EasyChair Preprint

№ 3899

Security Issues in Encrypting Cloud Data

Srishti Varma, Ritu Gupta, Priya Verma, Abhilasha Singh and Arun Kumar

July 18, 2020

SECURITY ISSUES IN ENCRYPTING CLOUD DATA

Ms. Srishti Varma[1], Ms. Ritu Gupta[2], Ms. Priya Varma[3], Dr. Abhilasha Singh[4], Mr. Arun Kumar[5]

[1,3]Student, Department of Information Technology, Amity University, U.P., India

[2,4]Assistant Professor, Department of Information Technology, Amity University, U.P., India

[5]SRM Institute of Science and Technology, NCR Campus, Ghaziabad, India

[1]srishtivarma98@gmail.com, [2]ritu4006@gmail.com, [3]priyaverma2099@gmail.com, [4]abhilashasingh28@gmail.com, [5]arunvlsi83@gmail.com

Abstract:

Cloud computing is the capacity to deliver a service over a system through the web. With the cloud, users can have access to any file or application present in the cloud. It provides several computing services such as files, folders, storage, database, software, network, and many more. Everyone is concerned about the privacy of their personal and business-related information present in the cloud. Data is secured in the cloud by the process of encryption which is performed by several cryptographic algorithms. These algorithms are also adopted by the Cloud Service Provider (CSP). Though cloud computing has several benefits, there are also some risks and challenges that should be kept in mind while using cloud computing.

Keywords: Data lifecycle, SPI Model, Cryptography, Cryptographic Algorithms, Cloud Security.

Introduction

In recent years, cloud computing is considered an emerging technology that connects different systems at the same time to share or exchange files, folders, software, and many other resources. Earlier, the traditional way of computing was used, in which the user can access the data only in the device in which it is stored. But by using cloud computing, the user can access the data whenever he wants and at any place. The data is not limited to only one system or framework. It helps in reducing the cost and storage space for the data. It allows a company to pay for only the amount it needs for the data storage unlike the traditional way of computing which requires a lot of hardware and software establishments. Thus, cloud computing gives us a lot of advantages over traditional computing. As the resources in cloud computing are shared over the web, there are chances that this data may get attacked and might go to the person for which the data may not be intended and thus hacking our cloud data, so the security of our cloud data is a must whether it is of our personal use or for any of our businesses. Cloud security can be defined as a complex interaction between technologies, control, processes, and policies. There are several cloud service providers such as AWS, Azure which provide the user with cloud-based security solutions by encrypting the data which had been uploaded on the cloud. The service provider must guarantee that the client's database and framework applications are secure constantly from undesirable accesses [1]. The client should find a way to ensure the safety of their applications by making sure about the passwords and restricting the number of individuals who can get to their sensitive information. Cloud-based applications are helpful for some organizations, as they empower secure information the board, investigation, and access from anyplace [2]. All the cloud computing services provided by the service providers are built upon the same conceptual framework which is housed in the data center. Data centers consist of any resource you have uploaded on the cloud, they are owned and maintained by the cloud service provider. These data centers help to keep your data safe from any kind of theft and destruction and make sure that your data is intact and you can access it without any disturbance. Cloud computing services are of three types- Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). These services are also known as the SPI (SaaS, PaaS, IaaS) model [3]. The most common question when we upload any resource in the cloud is how safe is our data in the cloud? The cloud service providers use different algorithms to protect your data using encryption of your data. In this, your readable text is converted into unreadable text so that only the person who has the key for the algorithm can decrypt the text. Also, the cloud systems can use authentication processes to limit any access by introducing username and password; although password can be hacked by several attacks (for example- brute force attack), this is where the encryption algorithm plays its role and your data is secured, it is very difficult to break encryption algorithm without the key, therefore only the person with the key can decrypt it [4].

Literature Review

Rachna Arora and Anshu Parashar discuss the importance of cloud computing which is rapidly increasing, as it provides convenient network access to many computing resources such as network, application, storage, etc. but there are certain challenges in cloud computing about security at all levels of the network. The SPI (SaaS, PaaS, IaaS) Model is also discussed in the paper in detail [5].

Dr. A. Padmapriya and P. Subhasri discuss cloud computing as an internet-based technology that consists of hardware, software, virtual resources, etc, and these can be shared over a network. But there is a chance that an unwanted attack takes place in an organization's cloud and may leak the data that is present there, some security issues and how we can overcome them are discussed there [6].

