ISSN 2320-9984
9 772320 998053 01

Volume 5 Issue 1 | March 2017 ISSN: 2320-9984 (Online)

International Journal of Modern Engineering & Management Research

Website: www.ijmemr.org

Survey on Security Mechanisms for Public Cloud Data

Dalveer Kaur
M. Tech. Research Scholar
Shri Ram Group of Institutions
Jabalpur (M.P.), [INDIA]
Email:dalveer.soni@gmail.com

Sapna Jain Choudhary
Assistant Professor
Department of Computer Science Engineering
Shri Ram Group of Institutions
Jabalpur (M.P.), [INDIA]
Email: choudharysapnajain@gmail.com

***Abstract*—*In recent years cloud computing is getting more and more attention every day. While outsourcing the hardware and software resources, still being able to manage them remotely with benefits like high computing power, competitiveness, cost efficiency, scalability, flexibility, accessibility and availability are revolutionary. For all of its advantages, on the other hand, nothing interesting is ever completely one-sided. Security and integrity of the data which is stored in untrustworthy server is critically important and raises concerns about it. The data can be modified, removed, corrupted or even stolen since it is in the remote server. This paper aims to provide a general survey about major cryptographic mechanisms used in cloud are conventional symmetric and asymmetric algorithms, quantum cryptography, elliptic curve cryptography, homomorphic encryption and DNA based cryptography.*

Keywords*—*Cloud Computing, Cryptography, DNA, Encryption Public Cloud, Security Issues, Security Mechanisms.

1. INTRODUCTION

Cloud computing has been emerged to increase the capabilities required by companies without investing much in new infrastructure, training of personnel or licensing new software. NIST [1] defines Cloud computing as "model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and delivered with minimal managerial effort or service provider interaction". Cloud provides benefits from flexible use of software, pay- per-use model and cost reduction. Cloud includes major risk factors such as security, data integrity, network dependency and centralization. A public cloud is one of the cloud computing models, in which a service provider makes resources available to the general public over the Internet. The public cloud environment is complex when compared to a traditional data store environment. Public cloud storage providers, provides storage infrastructure as a rentable commodity for both long-term as well as short-term storage.

Public cloud storage is used for backing up of data as well as archiving email and static non-core application data for Disaster Recovery Plan. Security and reliability are the two main challenges in cloud computing. The most common issues for public cloud storage is the data security and how cloud providers assures it [2]. Cloud computing often faces threats which are similar to that of physical workplace. Attackers can easily attack the data stored in cloud using malicious virus, hacking, working within the organisation, Denial of Service, etc. The virus can be sent easily through email which may bypass anti-virus tools. Hackers mainly focus on specific organizations for valuable data. In

some cases the unauthorised user may even try to access authorised information. The employees may unofficially use company computer for use of social media and downloading of applications which may be used to send attacks over the web. All of these malicious activities affect the security of data stored in public cloud.

2. SECURITY ISSUES IN THE CLOUD DEPLOYMENT MODELS

The three deployment models are private cloud, public cloud and hybrid cloud. The security issues of these deployment models are discussed below [6].

A. Security issues in a public cloud

In a public cloud model, the platform and infrastructure are shared among customers. The securities for these services are provided by the cloud service provider. A few of the key security issues in a public cloud include:

1. Since there is no control over the security mechanisms used by the cloud service provider, it is difficult to protect data in all its stages providing the basic requirements of confidentiality, integrity and authenticity
2. Since most service providers use a multitenant architecture, the possibility of data leakage between the tenants is very high
3. If the Cloud service provider uses a Third Party vendor for providing the services, then there is added overhead of verifying the agreements and contingency plans between them.
4. There is also a possibility of an insider attack at the service provider side. As the cloud architecture grows the number of insiders grow. Proper laws should be enforced to protect data from malicious insiders.

