group of important policy issues, which include several issues of privacy, security, anonymity, telecommunications capacity, government surveillance, reliability, and liability, compare among others. However the most important between them is security protection and how cloud provider assures it. In this paper, we have a tendency to discussed about introduction of cloud computing and security concerns after that number of symmetric and asymmetric algorithms like DES, 3DES, AES, RSA, ECC, Blowfish etc.

Keywords: Cloud Computing,Security, AES, DES, 3DES,RSA,ECC

I. INTRODUCTION

Cloud computing is that the delivery of computing services over the Internet. Cloud services allow individuals and businesses to utilize system software and hardware that are managed by third parties access at remote locations. Examples of cloud services contain webmail, online file storage, online business applications and social networking sites. The cloud computing model permits access to computer resources and information so that a network connection is available from anyplace. Cloud computing makes available a shared pool of resources, together with data storage space, networks, computer processing power, and user applications and specialized corporate company. Cloud computing is a model for enabling as more convenient, on-demand network services access to a shared pool of configurable computing resources (e.g., servers, storage, applications, networks, and services) that can be quickly provisioned and released with minimal management effort or interaction between service providers. As a result of these benefits each and every organization are transmitting their data to the cloud. Therefore, there is a necessity to protect that data against unauthorized access from anywhere, modification or denial of services, etc. The Cloud means that to secure storage (the Cloud provider hosted databases) and the treatments (calculations). Three important points are namely to secure data. They are Availability, Confidentiality, and Integrity. Cryptography is accomplished Confidentiality of data in the cloud storage. In Cryptography concept, the combinations of three types of algorithms have been considered in recent days. They are (1) Symmetric-key algorithms (2) Asymmetric-key algorithms and (3) Hashing algorithms. In Hashing algorithms is ensured Integrity of data.

Data cryptography is mainly considered as the scrambling of the content of the data, like text, image, audio, video and so as to make the data unreadable, meaningless or invisible during transmission or storage is termed Encryption. The main intention of cryptography is to make sure of data security from invaders. The opposite process of receiving back the original data is encrypted after that Decryption process handle, which restores the original data. Using symmetric-key and asymmetric-key algorithms are to encrypt data at cloud storage. Cloud storage contains a large set of databases for storing files and important documents. A large database asymmetric-key algorithm's is performed slower when compared to symmetric-key algorithms.

II. OVERVIEW OF CLOUD COMPUTING

In Cloud Computing, we discuss about a distributed architecture that centralizes server resources on a scalable platform, so that provide for cloud services and on-demand computing resources. Cloud service providers (CSP's) suggest cloud platforms for their customer's satisfaction by utilizing and creating their web services. Internet service providers (ISP's) offer costumers to improve the high speed broadband to access the internet. CSPs and ISPs (Internet Service Providers) together offer services. Cloud computing is a vital model that allows more convenient to access, on-demand network access to a shared pool of configurable computing resources like networks, servers, storage, applications that can be quickly provisioned and released with service provider's interaction or minimal management effort. In general, cloud suppliers offer three kinds of services, i.e. software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). There are several reasons for organizations to move towards IT solutions that include cloud computing as they are simply required to pay for the resources on consumption basis.

Clouds are the evolution of the distributed systems in the innovative trend, the predecessor of cloud being the grid. The user does not able to require expertise or acquaintance to control the infrastructure of clouds; it provides only abstraction concept. It can be developed as a service of an Internet with increase scalability, higher throughput, improves quality of service and computing power. Cloud computing providers deliver frequent online business applications, which are accessed through a web browser from servers [1].

