

Various Encryption Algorithms to Enhance Data Security in Cloud Storage

Anshul Jain¹ Prof. Ashok Verma²

^{1,2}Department of Computer Science & Engineering

^{1,2}Gyan Ganga Institute of Technology & Sciences, Jabalpur, India

Abstract— Cloud computing is the fastest growing technology nowadays; it is the technology for the next generation. This technology has changed the face of traditional computing technologies. This technology offers many benefits to the field of IT enterprises, even though it has to overcome many challenges to satisfy its maturity level. It provides services to an organization over a network with the ability to scale up or down their service requirements. Cloud computing services are established and provided by third parties, who have the infrastructure. Instead of buying IT equipment (hardware and/or software) and managing it themselves, many organizations today prefer to buy services from IT service providers. The number of service providers increase dramatically and the cloud is becoming the tools of choice for more cloud storage services. This model is attractive mainly for business oriented people because it reduces total cost of operation, maintenance cost, increases return of investment. Cloud computing is basically virtual pool of resources and it provides these resources to users via internet. It offers a range of services for end users; among which there's Storage as a service. In recent years, Storage in Cloud gained popularity among both companies and private users. However, data privacy, security, reliability and interoperability issues still have to be adequately solved. But the most important problem is security and how cloud provider assures it. The growth of the cloud users has unfortunately been accompanied with a growth in malicious activity in the cloud. More and more vulnerabilities are discovered, and nearly every day, new security advisories are published. Millions of users are surfing the Cloud for various purposes, therefore they need highly safe and persistent services. The future of cloud, especially in expanding the range of applications, involves a much deeper degree of privacy, and authentication. To secure the Cloud means secure the treatments (calculations) and storage (databases hosted by the Cloud provider). The objective of cloud security is to protect data as well as cloud systems from unauthorized access, use, disclosure, disruption, modification, or destruction. To protect the data in cloud database server cryptography is one of the important methods. Cryptography provides various symmetric and asymmetric algorithms to secure the data. This paper discusses the various benefits and major security challenges of cloud computing, it also highlights the various cryptographic encryption algorithms as the major solution of security challenges.

Key words: Cloud Computing, Cryptography, Data Security, Decryption, Encryption, Algorithms

I. INTRODUCTION

According to NIST, Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or

service provider interaction. Various cloud service providers are Amazon, Google, IBM, Microsoft, and Salesforce.com, offer their cloud infrastructure for services. The Cloud Computing provides three main services, Information as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS). Clouds can be classified as public, private or hybrid. It reduces the cost of hardware required to store data that could have been used at user end. Instead of purchasing the infrastructure that is required to store data and run the processes we can lease the assets according to our requirements. This type of data centre environment allows enterprises to get their applications up and running faster, with easier manageability, and less maintenance to meet business demands. For example, we can manage and store all smart phones or tablets apps at one location i.e. cloud. So we do not require any memory space at our end. The cloud computing provides the number of advantages over the traditional computing and it include: quickness, lower cost, scalability, device independency and location independency. Because of these benefits each and every organizations are moving their data to the cloud.

The first form of web based data storage is called cloud storage. Recently Storage as a service (STaaS) Cloud gained popularity both among private users and companies. STaaS is a Cloud business model in which a service provider rents space in its storage infrastructure to individuals or companies. The data stored in the cloud can be sensitive to the business. This is a form of networked data storage where data files are stored on multiple virtual servers. Cloud computing isn't just about accessing applications over the web. The cloud can also be used to store documents either as a large pool of backup drive or as primary store of file storage. The servers used for cloud storage are hosted by third party companies who operate large data centers. When we subscribe to cloud storage we lease storage capacity from the cloud storage. The data may be stored across multiple servers and at multiple locations. Security becomes big issue when any one stores its important information to a platform which is not directly controlled by the user and which is far away. While sending of data and during storage data is under threat because any unauthorized user can access it, modify it, so there is need to secure data. A data is secure, if it fulfils three conditions (i) Confidentiality (ii) Integrity (iii) Availability. Confidentiality means the data is understandable to the receiver only for all others it would be waste; it helps in preventing the unauthorized disclosure of sensitive information. Integrity means data received by receiver should be in the same form, the sender sends it; integrity helps in preventing modification from unauthorized user. Availability refers to assurance that user has access to information anytime and to any network. Currently, the most of users of cloud storage protect their data with SLAs contracts and are based on the trust and reputation of the provider. This weakness has motivated us to think about solutions that