B. Security issues in a private cloud

A private cloud model enables the customer to have local network and storage space. They provide the flexibility to the customer to implement any kind of required services. There are certain securities issues:

1. Due to virtualization, unauthenticated and unauthorized access to system is possible
2. Malware can be used to attack the host operating system
3. In order to protect from diverse HTTP request the access point of users to access the infrastructure must be protected with standard security techniques.
4. Security policies must be designed to protect attacks from insiders.

The hybrid cloud model is a combination of both public and private cloud and hence the security issues discussed with respect to both are applicable in case of hybrid cloud model. Each of the three ways in which cloud services can be deployed has its own advantages and limitations. And from the security perspective, all the three have got certain areas that need to be addressed with a specific strategy to avoid them [6].

3. SECURITY MECHANISM IN PUBLIC CLOUD

Despite of increased hacking of data in public cloud, data security in public cloud can be achieved with the use of high- quality cloud security. The three issues need to be addressed to provide security in cloud computing are: Availability, Confidentiality and Integrity known as the ACI triad [3].

1) Availability

Availability is a mechanism by which data will be available to the user in a manner irrespective of location of the user. It can be achieved by providing authentication and network security.

2) Integrity

Integrity provides security to data in the means that the data sent and the data received is always the same and it cannot be changed while transmitting. Integrity will be affected if the data gets affected. It can be achieved by using firewalls and intrusion detection.

3) Confidentiality

Confidentiality is a way to avoid unauthorized expose of user data to the unauthorized user. Providing security protocols and data encryption services confidentiality can be achieved.

Client's data in the cloud can be accessed by other clients. So there arise security issues on client's data. To achieve security on cloud data many techniques and algorithms are available. Some of these are [4]:

Authorization practices – Provides authorization to clients, who can access data stored on cloud system.

Authentication processes - which creates a user name and password to access the data.

Encryption - A technique which uses complex algorithm to hide the original information with the help of encryption key.

Many of the techniques used in physical data centers have to be used in the cloud environment too. The best cloud service providers build these techniques into their clouds. Some of the security mechanisms used in public cloud:

Implicit storage security mechanisms use the scheme of data partitioning to store data in online. The data is simply partitioned and stored instead of encrypting the data. The data can be divided and stored on different servers on the network. The location of the data where it is stored will be known only to the user. In order to obtain the data back for use, the user has to have the knowledge about where data is residing. There are several different mechanisms available for storing data online, one of which is to store the encryption key. The access to all the servers is given only to the user thus providing more security. It involves the roots of a polynomial in finite field.

A. Security for* Implicit *Data Storage in Online[5]

Implicit storage security mechanisms use the scheme of data partitioning to store data in online. The data is simply partitioned and stored instead of encrypting the data. The data can be divided and stored on different servers on the network. The location of the data where it is stored will be known only to the user.

In order to obtain the data back for use, the user has to have the knowledge about where data is residing. There are several different mechanisms available for storing data online, one of which is to store the encryption key. The access to all the servers is given only to the user thus providing more security. It involves the roots of a polynomial in finite field.

B. Dynamically Storage in Cloud [5]

A Flexible Distributed Storage Integrity Auditing Mechanism (FDSIAM) is a mechanism used to dynamically store data in cloud. It uses a protocol using the data reading protocol algorithm to check the data integrity. This mechanism uses homomorphism tokens, blocking erasure, unblocking factors and distributer erasure coded data. These concepts to provide secure data storage. It also used to check the data security provided by the service providers.

C. Identify –Based Authentication[5]

The security is provided with the help of private and public key pair without the need for certificates and deployment. The key is generated using the unique identity. The

private key is generated using the public identity of each entity.

A identify based encryption (IBE) and Identity Based Signature (IBS) are used to provide authentication based on identity. When SSH Authentication Protocol (SAP) is a very complex and hence an alternative to SAP is a new authentication protocol based on identity. It is hierarchical model with particular signature and encryption scheme.

D. Third Party Auditing (TPA)[5]

The small and medium enterprise may have huge amount of data. It is difficult and expensive for those data owners to check for the data correctness in a cloud environment. A trusted auditing organization works in the between to provide secure storage to the cloud users.