2.1 Characteristics of Cloud Computing

- **Ultra large-scale:** In ultra large-scale computing, the scale of cloud is large convergence. The cloud of Google has owned more than one million servers access. For example, IBM, Microsoft, Yahoo, Rediff, Amazon they have more than hundreds of thousands servers. There are hundreds of servers in an enterprise control access.
- **Virtualization:** Cloud computing makes user to get access service everywhere, through any type of terminal. Everything you can complete the process through an internet service by using a notebook PC or a smart phone or a Tablet or a Laptop. Users can achieve or share it securely through a simple way, anytime, anywhere. Users can complete a task that can't be completed in a single computer.
- **High reliability:** Cloud applies data multi transcript fault tolerant, the computation node isomorphism exchangeable and so as to improve and ensure the high reliability of the cloud service.By using cloud computing is highly reliable than local computer process interaction.
- **Versatility:** Cloud computing can produce several types of applications supported by cloud service, and single cloud can maintain different applications running at the same time.
- **High extendibility:** The scale of cloud can highly extend or dynamically prefer to meet the increasing requirement of cloud services.

- **On demand service:** Cloud is an enormous resource pool, which will you can pay according to your requirement; cloud is just like that running water, electric, and gas that can be charged by the amount that you used.
- **Extremely inexpensive:** The targeted management of cloud makes the enterprise needn't undertake the management cost of the data center that increase speed of the management. The versatility can improve the utilization rate of the accessible resources compared with traditional systems, thus users can totally enjoy the cloud service and low cost as an advantage or extremely inexpensive.

2.2 Cloud Computing Entities

Cloud consumers and providers are the two major entities within the business market. However, the cloud service brokers and cloud resellers are the two more emerging service level entities within the Cloud world market.

These are discuss as below,

- **Cloud Providers:** Comprises Internet service providers, huge business process outsourcers and telecommunications companies that offer moreover the media (Internet connections) or infrastructure (hosted data centers) that allow consumers to access cloud services. Service providers can also include systems integrators that create and support data centers hosting private clouds and they offer different services (e.g., SaaS, PaaS, IaaS, and etc.) to the consumers, resellers or the service brokers [2].
- **Cloud Service Brokers:** In the selection of cloud computing solutions, it includes technology consultants, registered brokers and agents, business professional service organizations, and influencers that help to support guide the consumers. Service brokers concentrate on the concession of the relationships within consumers and providers without managing or owning the entire Cloud infrastructure. Furthermore, they add extra services on top of a Cloud provider's infrastructure to make up the user's Cloud environment.
- **Cloud Resellers:** Cloud providers will develop their business across continents before that Cloud Resellers can turn into an important factor of the Cloud market. Cloud providers can select resellers of their existing products or local IT consultancy firms to proceed as "resellers" for their Cloud-based products in a particular county.
- **Cloud Consumers**: End users belong to the type of Cloud consumers. However, also Cloud resellers and Cloud service brokers can belong to this category as soon as they are customers of an additional Cloud provider, reseller or broker. In the next stage, we discuss about key advantages of possible risks and threats for Cloud Computing are listed [3].

2.3 Service Models of Cloud Computing

Cloud computing utilizes a service-driven business model. In other words, platform-level resources and hardware are provided as cloud services in an on-demand based process. Abstractly, clouds offer services is grouped into three categories: software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS).

- **Yes (Infrastructure as a service):** IaaS offers computers physical or (more often) virtual machines and other resources from providers. IaaS refers to online services with the purpose of abstract the user from the details of infrastructure such as backup, security protection, location, scaling, data partitioning, physical computing resources etc.
- **Paas (Platform as a service):** PaaS sellers offer a development environment to application developers. The provider typically develops standards and toolkit for improving the development and channels for distribution and payment process. In general the PaaS models, cloud providers deliver a computing platform together with the operating system, database,

programming-language execution environment and web server.

- **Saas (Software as a service):** In the SaaS model, cloud providers is mainly describe about how to install and operate application software within the cloud and cloud users access the software from cloud clients. Cloud users do not handle platform and the cloud infrastructure wherever the application processed or runs. Data is the essential aspect in all these architectures of cloud services. Data is a critical resource for several organizations, institute or individual. The data security authentication of cloud systems rest on the classical principles of availability, protectivity and integrity, however applied to distributed, virtualized, and dynamic architectures by using the cloud systems. Data security is especially important for the client side of cloud computing. In cloud computing, the main concern is to provide the security authentication to end user to safeguard files or data from unauthorized user. Security authorization is the main purpose of any technology cannot access your file or data in cloud services through that unauthorized intruder. This implementation can assist to encrypt and decrypt the data at the user aspect that provide security for data at rest similarly as whereas moving to the next stage. This model can utilize EAP-CHAP encryption similarly as an RSA encryption algorithm. This will provide authentication similarly as Security authentication to the data.