enable users to secure their data to prevent malicious use. . To secure the Cloud means secure the treatments (calculations) and storage (databases hosted by the Cloud provider). In the cloud confidentiality is obtained by cryptography. Cryptography is a technique of converting data into unreadable form during storage and transmission that it appears waste to intruder. The unreadable form of data is known as cipher text. When data is received by receiver it, will appear in its original form which is known as plain text. Conversion of plain text to cipher text is known as encryption and reverse of this (cipher text to plain) is known as decryption. Encryption takes place at sender's end whereas decryption takes place at receiver's end. Cryptography, in modern days is considered combination of three types of algorithms. They are (1) Symmetric-key algorithms (2) Asymmetric-key algorithms and (3) Hashing. DES, Triple-DES, AES, and Blowfish etc are some symmetric algorithms can be used to implement cloud security. RSA and Diffie-Hellman Key Exchange are the asymmetric algorithms these can be used to generate encryption and decryption key for symmetric algorithms. Security and privacy are one of the issues which users are concerned about as the data are with the providers. This paper studies the different security algorithms which are used to eliminate the concerns regarding data loss, privacy while accessing web application on cloud. Comparisons have been made between different algorithms to find the best security algorithm.

II. CLOUD COMPUTING

Cloud Computing is an important concept in computer development in recent years. This concept refers to the use of Computing capacity and storage of computers and servers in the world over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications.

The goal of cloud computing is to allow users to take advantage from all of these technologies, without the need for more knowledge about or expertise with each one of them. The cloud aims to cut costs, and helps the users to concentrate on their core business instead of being impeded by IT obstacles. Cloud computing can enable a user to access applications and data from any computer at any time since they are stored on a remote server. It also minimize the need for companies to acquire top-of-the-line servers and hardware or hire people to execute them since it is all maintained by a third party. Cloud computing is derived from earlier large scale distributed computing technology. In Cloud computing, files and software are not fully carried by the user's computer. National Institute of Standards and Technology (NIST) defines Cloud computing as follows: "Cloud computing is a Model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This

Cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models as shown in Figure 1.

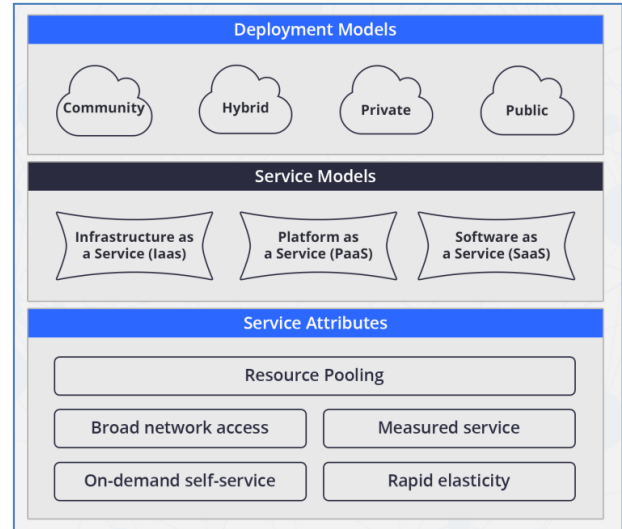


Fig. 1: The NIST Definitions of Cloud Computing

A. Cloud Data Storage versus Traditional Data Storage

Cloud in a terms defined by internet based applications. User send requests for services and server serve the desired data or application as services. Here, cloud becomes an organization of network and high computational hardware resources. These resources are connected for providing a high efficient computational experience. The cloud makes it possible for access information from anywhere and anytime. Traditional computing requires same location of data storage. Compared to traditional data storage as shown in Figure 2, cloud data storage offers numerous advantages