To achieve data storage security, BLS (Bonch-Lynn- Sachems) algorithm is used to sign the data blocks before outsourcing data into cloud. Reed Solomon technique is used to provide error correction and to support data storage correction. It is homogeneous in nature.

E. Secure and Dependable Storage Service[5]

The storage service provides a way to store data which can be used later for well qualified applications. A distributed auditing mechanism is used for storage service by utilizing the homomorphism token and distributed coded-data. They help us to utilize the available data which has been stored without worrying about security concerns. The proposed system support efficient dynamic operation on outsource data which includes block modification, deletion and append. Table 1 lists the factors provided by the each of the security mechanisms.

Table 1 Comparison of Security Mechanisms for Cloud

S. No	Technique	Influencing Factors
1.	Implicit Storage Security to Data in Online [5]	Confidentiality, Privacy
2.	Dynamically Store Data in Cloud [5]	Availability, Integrity
3.	Identify –Based Authentication[5]	Confidentiality, Integrity
4.	Efficient Third Party Auditing (TPA)[5]	Availability, Confidentiality, Integrity, Privacy
5.	Secure and Dependable Storage Service[5]	Availability, Privacy
6.	Key Aggregate Cryptosystem[5]	Availability, Confidentiality, Integrity

F. Key Aggregate Cryptosystem[5]

The Key Aggregate Cryptosystem (KAC) is one of the efficient techniques under public-key encryption. Here the messages are encrypted under the identifier of cipher text called class. Every cipher texts are grouped into different number of classes. The master secret key is used to extract the aggregate key. This aggregate key is a unique key is used for a single class.

Data owner provides this aggregate key to the respected user; the user decrypts the files for that particular class or set. The files out of the set remain confidential. The cipher text, public key, master secret key and aggregate keys are all of constant size. A key aggregate encryption has five polynomial-time algorithms as the following steps as setup phase, keygen phase, encrypt phase, extract phase and decrypt phase.

From all the above described techniques it's clear that encryption provides better security than other techniques. With cloud encryption, even if hackers find a way to access your virtual environment, none of the information will be readable. The best way to build "virtual walls" in the cloud and to prevent hackers from gaining access to your data is to encrypt it.

IV. CRYPTOGRAPHY METHODS

Cryptography derives from Greek kryptos means the art of secret writings i.e by encoding messages into a non-readable form will achieve more security".

- Plaintext (M) is the simple message that to be protected in encrypted form. In cryptography it is known as text, voice, image, video, and data.
- Ciphertext (C) is a message which cannot be understood by anyone or meaningless message.
- Encryption/ enciphering is the process of converting plain text into cipher text. Cryptography uses encryption techniques to send sensitive data through insecure channel.
- Decryption/ deciphering is the reverse process of encryption, i.e. the determination of the original text from the ciphertext
- Both encryption and decryption requires encryption/decryption algorithm and a key (ki).
- Cryptographic algorithm is the mathematical function or functions used for encryption (E)/ decryption (D).
- A Key is a numeric or alpha numeric text or may be a special symbol. The selection of key in Cryptography is very important since the security of encryption algorithm depends directly on it.
- Cryptology is the science of both cryptography and cryptanalysis.
- Cryptographer is the person dealing with cryptography.
- Cryptanalyst is the person dealing with cryptanalysis.
- Cryptologist is the person dealing with cryptology.
- Attack is the cryptanalytic attempt.
- Cryptosystem is the system where an encryption/decryption process takes place.
- Steganography is the technique of hiding secret messages into innocuous messages, such that every secret message is hidden (invisible).