2.4.Cloud Deployments Models

- **Private Cloud:** Private cloud is mainly to describe about a model of a new term that various vendors have recently used to explain offerings that replicate cloud computing on private networks. The private network is providing a set of connections within an organization's internal enterprise data center. In the private cloud, the cloud vendors are pooled together and available for cloud users to share and utilize to provide scalable resources and virtual applications. Only the organization and designated stakeholders may possibly have access to operate on a specific Private cloud [4].
- **Public cloud:** A public cloud is one of a model that allows users access to the cloud services and infrastructure and are provided off-site over the Internet [5]. It is typically based on a pay-per-use model, related to a prepaid electricity metering system which is flexible enough to cater for spikes on demand cloud services for cloud optimization. Public clouds are handled by vendors or third parties access over the Internet. Public clouds are less secure comparing than the other cloud models for the basis that it places an additional burden to ensure whole applications and data accessed on the public cloud are not focussed to malicious attacks. On the other hand, security and governance issues must be well planned and ample security access controls were located in any place.
- **Hybrid cloud:** In this model, a new idea combining resources from both external and internal providers will develop into the trendiest choice for enterprises mangagement. A hybrid cloud is mainly described about a combination of both public cloud model and private cloud model that aims to address the limitations of each approach. In a hybrid cloud, part of the service infrastructure runs in private clouds, whereas the left over part runs in public clouds. Hybrid clouds provide more flexibility than both public and private clouds. Particularly, they offer tighter security and control access over application data compared to public clouds, whereas still facilitating contraction and on-demand service expansion. On the down side, designing a hybrid cloud involves carefully determining the best split between private cloud components and public cloud components [6].
- **Community cloud:** The cloud computing community model is rarely offered; the infrastructure is shared for a shared cause and

will be managed a third party service provider or internally by many organizations. It brings along, in general, the structures with same interest (mostly security) and may even be within the same field of activity [7].

III. CLOUD COMPUTING SECURITY

The main concern is to protect security against unauthorized access of data. Data relocation on high level has negative implications for protecting the data safety and data security as well as data accessibility. Therefore the main apprehension with reference to safety of data residing within the Cloud is: at the remainder how to safe security and avoid unauthorization. Even though, customers understand the situation and no data mobility access, question with reference to security and confidentiality of data. The Cloud Computing area has no confusion become larger as a result of its accessibility and wide network access. However, we can also believe in terms of a secure and safe atmosphere for the personal data and information of the user is being needed.

3.1 Cloud Computing Security Elements

The cloud computing of the security elements is detailed about Data Integrity, Data confidentiality, Data availability, and Data privacy. In this paper explain the detail explanation about security elements of cloud computing as given below.

- **Data Integrity:** Data integrity is considered one of the most critical security elements in several information systems. In general, data integrity means that protecting data from unauthorized modification process, fabrication or deletion. Managing entity's rights and access to specific enterprise resources ensures that important data and services are not abused, illegal access, or stolen. Data integrity is definitely achieved in a standalone system with a single database. Data integrity in the standalone system is maintained through database transactions and constraints, which is frequently finished by a database management system (DBMS). Transactions ought to follow ACID (atomicity, consistency, isolation, and durability) properties to ensure data integrity. The majorities of databases are to support ACID transactions and can protect data integrity. Data integrity in the cloud system means that protecting information integrity. The data should not be modified or lost or by unauthorized users access. Data integrity is the basis to give cloud computing service like SaaS, PaaS, and IaaS. Moreover, data storage of large-scaled data, cloud computing environment typically provides data processing service. Data integrity can be obtained by using these techniques like digital signature and RAID-like strategies.
- **Data Confidentiality:** Data confidentiality is very important for users to store their confidential data or private information within the cloud services. In data confidentiality is used to ensure authentication and access control strategies. The data confidentiality, authentication and access control problems are mainly to protect in cloud computing might be self-addressed by improving the cloud reliability and trustiness [8]. As a result of the users don't trust the cloud providers and cloud storage service providers. These are virtually not possible to eliminate potential corporate executive threat; it is terribly dangerous for users to store and protect their sensitive data in cloud storage directly. The simple encryption process is faced with the key type management drawback and cannot support the advanced requirements like parallel modification, query, and fine-grained authorization. The cloud computing have several techniques for enhancing and developing data confidentiality. *1. Homomorphic encryption*: encryption is typically used to make sure the data confidentiality. Homomorphic encryption is a kind of encryption system to authority of the data. *2. Encrypted Search and Database*: Because the homomorphic encryption algorithm is