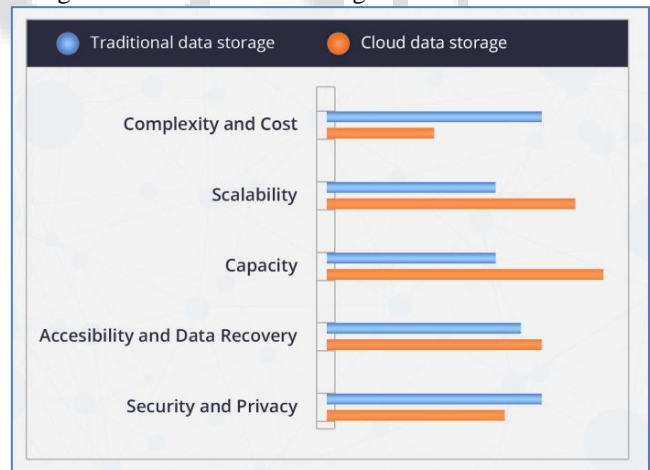


Fig. 2: Traditional Storage vs. Cloud Storage

1) Lower Complexity and Costs

Almost six out of 10 providers say that cost reduction is the main goal for customers to use cloud services. Consumers do not need to buy and configure new equipment. Cloud storage service allows them to get their application started immediately, and the providers charge the users based on the usage of resources (Pay As You Go). The service usually costs a fraction of what it would cost to implement an on-site solution.

2) Scalability and Capacity

As the consumer requires more capacity, the service provider can make more scalability, much simpler than if you had to add the equipment on your own premise. Therefore, you can scale your storage capacity regardless of the amount of space that you need.

3) Archival and Disaster Recovery Purposes

Cloud storage provider can help the organization enhance security from Internet services, by preventing loss due to fire, theft, or disaster. Therefore, companies who archive their information in the cloud do not have to worry too much about natural disasters.

4) Greater Accessibility and Reliability

Stored files can be accessed from anywhere via Internet connection. However, there are many other benefits to adopting cloud storage services, and there are also some factors affecting cloud adoption such as Usability, Bandwidth, Data Security and Privacy, and so on. Indeed, the two most significant barriers to cloud adoption are Security and Privacy. Except for these two barriers, the others are beyond the scope of our research.

5) Cloud Storage Security and Privacy Threats

For all the advantages that provide cloud storage; we cannot ignore the potential risks that face our data when storing them in the cloud environment. Most of the time, consumers move information into the cloud without any consideration of security. Once their data is outsourced to the cloud service providers, they have to trust the CSP, which means that data is out of control and the service provider can access the data in the cloud at any time. It could accidentally or deliberately alter, even delete, information.

B. Foundation for Cloud

In this section, we take a high level look at the underlying technology pieces from which cloud computing infrastructure is built. These can be broadly categorized as follows:

1) Virtualization

allows for server consolidation with great utilization flexibility. For cloud computing, virtualization has great value in rapid commissioning and decommissioning of servers.

2) Software

Enables all aspects of cloud infrastructure management, provisioning, service development, accounting, and security. It is critical that cloud infrastructure is able to dynamically enforce policies for separation, isolation, monitoring, and service composition.

3) Service Interfaces

The service interface between the provider and the consumer is a key differentiator for cloud. It represented a contract that enforces the value proposition with SLAs and price items.

C. Layers of Cloud Computing

There are different layers of cloud services that refer to different types of service model, each offering discrete capabilities. Apart from management and administration, the major layers are:

1) Infrastructure as a Service (IaaS)

Infrastructure as a service delivers computing resources as a service, servers, network devices, and storage disks are made available to organizations as services on a need-to basis.

Virtualization, allows IaaS providers to offer almost unlimited instances of servers to clients, while making cost-effective use of the hosting hardware. Companies can use IaaS to build new versions of applications or environments without having to invest in physical IT assets. Some cloud solutions also rely solely on this layer like the Amazon's product EC2, Amazon S3.

2) Platform as a Service (PaaS):

This layer provides a platform for creating applications. PaaS solutions are essentially development platforms for which the development tool itself is hosted in the Cloud and accessed through internet. With PaaS, developers can build Web applications without installing any tools on their computers and then deploy those applications without any specialized systems administration skills. Examples include Google App Engine, Force.com and Microsoft Azure.