M. Vijaypriya discusses network security which is rapidly becoming important, as it ensures that the users are connected and have access to the data without any malicious attack. For the security of their data, organizations are using security algorithms such as RSA, ECC, AES, etc for data encryption and decryption [7].

Dr. Rajamohan Partasarthy et al. gives insight into the detailed review of the cloud computing SPI model. Also, it discusses one of the widely used security algorithms – the RSA (Rivest-Shamir-Adleman) algorithm which is a public key algorithm [8].

Martan van Dijk et al. exclusively discuss fully homomorphic encryption with a small size of ciphertext and key. It also discusses the data life cycle in detail [9, 10].

Nasarul Islam et al. discusses various cloud service providers such as Amazon, Google, Microsoft, Salesforce.com, etc. They compared several algorithms that these cloud service providers use for data encryption based on recent studies [11].

R. Gowthami Saranya et al. show how different cryptographic algorithms works and help in securing the cloud data by applying them [12].

Data Lifecycle

There is a sequence of stages through which the data present in the cloud goes through, this is known as the data life cycle in the cloud. The data life cycle provides a significant level synopsis of the stages involved in ineffective organization and security of data for utilizing and reuse. The data lifecycle includes six phases, which are:

- **Create:** It means to create or apply changes to any data, and not just a document or database. It is the development of new data or alteration of existing information.
- **Store:** The data is stored from where it continuously appears from its creation.
- **Use:** The data can be used by the organization and can also be processed.
- **Share:** the data present in the cloud can be shared among employees of the organization, a trusted third party, partners, customers, etc.
- **Archive:** Data leaves dynamic use and enters long haul storage.
- **Destroy:** Data is indefinitely destroyed using tangible or digital methods.

Although, once a data is created, it can bounce between phases without any restriction and may not pass through all stages. For example- not all data are destroyed. Figure-1 represents the data life cycle in the cloud.

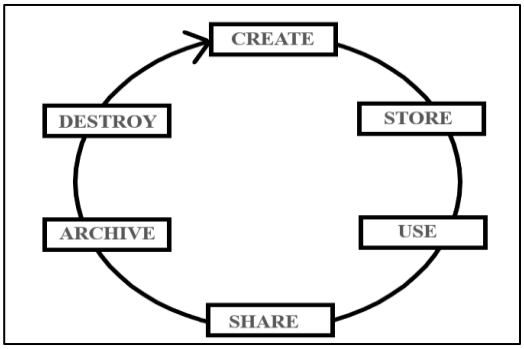

Fig.1. Data Lifecycle

Cloud Service Models- The SPI Model

Cloud computing is differentiated based on the services they provide to their customers. There are mainly three types of service models provided by cloud service providers to their customers (Figure-2).

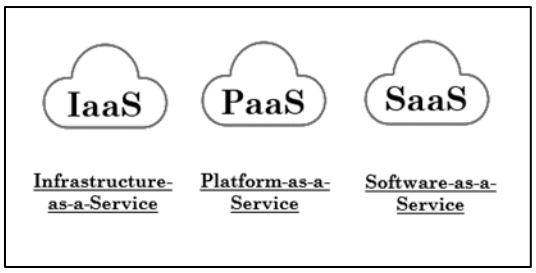

Fig.2. Types of Cloud Service Model

They are as follows:

- **Information-as-a-Service (IaaS):** The basic function of IaaS can be phrased as "Host". IaaS is considered as the most adaptable cloud model that permits total versatile power over the administration and customization of the foundation. In this administration, the cloud administration gives the client virtual machines and various resources as help. Amazon Web Service (AWS) is an example of IaaS.
- **Platform-as-a-Service (PaaS):** The basic function of PaaS can be phrased as "Build". In PaaS, an outcast seller provides the association with a phase where you can run applications and create itself. As the seller is empowering the cloud administration which supports the stage, it discards your need to introduce in-house hardware. In this you can't control the fundamental structures, for example, working frameworks, stockpiling, servers, and so forth. Google app engine is an example of such a model.
- **Software-as-a-Service (SaaS):** The basic function of SaaS can be phrased as "Consume". SaaS allows your association to briskly get the opportunity to cloud-based web applications without centering for introducing in the fresh framework. The applications run on the seller's cloud, which they, control and keep up. The applications are open for use with paid support, or with no amount with limited access. SaaS doesn't need any kind of establishments in your current structure, which hence takes out the need to present, keep up, and update applications. Salesforce is an example of such a model.