ineffective. The homomorphic encryption algorithm is the study of the applications of limited within the cloud environment researchers. Encrypted search is a general operation to protect data from unauthorized resources. *3. Distributed Storage:* In the Distributive storage of data is also a promising approach in the cloud environment. *4. Hybrid Technique.* A hybrid technique is projected for ensuring data integrity and data confidentiality, which uses both key sharing technique and authentication technique. *5. Data Concealment.* Data concealment is mainly used to maintain the data confidentiality in the cloud.

- **Data Availability:** Data availability mean that the following: when accidents occur like hard disk damage, IDC fire, electronic circuit failure, and network failures, the coverage that user's data are oftenly recovered or utilized and how the users verify their data by techniques rather than depending on the credit guarantee by the cloud service provider alone. The transboarder servers under the main issue of storing data is detail about a serious concern of clients for the reason that the cloud vendors are governed by the local laws and, as a result, the cloud clients must be cognizant of these laws. In addition, the cloud service provider should make sure the data security, notably data confidentiality and data integrity. The cloud provider should share and protect all such concerns with the client and establish trust relationship with this connection establishment. The cloud marketer ought to give guarantees of data safety and build a case for jurisdiction of native laws to the client's process management. Establishing data connection can support users to extend their trust relationship on the cloud. Cloud storage affords the transparent storage service for performing with users, which can reduce the cloud complexity, however, it also reduces the control ability of data storage of users.
- **Data Privacy:** Privacy is that the ability to perform an individual or group to seclude them or information about themselves and thus reveal them selectively [9]. Privacy has, followed by this set of query elements. (i) When: a subject may describe a lot of concerned regarding about the current or future information being revealed than information from the past. (ii) How: a user could also be comfortable to handle if his/her friends can set up manually request his/her information, however the user may not like alerts to be sent automatically and often utilized. (iii) Extent: a user may be to a certain extent have his/her information reported as an ambiguous region rather than an accurate point while unauthorized access occurred. In the cloud, the privacy suggests that when users visit after perform with the sensitive data, the cloud services can prevent potential adversaries from inferring the user's behavior by the user's visit model (non- leakage of direct data).

3.2 Security Issues in Cloud Computing

- **Data Transmission:** Encryption techniques are mainly utilized for protecting data in transmission. To provide the protection for data only goes wherever the customer needs it to go by using authentication policy and data integrity and is not modified during transmission time. SSL/TLS protocols are mainly used to perform at this time. In Cloud environment the majority of the data is not encrypted and decrypted within the processing time management. However to process data, for any application that data should be unencrypted. This encryption technique, authorizes data to be processed without being decrypted by using a homomorphism encryption scheme advance in cryptography. The cloud provider utilizes access controls such as authorization, authentication, auditing for using resources, and ensure the availability of the Internet-facing resources at cloud provider, and

provide the confidentiality and integrity during data-in-transmission process.