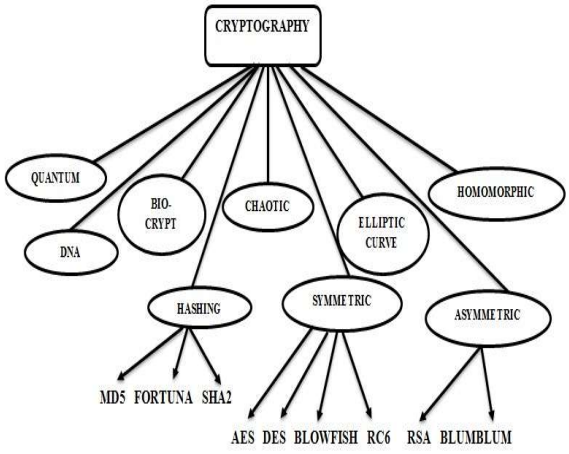

Figure 1: Classification of Cryptography

Figure 1 gives the overall classification of the general cryptographic techniques. These techniques are briefly described below.

There are three types of techniques:–

1. ***Symmetric Key Cryptography*** – Private-key cryptography, also known as symmetric cryptography, a single key or private key is used for both encryption and decryption process. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data.
2. ***Asymmetric Key cryptography*** - Public-key cryptography, also known as asymmetric cryptography, requires two separate keys, one to

encrypt the plaintext, and one decrypt the cipher text. One of these key is public and the other is kept private. Although, the two different parts of this key pair are mathematically linked.

3. ***Hash function Cryptography*** - The hash function cryptography (One way cryptography) offers a way of creating a fixed-size blocks of data by using entry data with variable length. It is also known as taking the digital fingerprint of the data, and the exit data are known as message digest or one- way encryption. If the data is modified after the hash function was generated, the second value of the hash function of the data will be different. Even the slightest alteration of the data like adding a comma into a text, will create huge differences between the hash values. The hash values solve the problem of the integrity of the messages.

Encryption algorithms review:

A. Symmetric Encryption:

1) Blowfish [7]

Blowfish is a fast, compact and simple block size of 64 bits encryption algorithm with variable key length from 32 to 448 bits. It is a 16-roundFeistel cipher and uses large key dependent permutation in P-Box and substitution in S-Boxes. Each S-box contains 32 bits of data. This algorithm consists of two sub parts, one is key expansion part and the other is data encryption part. In which the key expansion part converts a key of at most 448 bits into 4168 bytes of sub keys and the data encryption is done by completing 16 rounds fiestel network which can be implemented on 32 or 64-bit microprocessor. This algorithm is suitable when the key is not changing frequently in any other applications.

Advantages:

1. Provides high level of security to cryptanalysis.
2. It is considerably faster than most encryption algorithms.
3. Blowfish is invulnerable against differential related- key attacks.

Limitations:

1. Blowfish has some classes of weak keys.
2. The reliability of Blowfish is questionable due to the large no. of weak keys.

2) Data Encryption Standard [8]

The Data Encryption Standard (DES) is a symmetric-key algorithm for the encryption of data. DES is a block cipher that enciphers 64-bit blocks of data with a 56-bit key. The remaining eight bits are used for checking parity. Decryption uses the same structure as encryption but with the keys used in reverse order.

Advantages:

1. The same hardware or software can be used in both directions.

Disadvantages:

1. Small key size which offers less security.
2. Its encryption speed which is very slow.
3. Advanced Encryption Standard [7]

AES is a symmetric key block cipher and is fast in both software and hardware. AES has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits with variable 10, 12, or 14 rounds. The AES algorithm holds a 4 by 4 array of bytes called the state, which is initialized to the input of 128 bits (i.e., 16 bytes) to the cipher. The substitution and permutation operations are all applied to

the state array. There are four stages in every round of AES. It also contains a single S- box and same algorithm is used in reversed for decryption. Its symmetric and parallel structure provides great flexibility for implementers, with effective resistance against cryptanalytic attacks. AES can be implemented and well adapted on processors such as Pentium, RISC and parallel processors.

Advantages:

1. AES is compact cipher and it works fast by using variable key length.
2. It provides resistance against certain collision attacks.