3) Software as a Service (SaaS):

This layer includes applications that run off the Cloud and are available on demand to Web and paid for on a per-use basis, anytime-anywhere basis. There is no need to install and run the special software on your computer if you use the SaaS. A more efficient form is fine grained multi-tenancy. The concept of SaaS is attractive and some software runs well as cloud computing, but the delay of network is fatal to real time or half real time applications such as 3D online game. Examples include online word processing and spreadsheet tools, customer relationship management (CRM) services and web content delivery services (Salesforce CRM, Google Docs, etc.). These three are the main layers, although there can also be other forms of service provided, such as business process as a service, data as a service, security as a service, storage as a service, etc.

D. Cloud Computing Deployment Types

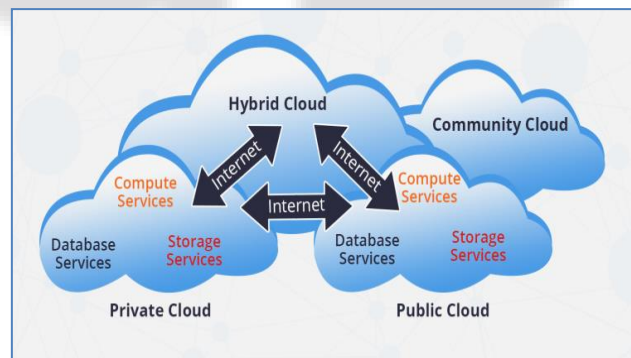


Fig. 3: Models in Cloud Computing

1) Public Cloud

The most recognizable model of cloud computing to many consumers is the model, under which cloud services are provided in a virtualized environment, constructed using pooled shared physical resources, and accessible over a public network such as the internet. To some extent they can be defined in contrast to private clouds which ring-fence the pool of underlying computing resources, creating a distinct cloud platform to which only a single organization has access. Public clouds, however, provide services to multiple clients using the same shared infrastructure.

2) Private Cloud

Private clouds are those that are built exclusively for a single business. For many companies considering cloud computing,

private clouds are a good starting point. They allow the organization to host applications, development environments, and infrastructure in a cloud, while addressing concerns regarding data security and control that can arise in the public cloud environment.

3) *Community Cloud*

The cloud foundation is imparted by numerous associations and backings a specific group that has imparted issues (e.g., mission, security necessities, arrangement, and consistence contemplations).

4) *Hybrid Cloud*

A hybrid cloud is generally best-of-breed. It combines the comfort level of a private cloud with the flexibility and versatility of the public cloud. Hybrid platforms use either public clouds or off-site Hosted Virtual Private Clouds for some applications and processes. They merge these with on premises private clouds for high security application environments to leverage the best of both worlds.

E. Challenges of Cloud Computing

1) *Privacy of Data*

Privacy of data is key security concern for cloud computing. Most of the organizations feel comfortable in keeping their valuable data in their site than on cloud space. Consumers do not have any idea regarding the location of data, transfer of data, operations on cloud, etc. Most of the organizations are unaware of security mechanism implemented by service providers. Many questions are raised by consumers such as

- 1) Which are the organizations sharing services?
- 2) How creation and back-up of files taking place?
- 3) What happened to the deleted files?
- 4) Which type of consumers can access data?
- 5) Location of data?

2) *Confidentiality of Data*

Confidentiality is related to data privacy; it ensures data visibility to only authorized users. Confidentiality is the responsibility of service provider. Common solution to the confidentiality is encryption. Many symmetric and asymmetric algorithms are available for data confidentiality, even though encryption and decryption is the solution to the confidentiality; there are many questions which are arising related to it. They are

- 1) Where is encryption and decryption taking place (client side or cloud side)?
- 2) How can search be performed on the data in an encrypted form?
- 3) What are threats while transferring data from client to cloud?
- 4) Any miss use of data by service provider?
- 5) Any miss use of key by service provider?

3) *Data Remanence*

Data should be deleted from cloud after the life-cycle, or the memory should be reformatted or recycled. The reformatting of storage media does not remove the previously written data from the media, but also it can be accessed or recovered from the media later. No clear standard is available for recycled storage media. This data remanence makes difficult the vacation of hardware resources from the cloud. Most consumers are unknown of allotted resources and storage space, due to this issue consumers are locked with one service provider. Various techniques have been developed to counter

data remanence. These techniques are classified as cleaning, purging/sanitizing, or destruction. Specific methods include overwriting, degaussing, encryption, and media destruction.