- **Privacy and Confidentiality:** Formerly, the client show data to the cloud there should be some security purpose that access the data will allow only be incomplete issues to the authorized access. Inappropriate access to client sensitive data by accessing cloud staff is another risk that can produce a potential threat to protect cloud data. The client is being provided data assurance and safe policies and proper practices and procedures should be in place to ensure the cloud users of the data safety. The cloud seeker should be assured that data transmit on the cloud will be confidential during secure access of information.
- **Access to Servers & Applications:** In standard data centers, administrative access to servers is restricted and controlled with direct access or on-premise a connection which is not the case of cloud data centers. In cloud computing, administrative access should be conducted through the internet, improving exposure and reduce risk issues. It is extremely necessary to control administrative access to data and monitor this access to maintain visibility during modification in system management. Data access concern primarily relates to security policies provided to the users while accessing the data. General scenario typically, a small business organization can utilize a cloud provided by another provider for implementing its business processes. Several organizations will have its own security policies depend on which each and every employee can have access to a particular set of data. The security policies could entitle some issues wherein some of the employees are not known access to a specific amount of data. These security policies must be adhered by the cloud to avoid intrusion of data by unauthorized users access [10].
- **Data Location:** Generally, cloud users are not controlled over the physical access mechanisms to that data and also they do not have any responsive of the accurate location of the data center. The majority of well-known cloud service providers have data centers around the globe. In many cases, this can be the main issues. As a result of data privacy and compliance laws in various countries, locality of data is of utmost importance in a lot of enterprise architecture.
- **Data Integrity:** To get the security of data access, cloud service providers should apply mechanisms to ensure data reliability and be able to tell what happened to a definite data set and at what point.
- **Data Location and Relocation:** Cloud computing provides a high amount of data mobility access. Consumers do not always recognize the location of their data. However, while a venture has several sensitive data that is reserved over a memory device within the Cloud, they will maintain often asking the career than it. They will also seek to specify a chosen location (e.g. Data being trapped in India). The server needs a contractual agreement between your Cloud providers and moreover the consumer that data should live in an exact location or reside in a given known place. Moreover, cloud providers should take accountability to ensure the security of systems (including data) and provides robust certification to protect customer's information against unauthorized access.
- **Data Segregation:** Data in the cloud is usually in a shared environment together perform with data from other customers. The encryption cannot be assumed for data segregation issues, as the result of the single solution is obtained. In some situations, customers may not require to encrypt data because there could also be a case when encryption accident will occur during destroys of the data. Make certain that encryption is accessible at all stages, and that these encryption schemes were planned and tested by performing experience professionals [11].
- **Another concern** is that the development of web data in one location completely to another location. Cloud provider is initially deciding

suitable location for storing data. However, it is stimulated derived from one destination to another destination. Cloud providers have contracts jointly and in addition they use each other's resources.

- **Data Availability:** Customer information is generally stored in chunk on completely different servers often residing in different Clouds or even in different locations. In such cases, data availability turn into a major legitimate concern as a result of un-interruptible and seamless provision becomes relatively troublesome.
- **Storage, Backup and Recovery:** If you select to maneuver crucial computer data in the cloud, the cloud provider make sure adequate data flexibility storage systems. RAID (Redundant Array of independent Disks) storage systems is mainly by the side of a minimum they need to be able to present, whereas most cloud providers will store the details in several copies some independent servers. In general, the majority of the cloud providers has to be offered choices for backup and restore services which are definitely necessary for those businesses that jog cloud based applications so that within the occasion of a grim hardware failure and can roll back to an earlier state.

IV. SECURITY ALGORITHMS

In Cloud Storage, any individual's or organization's data is describing about accessible and maintain from multiple connected and distributed resources that provide to a cloud. Encryption algorithm [12] plays an important role to provide secure communication over connected and distributed resources by using the fundamental tool for protecting the data. Encryption algorithm has mainly converted the data into scrambled type to protect by using "the key" and transmitter user only have the key to decrypt the data. There are two types of key encryption techniques used in security algorithms; they are symmetric key encryption and assymmetric key encryption.

In symmetric key encryption, single key is used to encrypt and decrypt the data. Two keys are mainly used in asymmetric key encryption. They are private key and public key. In Public key process, it is used for encryption. Another private key is used for decryption [13]. There are a number of existing techniques used to realize security in cloud storage.