Disadvantages:

1. AES has no serious weakness.
2. The mathematical property of the cipher might be vulnerable into an attack.

B. Asymmetric* Encryption*:

1) RSA [8]

RSA (stands for Rivest, Shamir Adleman) is a public-key cryptography and is widely used for secure data transmission. In RSA, one of the key can be shared with everyone and another key must be kept private. The public key consists of the modulus n and the public (or encryption) exponent e. The modulus n is the product of two large prime numbers p and q. The private key consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q, and φ(n) must also be kept secret because they can be used to calculated. Anyone can use the public key to encrypt a message, but in some cases if the public key is large enough, only someone with knowledge of the prime factors can get the possible decode of the message. The decryption of message does not take excessive time to get the original text.

Advantages:

1. Its security is based on the difficulty of factoring large integers.
2. The RSA scheme can be used for security and authenticity.

Disadvantage:

1. Slow compared to existing encryption algorithms. Table 2 Comparison of Encryption Algorithms.

The above compares the four algorithms discussed above based on some common parameters such as key size, execution time, memory required by that algorithm, attacks that are vulnerable to, usage of random sequence, confusion and diffusion.

C. Quantum Cryptography [9]

Quantum cryptography uses quantum mechanical properties to perform cryptographic tasks. The polarization property of quantum mechanics restricts attackers. An invisible photon is used as key. Since it is based on cloning theory, replacing the data without the knowledge of owner is impossible. It also provide reliable digital signature.

Advantages:

1. Robust to brute force attack.
2. Encrypted data cannot be copied or read.

Disadvantage:

1. Vulnerable to man in middle and denial of service attacks.

D. Elliptic Curve Cryptography (ECC)[9]

Elliptic curve public key cryptography (ECC) is a new approach with low key size based on the algebraic structure of elliptic curves over finite fields. On sharing the secret key, the ECC deals with two points(x, y)

which satisfy the equation $y_2=x_3+ax+b$ with some condition $(4a_3+27b_2=0)$.The points which lies on the curve act as a public key and the selection of random numbers is used as private key. ECC is used in several integer factorization algorithms that have applications in cryptography

Table 2: Comparison of Encryption Algorithms

CHARACTERISTICS	DES	AES	RSA	BLOWFISH
Key Size	Small 56 bits	Medium 128,192, 256 bits	Large 1024 bits	Small/ Large 32-448 bits
Execution Time	Faster (equals to AES)	Faster	Slow	Faster (less than AES)
Memory Usage	High (more than AES)	Low	Highest	Least (require less than 5KB)
Vulnerable to attack	Differential & Linear crypt analysis, Brute force attack	Known plaintext, side channel attack	Related key attack, algebraic attack	Second order differential attack, weak key
Random Number	Yes	Yes	Yes	Yes
Confusion/Diffusion	By Feistel Structure	By Feistel Structure	Based on Factoring of Prime Numbers	By Feistel Structure
No. of Rounds	16	10 or 12 or 14	1	16

Advantages:

1. ECC offers considerably greater security for a given key size.
2. ECC uses short key length which leads to fast encryption speed and less power consumption.
3. Because of its low key size which became time challenge for an intruder to break into the system.

Disadvantage:

1. ECC increases the size of encrypted text.
2. ECC is dependent on very complex equations which lead to increase the complexity of encryption algorithm.

E. Bio Cryptosystems [9]

Bio cryptosystem is an emerging technology which combines biometrics with cryptography. It is based on Biometric key authentication to avoid duplication cryptography keys are much harder to remember but in bio- cryptography the password codes are short and it is easy to use them often. Biometric system protection schemes are in high demand nowadays.

Advantages:

1. No need to remember such large key values.
2. It provides more secure identification and privacy for the users.

Disadvantage:

1. The major issue with Bio Cryptosystems is the high variability of biometric traits which creates fuzziness problems.

F. Chaotic Cryptography[10]:

Chaotic cryptography is the application of the mathematical chaos theory to the practice of the cryptography, the study or techniques used to privately and securely transmit information with the presence of a third-party or adversary. Properties in chaotic systems and cryptographic primitives share unique characteristics that allow for the chaotic systems to be applied to cryptography. Chaos theory used in cryptosystems for commercial implementation has proven to be unsuccessful mainly because a chaos theories' requirement to use intervals of real numbers.