4) *Data Integrity*

Preservation of information from loss or modification by unauthorized users is referred as data integrity. Multiple organizations are sharing the application or platform by multi-tenancy, consumers working on same work may share data can be modified by any other unauthorized user sharing the application or platform in the cloud, this cause the integrity failure. As data are the base for providing cloud computing services, such as Data as a Service, Software as a Service, Platform as a Service, keeping data integrity is a fundamental task.

5) *Transmission of Data*

Most of the time data is transferring between consumer and cloud. Initially data is sent from client site to cloud, data is returned from cloud to client after queries during the operation. Encryption is used provide protection while the transmission of data. Most of the time data is transferred without encryption due to lot of time is required for encryption and decryption for each operation upon data. During transfer an attacker can trace the communication, interrupt the data transfer, miss use the data, etc.

6) *Malicious Insiders*

Malicious insiders are authorized employees; these users are appointed for managing and maintaining cloud by cloud service provider. These users sometimes steal or corrupt the sensitive data of organizations in the cloud and convey this sensitive information to other organizations sharing the same cloud. These malicious insiders may get payment for this malicious work. Sometimes service providers are not able to take any action against these employees.

III. CRYPTOGRAPHY

Cryptography in the cloud allows for securing critical data beyond your corporate IT environment, where that data is no longer under your control. Cryptography expert Ralph Spencer Poore explains that "information in motion and information at rest are best protected by cryptographic security measures. In the cloud, we don't have the luxury of having actual, physical control over the storage of information, so the only way we can ensure that the information is protected is for it to be stored cryptographically, with us maintaining control of the cryptographic key." It is the method of using different algorithms to encrypt and decrypt message and data. Data when sent by sender cannot be hacked by hacker in between the transmission. It allows users to conveniently and securely access shared cloud services, as any data that is hosted by cloud providers is protected with encryption. Cryptography in the cloud protects sensitive data without delaying information exchange.

There are various approaches to extending cryptography to cloud data. Data can be encrypted prior to uploading it to the cloud altogether. This approach is beneficial because data is encrypted before it leaves the owners environment, and data can only be decrypted by authorized parties that have access to the appropriate decryption keys. Thus for preserving the security and privacy

of data the cryptographic techniques are utilized. The art of preserving information in to cipher text using a secret key to decipher is known as cryptographic approach. Modern cryptography is virtually unbreakable. The primary purpose of encryption is to ensure the confidentiality of the data stored on a specific device or transmitted via the internet.

Components of cryptosystem are as follows:

- Plaintext

Original form of data, data to be protected during transmission and storage.

- Cipher text

It is the unreadable form of the plaintext after encryption operation.

- Encryption Algorithm

Used to convert plaintext to cipher text, it is a mathematical process.

- Decryption Algorithm

It performs reverse operation of encryption algorithm, and converts cipher text to plaintext.

- Encryption Key

It is a value used by sender with algorithm to convert plaintext to cipher text.

- Decryption Key

It is a value used by receiver with algorithm to convert cipher text to plaintext.

Various level of encryption can be applied to the plaintext to make data more secure. Even if one level of encryption is cracked by hacker, the text will be again text, which makes it difficult to get the plaintext.

A. Cryptographic Algorithms

The three main cryptographic algorithms are: Symmetric-Key Algorithm, Asymmetric-Key Algorithm and Hashing Algorithms.

1) Symmetric-Key Algorithm Also Known as Secret Key Encryption

A single key is used for both encryption and decryption. The key, in practice, represents a shared secret between two or more communicating parties for secure communication. A few of the well-known symmetric encryption algorithms include DES, AES, and Blowfish.

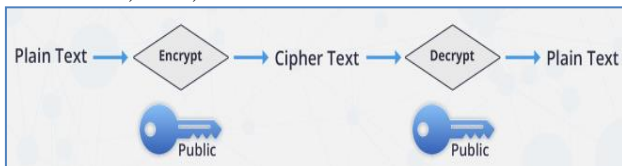


Fig. 4: Symmetric-Key Algorithm

2) Asymmetric-Key Algorithm or Public-Key Encryption

The asymmetric-key algorithm or public-key encryption utilizes a pair of keys—public key and private key. The public key can be revealed, but, to protect the data, the private key must be concealed. Additionally, encryption and decryption of the data must be done by the associated private and public keys. For instance, data encrypted by the private key must be decrypted by the public key and vice versa. Some of the common examples of this algorithm are RSA (Rivest-Shamir-Adleman), Diffie–Hellman key exchange, and elliptic curve techniques.