The main focus is about cryptography to create data secure while transmitted over the network. Cryptography concept is that the revise and pratice of techniques for securing communication and data within the presence of adversaries. In cryptography concept, encryption and decryption techniques are used. An encryption technique converts message or plaintext into cipher text and decryption technique extracts the original message or plaintext into the same cipher text. Initially, the information must be encrypted and transmitted by using the encryption algorithm in cryptography. Secondly, the information should be decrypted by using the decryption technique the receiver side can read the original information. To provide security to cloud several algorithms are designed and describe below.

- **RSA Algorithm:** RSA algorithm has used public key encryption technique. This algorithm is delivered to life by Ron Rivest, Adi Shamir and Len Adelman in 1977. It is most recent asymmetric key cryptography algorithm. It may possibly well used to provide secrecy protection. In this algorithm utilizes the top number to come up with public key and private key depending on mathematical accuracy and multiplying large numbers together. It utilizes the block size of data during transmission; that its plain-text and cipher text integers between 0 and n for plenty of n values. Size of data n (i.e.values) is known as 1024 bits. The real challenge within the case of RSA algorithm would be the generation and

selection of the public key and private key. At intervals these two different keys can be performed encryption and decryption techniques. As the sender is aware of regarding the encryption key and receiver recognizes about the decryption key, these techniques we can generate encryption and decryption get into RSA.

- **Blowfish Algorithm:** Blowfish algorithm is a symmetric key algorithm that was developed in 1993 by Bruce Schneier. Its working is nearly almost like DES, however in DES key is small in size and can be decrypted in simple manner, however in Blowfish algorithm the size of the key is massive [14] and it can differ from 32 to 448 bits. Blowfish also consists of 16 rounds like DES [15]. Blowfish algorithm can encrypt data having multiple size of eight and if the size of the message is not multiple of eight than bits are protected. In Blowfish algorithm also 64 bits of plain text are separated into two parts of message as size 32 bits length. One part acquires as the left part of message and another one is right part of the message. The left part of the message is XOR with the elements of the P - array which creates some value, after that value is transmitted through transformation function F. The value initiated from the transformation function is again processed XOR with the other half of the message i.e. with right bits, after that F| function is called which replace the left half of the message and P| replace the right side of the message.
- **Diffie Hellman Key Exchange (D-H):** Diffie Hellman key algorithm substitute was discovered by Whitfield Diffie and Martin Hellman. It is a technique for exchanging securely by using cryptographic keys over a public network and was the primary specific sample of public-key cryptography. It enables only two users to exchange a secret key over an untrusted network. These two users do not need any prior knowledge about secrets sharing information between them. It is predicated on the complexity of computing discrete logarithms of massive prime numbers. It needs two large numbers, one prime (P) and another is (G), a primitive root of P.
- **Elliptic Curve Cryptography Algorithm:** ECC was discovered by Neil Koblitz (University of Washington) and Victor Miller (IBM) in 1985. It is a public key encryption technique depends upon discrete alogarithms which is utilized to create efficient, quicker and smaller cryptographic keys. Elliptic curve public key cryptography (ECC) is an innovative approach based on the algebraic structure of elliptic curves over finite fields with low key size. The ECC deals with two points (x, y), which satisfies the equation y2 =x3 +ax+b with some condition (4a3 +27b2 =0) by sharing the secret key. The points that lies on the curve operate as a public key and the selection of random numbers is used as private key encryption. ECC is used in some integer factorization algorithms that have applications in cryptography.
- **Data Encryption Standard (DES) Algorithm*:*** The Data cryptography standard (DES) [16] is a symmetric- key block cipher discovered as FIPS-46 within the Federal Register in January 1977 by the National Institute of Standards and Technology (NIST). In encryption site, DES takes a 64- bit plaintext and creates a 64-bit cipher text, after that the decryption site, it takes a 64-bit cipher text and creates a 64-bit plaintext. Each encryption and decryption techniques are used for same 56 bit cipher key. The encryption process is made of two permutations (P-boxes), that we have a tendency to call initial and final permutation, and sixteen Feistel rounds [17]. Each round transmits a different 48-bit round key generated from the cipher key encryption.
- **EI Gamel:** The ElGamal encryption system is an asymmetric key encryption algorithm for performing public-key cryptography, which is based on the Diffie–Hellman key exchange

process by using cryptography. It was illustrated by Taher Elgamal in 1984. ElGamal encryption is protected in the free GNU Privacy Guard software, latest versions of PGP, and other cryptosystems. The Digital Signature Algorithm is detailed about a variant of the ElGamal signature scheme, which should not be confused with ElGamal encryption. ElGamal encryption can be described over any cyclic group G. Its security based on the difficulty of a certain issue in G related to computing discrete logarithms.