Introduction to Cryptography

Cryptography or cryptology is defined as a practice of protecting information through the utilization of rules so that just the individual for whomever the data is planned can get and understand it; consequently, hindering unapproved entry to data. The prefix 'crypt' means 'hidden' and suffix 'graphy' means 'writing'. Cryptography has four main purposes:

- **Confidentiality:** Information is available to only those for whom the information is aimed and no other individual can retrieve it.
- **Integrity:** This ensures that the information has not been manipulated in storage or transition between the sender the intended receiver.
- **Authentication:** This confirms the individuality of the sender and the recipient, as well as the starting and ending place of the information.
- **Non-Repudiation:** This prevents the sender from denying his intention to send any information at later stages.

In cryptology, the procedures which are utilized for security of data are acquired from scientific ideas and a set of rule-based calculation called algorithm to change the messages so that they are unreadable and hard to decode. Cryptography is the process of converting readable text to unreadable text, and only the intended person could read it is acknowledged as encryption. The procedure of changing back the unreadable message (ciphertext) to readable messages (plain text) is acknowledged as decoding.

Types of Cryptography Algorithms

There are mainly three types of cryptographic algorithms by which encryption and decryption work. These algorithms use at least one encryption key which makes encryption simple but the decryption is relatively difficult without knowing the keys, these are:

- **Symmetric key cryptography:** An encryption algorithm is known as symmetric if it uses the same key to encrypt and decrypt messages. Here, the encryption key 'e' and decryption key 'd' are meant to be the same. Symmetric encryption is also known as a shared key, shared secret, secret key encryption. In this, all the intended recipients have access to the shared key. But sharing the key can be a problem, sharing the key manually can be considered as a cumbersome task. Therefore, safe communication needs to be established between the recipients so that the ciphertext and key can be shared among them. Symmetric algorithms are considered to be more secure and faster. Some algorithms that use symmetric encryption are Data Encryption Standard (DES), Triple-DES (3DES), Advanced Encryption Standard (AES), RC5, Blowfish, etc. Figure-3 shows how the symmetric algorithm works with the shared key.

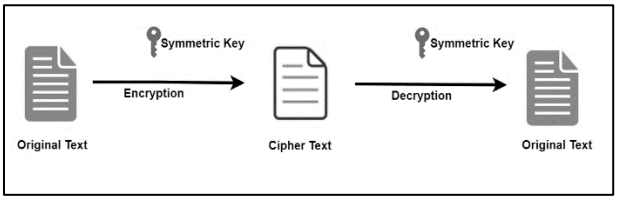

Fig.3. Symmetric Algorithm

- **Asymmetric Algorithm:** An encryption algorithm is known as asymmetric if it uses one key to encipher the information and a different, but mathematically related key to decipher the information. It is reckoning impracticable to determine a key in the event if somebody knows the other key, thus one key can be distributed publicly, this key is public key; and the other related key is kept safe and secure, this key is a private key. Together both the keys are referred to as key pairs. The asymmetric algorithm is also known as public-key cryptography. It is easy to solve mathematical problems but it is difficult to reverse it. Some algorithms that use asymmetric encryption are Rivest-Shamir-Adleman (RSA) algorithm, Elliptic Curve Cryptography (ECC), Digital Signature Algorithm (DSA), etc. Figure-4 illustrates how the asymmetric algorithm works using a public key and a private key.

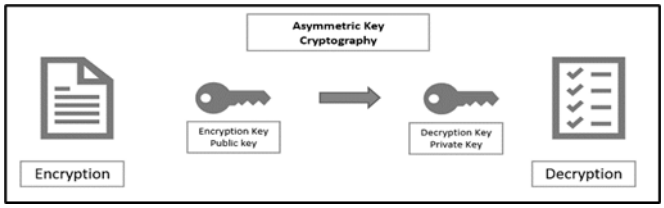

Fig.4. Asymmetric Algorithm

- **Hash function:** In this, there is no utilization of a key for encryption or decryption. A hash value with irreversible length is determined by the original text making it difficult to recover the contents of the original text. Example of hash functions include: SHA-256, SHA-328, SHA-224, SHA-512 etc.

Cryptographic Algorithm

Algorithms are necessary as they provide the security that the data needs when it is being transferred over the internet. They provide encryption methodology that is the best technique to protect your cloud data. Some of the known algorithms that are also adopted by cloud service providers are explained in this section.