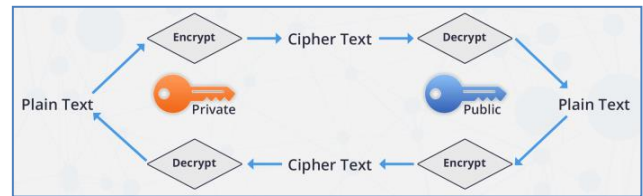


Fig. 5: Asymmetric-Key Algorithm

3) Hashing Algorithms, Also Called One-Way Encryption

Hashing algorithms, also called one-way encryption, are algorithms that, in some sense, use no key. It is a vital information security tool and is used to authenticate messages, digital signatures and documents. A hash function accepts a variable-length block of data as input and produces a fixed-length hash value called message digest. Having a message digest, it is impossible to recover or find the original string. Some examples of hashing algorithms are: MD5, and SHA.



Fig. 6: Hashing Algorithm

B. Cryptographic Techniques

Following techniques are the mostly used cryptographic techniques for cloud computing.

1) Data Encryption Standard (DES)

The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST). It uses single key (secret key) for both encryption and decryption. DES is very commonly used symmetric key algorithm. It was developed by IBM in 1974. It encrypts data in blocks of size 64 bits each. That is 64 bits of plain text goes as input to DES, which produces 64 bits of cipher text. The same algorithm and key are used for encryption and decryption, with minor differences. The key length of this algorithm is 56 bits; however a 64 bits key is actually input. The DES (Data Encryption Standard) algorithm is one of the most used encryption algorithm in the world. The algorithm is more suitable to implement on hardware and not for software, because it gives low performance and it is time consuming.

2) Advanced Encryption Standard (AES)

AES is a symmetric-key block cipher published by the National Institute of Standards and technology (NIST). Most adopted symmetric encryption is AES. Advanced Encryption Standard (AES), also known as Rijindael named after Joan Daemen and Vincent Rijmen is used for securing information. AES is a symmetric block cipher that uses the basic techniques of substitution and Transposition. The key size used for an AES cipher specifies the number of repetitions of transformations rounds. All other rounds are identical for encryption and decryption; except for the last round in each case. The number of cycles of repetition is as follows:

- 10 cycles of repetition for 128-bit keys.
- 12 cycles of repetition for 192-bit keys.
- 14 cycles of repetition for 256-bit keys.

The advantages of AES are many. AES is not susceptible to any attack but Brute Force attack. However, Brute Force attack is not an easy job even for a super

computer. This is because the encryption key size used by AES algorithm is of the order 128, 192 or 256 bits which results in billions of permutations and combinations. High speed and low RAM requirements were criteria of the AES selection process. Thus AES performs well on a wide variety of hardware; from 8-bit smart cards to high-performance computers. AES is also much faster than the traditional algorithms. It provides greater efficiency for software as well hardware also. AES is most frequently used encryption algorithm today this algorithm is based on several substitutions, permutations and linear transformations, each executed on data blocks of 16 byte. As of today, no practicable attack against AES exists. Therefore, AES remains the preferred encryption standard for governments, banks and high security systems around the world. It is useful when we want to encrypt a confidential text into a decrypted format, for example when we need to send sensitive data in e-mail. The decryption of the encrypted text is possible only if we know the right password. AES is an iterative rather than Feistel cipher. It is based on "substitution– permutation network". It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).

3) Blowfish Algorithm

Blowfish Algorithm is a symmetric key algorithm which was developed in 1993 by Bruce Schneier. Its working is almost similar to DES but in DES key size is small and can be decrypted easily but in Blowfish algorithm the size of key is large and it can vary from 32 to 448 bits. Blowfish also consists of 16 rounds like DES. Blowfish algorithm can encrypt data having size multiple of eight and if the size of the message is not multiple of eight than bits are padded. Blowfish is a very strong symmetric key cryptographic algorithm. Blowfish encrypts 64 bit blocks with a variable length key of 128-448 bits. According to Schneier, Blowfish was designed with the followings objectives in mind:

- Fast- Blowfish encryption rate on 32-bit microprocessors is 26 clock cycles per byte.
- Compact- Blowfish can execute in less than 5 kb memory.
- Simple- Blowfish uses only primitive operation -s, such as addition, XOR and table look up, making its design and implementation simple.
- Secure- Blowfish has a variable key length up to maximum of 448-bit long, making it both secure and flexible.