Table 3 Comparison of Cryptography Algorithms

Crypto graphic tech-niques	Memory usage	Execution time	Descrip-tion	Com-plexity	Pub-lic/ Pri-vate Key
etric	Depends on the algorithm	Fast	Single key is used for encryption an decryp-tion	Less	key
Asym metric	Depends on the algo-rithm	Slower than sym-metric	Uses public and private keys for encryption and de-cryption	More than sym-metric	Public and Private key
Homo-morphic	High	Slow	Encrypts the encryp-tions of the prod-uct or sum of two messages	More	Either Private or Public key
Hashing	Similar to symmetric cryptogra-phy	Fast	Encrypts based on a hash function	Less	Private key
Bio–cryptogra-phy	high	Medium	Based on biometric key for en-cryption	More	Public and Pri-vate key
Elliptic curve	High	Slower than symmetric	Based on mathe-matical equation	More	Either Public or Private key
Chaotic Cryptogra-phy	High	Slow	Based on mathe-matical chaos theory defined on real num-bers	More	Private key

Advantages:

If chaotic parameters as well as cryptographic keys can be mapped symmetrically, it is difficult to find the outputs without any knowledge the initial values.

Disadvantages:

Low acceptable performance.

G. Homomorphic encryption [11]

Homomorphic encryption is the process of data encrypted on a remote storage which the decryption does not take place since the consumer will have the private key (secret key). In homomorphic, while before sending the data to the provider, they encrypt the data in advance. The decryption of data takes place every time to required that data, the same process is done to obtain the plaintext.

Advantage:

1. They protect the data confidentiality and privacy.
2. Allows processing without giving away access.

5. DNA CRYPTOGRAPHY

The strength of cryptography mechanisms lie on the degree of randomness and uncertainty present in the cipher.

To provide these, many phenomenon of nature have been used. DNA (De-oxy Ribonucleic Acid) cryptography is one such ph*enomenon that exploits the extreme* complexity *and randomness* in the DNA structure for coding and decoding. DNA is used in cryptography as a means for storing and retrieving information, as well as for computation. But the use of DNA for these purposes requires highly technical laboratories and has computational limitations, making efficient use of DNA cryptography difficult. To overcome these difficulties it is necessary to provide theoretical analysis first and thus the concept of DNA cryptography was introduced. It is based on the central dogma of molecular biology and utilizes the special properties of DNA for encryption.

DNA based cryptography methods:

A. Pseudo DNA Cryptography [12]:

This method was developed by Ning Kang. It makes use of the concepts of how

messages are stored in DNA and then transferred to messenger RNA (Ribonucleic Acid) and then to proteins which is the cipher text. The key contains introns starting and pattern codes, codon-amino acid mapping of proteins. This is mostly used to enhance the security of other cryptographic algorithms.

Advantages:

1. Easy to encrypt
2. Since the cipher is in the form of protein, it is generally smaller than the plaintext.
3. One-time pad can be used as a key.

Disadvantages:

1. Mostly confusion and little diffusion. Hence partial information is available which makes the cipher vulnerable to differential analysis attacks.
2. The complexity of decryption increases with key complexity.

B. Secure Communication Protocol With DNA Primer [13]:

A primer is a short DNA sequence for recognizing genes. The primers are used as keys. Inspired from this, this protocol was proposed where the messages are treated as primers to select a sequence prefabricated in a codebook. The sender and receiver each have a copy of codebook containing large number of DNA sequences. The messages are predesigned and every primer can encode only one message.

Advantage:

1. The original message was never transmitted

Disadvantage:

1. Sequences in codebook have to be pre -fabricated.
2. Code book has to be securely delivered.
3. Not possible to communicate new messages.