- ***Advance Encryption Algorithm (AES):*** (Advanced Encryption Standard), is the new encryption standard suggested by NIST to replace DES. The Brute force attack, in this attacker tries to test all the character combinations to unlock the encryption, it is the only effective attack known against protection. Together AES and DES are block ciphers. It has an uneven key length of 128, 192, or 256 bits; default 256 bits. It encrypts data blocks of 128 bits in 10, 12 and 14 round depends upon the key length. AES Encryption is rapid and flexible; it can be implemented on different platforms particularly in small devices. In addition, AES has been carefully tested for numerous security applications. [18][19].
- ***DSA:*** DSA is the full form of Digital Signature Algorithm. DSA is a Federal Information Processing Standard for processing digital signatures. It was projected by the National Institute of Standards and Technology (NIST) in August 1991 to be used in their Digital Signature Standard (DSS) and approved as FIPS 186 in 1993.Four reviews to the initial specification has been released: FIPS 186-1 in 1996,FIPS 186-2 in2000,FIPS 186-3 in 2009and FIPS 186-4 in 2013. In DSA, key generation has described about two phases. In primary phase is to decide on algorithm parameters that can be shared between different users of the system. Second phase is to compute public and private keys for providing to a single user. The random signature values *k are* more crucial for performing entropy, secrecy, and uniqueness. These three requirements can disclose the whole private key to an assaulter.
- **3DES:** This was developed as an improvement of DES in 1998. In this typical the encryption technique is related to original DES but applied three times to improve the encryption level. However, it is a well-known fact that 3DES is slower than other block cipher techniques. This is a development of DES and 64 bit block length with 192 bits key size. 3DES has reduced performance in terms of throughput level and power consumption when compared with DES. It always needs more time than DES as a result of its triple phase encryption characteristics [20] [21].
- **MD5- (Message-Digest algorithm 5):** Generally, the cryptographic hash function algorithm is used with a 128-bit hash value and processes a variable length message into a fixed-size output of 128 bits. Initially, the input message is broken up into chunks of 512- bit blocks afterward the message is protected so that its total length is divisible by 512. In this process, the transmitter of the data utilizes the public key to encrypt the message and the receiver uses its private key to decrypt the message.

V. CONCLUSION

Cloud computing proves an extremely successful application for each and every organization's performance. For the reason that organizations have large amount of data to store and cloud provides that space given to user and also enables its user to access their data from anyplace anytime in a simple manner. Improved use of cloud computing for storing data is definitely increasing the trend of improving the ways of storing data in the cloud. As peoples are saving their personal information and important data to clouds, therefore it becomes a major issue to store that data safely. Data available in

the cloud can be at risk if not protected in a trustful manner. In the cloud there are a number of existing techniques used to implement security prevention. The study provided an overview and discuss about the cloud computing and security issues and how to improve the security algorithms for cloud computing.

VI. REFERENCES

[1]. Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Karl W., "Scientific Cloud Computing: Early Definition and Experience," 10th IEEE Int. Conference on High Performance Computing and Communications, pp. 825-830, Dalian, China, Sep. 2008, ISBN: 978-0-7695-3352-0.

[2]. Pring et al., "Forecast: Sizing the cloud; understanding the opportunities in cloud services," Gartner Inc., Tech. Rep. G00166525, March 2009.

[3]. Aman Bakshi, Yogesh B. Dujodwala, "Securing cloud from DDoS Attacks using Intrusion Detection System in Virtual Machine," ICCSN '10 Proceeding of the 2010 Second International Conference on Communication Software and networks, pp. 260-264, 2010, IEEE Computer Society, USA, 2010. ISBN: 978-0-7695-3961-4.