Blowfish suits applications where the key remains constant for a long time (e.g. Communications link encryption), but not where the key changes frequently (e.g. Packet Switching).

4) Rivest-Shamir-Adleman (RSA)

RSA is a public key cipher developed by Ron Rivest, Adi Shamir and Len Adleman in 1977. It is most popular asymmetric key cryptographic algorithm. This algorithm uses various data block size and various size keys. It has asymmetric keys for both encryption and decryption. It uses two prime numbers to generate the public and private keys. This algorithm can be broadly classified in to three stages; key generation by using two prime numbers, encryption and

decryption. Functioning of RSA is based on multiplication of two large numbers. Two large prime numbers are generated and multiplied. After multiplying two numbers, modulus is calculated the number that is generated is used as the public and private key. The two numbers that are used for multiplication-one of them is public other is private. Public key is known to all, whereas Private Key known only to user who originally owns the data. Thus encryption is done by the cloud service provider and decryption is done by the cloud user or consumer. Once the data is encrypted with the Public key, it will be decrypted using the corresponding Private Key only. RSA today is used in hundreds of software products and can be used for key exchange, digital signatures, or encryption of small blocks of data. This algorithm is mainly used for secure communication and authentication upon an open communication channel.

5) Diffie- Hellman Key Exchange Algorithm

Diffie Hellman key exchange algorithm was developed by Whitfield Diffie and Martin Hellman in 1976. Diffie-Hellman key exchange, also called exponential key exchange, is a method of digital encryption that uses numbers raised to specific powers to produce decryption keys on the basis of components that are never directly transmitted, making the task of a would-be code breaker mathematically overwhelming. Diffie Hellman also required two different keys. In this, a shared secret key is established, that is used for communication over the public network. In Diffie Hellman Key Exchange Algorithm Sender and Receiver picks two secret numbers and these numbers are known to both sender and receiver. The most serious limitation of Diffie-Hellman in its basic or "pure" form is the lack of authentication. Communications using Diffie-Hellman all by itself are vulnerable to man in the middle attacks. Ideally Diffie-Hellman should be used in conjunction with a recognized authentication method such as digital signatures to verify the identities of the users over the public communications medium. Diffie-Hellman is well suited for use in data communication but is less often used for data stored or archived over long periods of time.

6) Message-Digest Algorithm 5(MD5)

MD5 is a very famous and well known hash function and it generates a 128-bit resulting hash value. MD5 is commonly used in various applications to provide security, and it is also used to ensure the integrity of files. The MD5 value generated for specific file is considered as reliable fingerprint that can be used to check the integrity of the file contents. This algorithm had been implemented in different computer languages including C, Perl, and Java. In MD5 algorithm sender uses the public key provided by the receiver to encrypt the message and receiver uses its private key to decrypt the message.

7) Secure Hashing Algorithm (SHA)

SHA stands for secure hashing algorithm it produces 20 bytes 160 bit hash value. This gives message authentication and preserves the integrity during transaction. Authentication Requirements:

- Masquerade – Insertion of message from fraudulent source
- Content Modification – Changing content of message

- Sequence Modification – Insertion, deletion and reordering sequence.
- Timing Modification – Replaying valid sessions.

C. Comparison

The most widely used cryptographic algorithms are compared below:

	RSA	AES	DES	BLOWFISH
Key used	Asymmetric key	Symmetric key	Symmetric key	Symmetric key
Key size	1024 bits	128,192,256 bits	56 bits	32-448 bits
Initial vector size(plain text)	1024 bits	128 bits	64 bits	64 bits
Data encryption on capacity	Small amount of data can be encrypted	Large data can be encrypted	Data less than AES can be encrypted	Data less than AES can be encrypted
Security	Secured only for user	Secured for both user and provider	Secured for both user and provider	Secured for both user and provider
Authentication provided	Robust authentication	Best authentication provided	Somewhat less than AES	Can be compared with AES
Memory usage	Highest memory usage	Low RAM required	More memory usage as compared to AES	Can execute in less than 5 kb
Execution time	Requires maximum time	Faster	Requires same time as AES	Requires less time