C. Data Security and Cryptography based on DNA sequencing [14]:

In this method, a session key is shared between the sender and receiver for encryption. There are two round of encryption. The round 1 key for encryption is generated by a random number generator. In Round 2, a DNA sequence is selected as a key randomly from publicly available DNA sequences. The first round is based on cipher block-chaining methods. In round 2, the DNA sequence is segmented and converted to hexadecimal form. Then addition is performed between round 1 encrypted text and the segmented DNA sequence in 8-bit blocks. It is then converted to fake DNA sequence by binary coding scheme and extra information regarding starting and ending primers are added. This method is based on the concept of conventional symmetric key cryptography.

Advantages:

1. The availability of a large collection of DNA sequences makes it difficult to predict the selected sequence.
2. Extra information present in cipher text provides more security to algorithm.

Disadvantage:

1. Extra space required.
2. Involves random number generation.

D. DNA based Encryption Methods [15]:

Based on the special properties of DNA sequences three DNA based encryption methods have been introduced. They are all based upon a reference DNA sequence S known only to the sender and the receiver.

In the 'Insertion Method', S is coded into a binary sequence based on binary coding rule. It is then divided into segments of each k bits and message bits are appended to it. Binary coding scheme is again applied to produce the fake DNA sequence.

The 'Complementary Pair Approach' is based on the base pairs of RNA. An artificial sequence is generated. Message is divided to segments of two bits and converted to DNA sequences. The segments are inserted within the complementary substrings of length k, based on random number generator.

In the 'Substitution Approach', p (number of bits in message) distinct numbers are randomly generated between 1 to length of reference sequence. It is then transformed into fake DNA sequence by three substitution rules:

1) Substitute Si by Si
2) Substitute Si by its complement
3) Substitute Si by its double complement.

Advantage:

1. The availability of a large collection of DNA sequences makes it difficult to predict the selected sequence.

E. Index based Symmetric DNA Encryption [16]:

In this method, two keys are used. Initial key is generated randomly consisting of two double numbers. The second key is a special DNA sequence. The plaintext is transformed into ASCII notation. XOR operation is performed between 32-bit plaintext and the initial key, to get sequence m1. According to DNA binary coding scheme, m1 is converted into DNA sequence consisting of 16 nucleotides. From the special DNA sequence, a position X is selected randomly to find the special string which is same as m1. The process is repeated for all 32 - bit blocks of the plain text. Then finally all the positions are converted into a cipher text array pointer.

Advantages:

1. It is robust to plaintext oriented attacks.

F. Data Encryption using Bio-molecular Information[17]:

Several stages of conversions are performed based on different conversion tables. The first table maps DNA and RNA alphabets to binary bits. Each 3 letter codon DNA sequence is mapped to an alphanumeric value in another table. The alphanumeric representations are used for insertion or substitution of message into fake DNA sequence. The main strength of the algorithm lies on the secret key which is based on the amino acid properties of associated codons and sequences. This key is used in the alpha numeric conversion table.

Advantage:

1. Size of cipher is not same as plain text.
2. Adds uncertainty to key and message exploitation.

G. DNA based Data Encryption and Hiding using Play- fair Cipher and Insertion Techniques[18]:

This method combines DNA based cryptography method with data hiding techniques to improve security. The algorithm is implemented in two stages: The first stage encrypts plaintext using DNA and Amino Acid based play fair cipher. The second applies a secure insertion method to hide the encrypted DNA cipher text into some reference DNA sequence.

Advantage

1. It is difficult to predict whether or not there are secret messages hidden in DNA sequence.

2. It is difficult to correctly decrypt without play fair cipher secret key.

H. Novel DNA Computing based Encryption and Decryption Algorithm [19]:

The algorithm has two parts: 1) DNA computing based encoding algorithm 2) DNA computing based encryption and decryption algorithm. The amino acid encoding table is generated dynamically providing dynamicity of encryption process.

Advantages

1. Complete character set encoding.
2. Robust.

The various DNA based cryptographic algorithms were discussed.

6. CONCLUSION

Cloud computing is a set of IT services that are provided to a customer over a network on a leased basis and with the ability to scale up or down their service requirements. The major data security issues in cloud and the techniques to overcome them were discussed. And a survey was presented on the major cryptographic mechanisms used in cloud.