[4]. H. KAMAL IDRISSI, A. KARTIT, M. EL MARRAKI FOREMOST SECURITY APPREHENSIONS IN CLOUD COMPUTINGJournal of Theoretical and Applied Information Technology 31 st January 2014. Vol. 59 No.3

[5]. Kuyoro S. O, Ibikunle F. & Awodele O Cloud Computing Security Issues and ChallengesInternational Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011

[6]. Chunye Gong, Jie Liu, Qiang Zhang, Haitao Chen and Zhenghu Gongng The Characteristics of Cloud Computing2010 39th International Conference on Parallel Processing Workshopse Brazilian Computer Society 2010

[7]. SO, Kuyoro. Cloud computing security issues andchallenges. International Journal of Computer Networks, 2011, vol. 3, no 5.

[8]. D. H. Rakesh, R. R. Bhavsar, and A. S. Thorve, "Data security over cloud," International Journal of Computer Applications, no. 5, pp. 11-14, 2012.

[9]. J. Krumm, "A survey of computational location privacy," Personal and Ubiquitous Computing, vol. 13, no. 6, pp. 391-399, 2009.

[10]. K. Hwang, S Kulkarni and Y. Hu, "Cloud security with virtualized defence and Reputation-based Trust management," Proceedings of 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing (security in cloud computing), pp. 621-628, Chengdu, China, December, 2009. ISBN: 978-0-7695- 3929 -4.

[11]. Marios D. Dikaiakos, Dimitrios Katsaros, Pankaj Mehra, George Pallis, Athena Vakali, "Cloud Computing: Distributed Internet Computing for IT and Scientific Research," IEEE Internet Computing Journal, vol. 13, issue. 5, pp. 10-13, September 2009. DOI: 10.1109/MIC.2009.103.

[12]. AL.Jeeva, Dr.V.Palanisamy And K.Kanagaram "Comparative Analysis Of Performance Efficiency And Security Measures Of Some Encryption Algorithms" International Journal Of Engineering Research And Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 3, pp.3033- 3037, May-Jun 2012.

[13]. Maha TEBAA, Saïd EL HAJJI, Abdellatif EL GHAZI, "Homomorphic Encryption Applied to the Cloud Computing Security", World Congress on Engineering, Volume I, ISBN: 978-988-19251-3-8; ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online) , 2012.

[14]. Pratap Chandra Mandal, 'Superiority of Blowfish Algorithm', International Journal of Advanced Research in Computer Science and Software Engineering. September (2012) ISSN: 2277-128X Vol. 2, Issue 7.

[15]. G. Devi and M. Pramod Kumar, 'Cloud Computing: A CRM Service Based on a Separate Encryption and Decryption using Blowfish Algorithm', International Journal of Computer Trends and Technology. (2012) Vol. 3 Issue 4, ISSN: 2231-2803, pp.592-596.

[16]. Neha Jain and Gurpreet Kaur 'Implementing DES Algorithm in Cloud for Data Security" VSRD International Journal of CS & IT Vol. 2 Issue 4, pp. 316-321, 2012.

[17]. G. Devi , M. Pramod Kumar, "Cloud Computing: A CRM Service Based on a Separate Encryption and Decryption using Blowfish algorithm" International Journal Of Computer Trends And Technology Volume 3 Issue 4, ISSN: 2231-2803, pp. 592-596,2012.

[18]. D. S. Abdul. Elminaam, H. M. Abdul Kader and M. M. Hadhoud ,"Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMA Volume 8, 2009.

[19]. Gurpreet Singh, Supriya Kinger "Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security" International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.

[20]. Mr. Gurjeevan Singh, , Mr. Ashwani Singla and Mr. K S Sandha " Cryptography Algorithm Compaison For Security Enhancement In Wireless Intrusion Detection System" International Journal of Multidisciplinary Research Vol.1 Issue 4, August 2011.

[21]. Gurpreet Singh, Supriya Kinger"Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security "International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.