IV. CONCLUSION

Cloud computing is world emerging, next generation technology in the field of information technology. It has numerous advantages but some challenges still exist in this technology. Security is the most challenging issue in this technology. Through this paper different encryption algorithms have been proposed to make cloud data secure, vulnerable and gave concern to security issues, challenges. The comparisons between AES, DES, Blowfish and RSA algorithms are shown. Comparison is done to find the best security algorithm, which has to be used in cloud computing for making cloud data secure which cannot be hacked by attackers. Encryption algorithms play an important role in data security on cloud. Through the comparison, it has been found that:

- AES algorithm uses least time to execute cloud data.
- Blowfish algorithm has least memory requirement.
- DES algorithm consumes least encryption time.

- RSA consumes longest memory size and encryption time.

The comparison shows the effectiveness of different algorithms. In future such type of more comparisons with different approaches can be done to show effectiveness of different algorithms. Looking into the comparisons a framework can also be proposed.

REFERENCES

- [1] Zaid KARTIT, Mohamed EL MARRAKI, "Applying Encryption Algorithm to Enhance Data Security in Cloud Storage", Engineering Letters, 23:4, EL_23_4_06.
- [2] Er. Ashima Pansotra, Er. Simar Preet Singh, "Cloud Security Algorithms", IJSIA, Vol.9, No.10 (2015), pp.353-360.
- [3] Papri Ghosh, Vishal Thakor, Dr. Pravin Bhathawala, "Data Security and Privacy in Cloud Computing Using Different Encryption Algorithms", IJARCSSE, Volume 7, Issue 5, May 2017.
- [4] Bokefode Jayant D., Ubale Swapnaja A, Pingale Subhash V., Karande Kailash J., Apate Sulabha S., "Developing Secure Cloud Storage System by Applying AES and RSA Cryptography Algorithms with Role based Access Control Model", IJCA, Volume 118–No.12, May 2015.
- [5] Omer K. Jasim, Safia Abbas, El-Sayed M. El-Horbaty and Abdel-Badeeh M. Salem, "Efficiency of Modern Encryption Algorithms in Cloud Computing", IJETTCS, Volume 2, Issue 6, November – December 2013.
- [6] Mr. Santosh P. Jadhav, Prof. B. R. Nandwalkar, "Efficient Cloud Computing with Secure Data Storage using AES", IJARCC, Vol. 4, Issue 6, June 2015.
- [7] Manisha R. Shinde, Rahul D. Taur, "Encryption Algorithm for Data Security and Privacy in Cloud Storage", AJCSES [3][1][2015] 034-039.
- [8] Namita N. Pathak, Prof. Meghana Nagori, "Enhanced Security for Multi Cloud Storage using AES Algorithm", IJCSIT, Vol. 6 (6) , 2015, 5313-5315.
- [9] Faheem Gul, Aaqib Amin, Suhail Ashraf, "Computing Security with Secure Data Storage using AES", IJCSMC, Vol. 6, Issue. 7, July 2017, pg.27 – 32.
- [10] Abha Sachdev, Mohit Bhansali, "Enhancing Cloud Computing Security using AES Algorithm", IJCA, Volume 67– No.9, April 2013.
- [11] Rajput Snehal, Prof. J S Dhobi, "Enhancing Data Security in Cloud Computing using AES encryption Algorithm", IJARIE, Vol-2 Issue-3 2016.
- [12] Nitin Rajput, "Performance Evaluation of AES with Different Key Size on Cloud Computing", IJRRETAS, Vol 2 Issue 5 June 2016.
- [13] Ming Li Member, Shucheng Yu, Yao Zheng, Kui Ren, Wenjing Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption", IEEE Transactions on Parallel and Distributed Systems, Volume: 24, Issue: 1, Jan. 2013 .
- [14] K.R.MONISHA, "Secure Cloud Computing Using AES and RSA Algorithms", Proceedings of 20th IRF International Conference, 1st March 2015.

- [15] Sumit Devray, Awdhesh Kumar, "Secure Search over Encrypted Data in Cloud Computing: A Survey", IJSRD, Vol. 3, Issue 07, 2015.