REFERENCES:

[1] http://www.nist.gov/itl/csd/cloud-102511.cfm

[2] Farzad Sabahi, "Cloud Computing Security Threats and Responses," Communication Software and Networks (ICCSN), Institute of Electrical and Electronics Engineers Third International Conference, 2011.

[3] Ashish Agarwal, Aparna Agarwal, "The Security Risks Associated with Cloud Computing," International Journal of Computer Applications in Engineering Sciences, vol. I, Special Issue On Cns, Issn: 2231-4946, July 2011.

[4] Selvamani K, Jayanthi S, "A Review on Cloud Data Security and its Mitigation Techniques", *International Conference on Intelligent Computing, Communication & Convergence,* Procedia Computer Science 48, 347 – 352, 2015.

[5] Spoorthy V, Mamatha M, Santhosh Kumar B, "A Survey on Data Storage and Security in Cloud Computing", *International Journal of Computer Science and Mobile Computing,* IJCSMC, Vol. 3, Issue. 6, pg. 306 – 313, June 2014.

[6] Rohit Bhadauria, Sugata Sanyal, "Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques".

[7] Hemalatha N, Jenis A, Cecil Donald A, Arockiam L, "A Comparative Analysis of Encryption Techniques and Data Security Issues in Cloud Computing", *International Journal of Computer Apllicaions,* Vol. 96, No.16, June 2014.

[8] Jyotirmoy Das, "A Study on Modern Cryptography and their Security Issues", *International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 10, October 2014.*

[9] Ijaz Ali Shoukat, Kamalrulnizam Abu Bakar, Mohsin Iftikhar, "A Survey about the Latest Trends and Research Issues of Cryptographic Elements", *International Journal of Computer Science Issues,* Vol. 8, Issue 3, No. 2, May 2011.

[10] Woods, Christopher A, "Chaos based Symmetric-Key Cryptosystems", cs.rit.edu,2015.

[11] Rashmi Nigoti, Manoj Jhuria, Shailendra Singh, "A Survey of

Cryptographic Algorithms for Cloud Computing", *International Journal of Emerging Technologies in Computational and Applies Sciences*, ISSN 2279-0047, pp.141-146, March-May 2013.

[12] Kang Nin,. "A Pseudo DNA Cryptography Method", http:// arxiv.org/abs/0903.269, 2009.

[13] Qinghai Gao, "A few DNA Security".

[14] Nirmalaya Kar, Atance Majumder, Ashim Saha, Suman Deb, "Data Security and Cryptography based on DNA Sequencing", *International Journal of Information Technology & Computer Science (IJITCS)*, Volume 10 : Issue No:3,ISSN No :2091-1610, August 2013.

[15] H. Z. Hsu, R. C. T. Lee, "DNA Based Encryption Methods", The 23rd Workshop on Combinatorial Mathematics and Computation Theory, April 2006.

[16] Y. Zhang, Y. Zhu, Z. Wang, R.O. Sinnott, "Index based Symmetric DNA Encryption Algorithm", Proceedings of the 2011 4th International Congress on Image and Signal Processing, pp. 2290 - 2294, 2011.

[17] Behnam Bazil, Mustafa Anil Tuncel, "Data Encryption using Bio-Molecular Information", *International Journal on Cryptography and Information Security, Vol. 4, No.3, Sept 2014.*

[18] Ahmed Atito, Amal Khalifa, S.Z Rida, "DNA – Based Data Encryption and Hiding using Playfair and Insertion Techniques", *Journal of Communications and Computer Engineering*, Vol.2, Issue.3, pg 44-49, 2012.

[19] Noorul Hussain Ubaidur Rahman, Chithralekha Balamurugan, Rajapandian Mariappan, "A Novel DNA Computing based Encryption and Decryption Algorithm", International Conference on Information and Communication Technologies (ICICT 2014), Procedia Computer Science 46, 463 – 475, 2015.