A. RSA Algorithm

RSA Algorithm was developed in 1977, by three scientists namely Ron Rivest, Adi Shamir, and Leonard Adleman. It is the most widely used encryption techniques. RSA Algorithm is an asymmetric cryptographic algorithm i.e. this uses two distinct but related keys, one is a public key and the other is a private key. The public key is distributed among trusted parties but the private key is only given to the intended receiver. As it is asymmetric, so no one can decrypt the data except the one intended receiver who has the private key,

the data cannot be decrypted using the public key even though it is mathematically related to the private key [13].

The methodology of RSA:

- It is hard to factorize a large number.
- In this, the public key comprises of two numbers where two large prime numbers are multiplied to form one large number.
- Also, the private key is acquired from the two large prime numbers only.
- So, if anyone factorizes this number, the private key will be compromised.
- Thus, encryption stability lies on the key size.
- RSA keys can be 1024 bits or 2048 bits long.

Algorithm of RSA:

1. Key generation:
- Choose two definite prime numbers A & B.
- Determine N=A*B.
- Determine the Euler's function:
- Ø(N) = (A-1) * (B-1).
- Select an integer e such that 1<e<Ø(N). e should not be a factor of N; it is released as a public key exponent.
- Now, the private key component d is calculated as d=e-1(mod Ø(N)). This shows that d is the multiplicative inverse of e-1(mod Ø(N)) or d*e = mod Ø(N).
- Thus, the public key consists of (e, N), and the private key consists of (d, N).

2. Encryption:
- When the data is encrypted, the ciphertext C is obtained as C=me (mod N), where m is mapped data or the message simply.
- This encrypted text is then collected by the cloud service provider.

3. Decryption:
- Whenever a user seeks the CSP for the data, it verifies its authenticity and provides the user with ciphertext C.
- The user then decrypts C using the private key d as m= Cd (mod N).
- So once m is obtained, and the original message is also obtained.

B. Data Encryption Standard (DES)

DES algorithm originated in 1997. It was published by the National Institute of Standards and Technology (NIST). This algorithm has been found at risk against very powerful attacks, thus there is a decrease in its popularity. It is a symmetric key block cipher. DES is an execution of Feistel Cipher. It encodes the data in a block size of 64-bits each, i.e. 64-bits plain text is taken as input to DES which produces 64-bits ciphertext. The size of its key is 56-bits. It uses 16-round of Feistel cipher or steps known as rounds.

As mentioned, that DES uses 56-bits key, initially its 64-bits only but as the process starts every 8th bit is rejected to produce 56-bits key. DES has two fundamental attributes-confusion (substitution) and diffusion (transposition). Figure-5 depicts how a DES algorithm works.

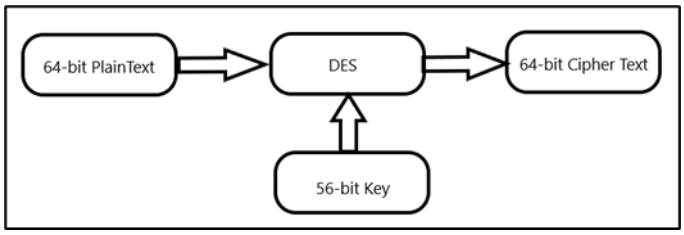

Fig.5. DES Algorithm

Steps involved in DES:

- The 64-bit plain text is passed through initial permutation (IP). This IP takes place only once and before the first round. IP tells us that how diffusion proceeds.
- Then, IP produces two halves of the permuted block, known as Left Plain Text (LPT) and Right Plain Text (RPT).
- These LPT and RPT undergo 16 rounds of Feistel Cipher. At this stage, LPT and RPT have 32-bits.
- Then, LPT and RPT are combined to perform Final Permutation (FP).
- And thus, the 64-bit ciphertext is produced.

Algorithm of DES:

DES_Encrypt (N, K) where M = (LPT, RPT)
N ←IP(N)
For round ←1 to 16 do
Ki ←SK (K, round)
LPT ←LPT xor F (RPT, Ki)
swap (LPT, RPT)
end
swap (LPT, RPT)
M ←IP-1(N)
return N
End

C. Double DES (2DES)

- Double DES (2DES) is an encryption technique that uses two instances of DES on the original message. On this message, two different keys are required to encrypt in both instances. Both keys are required at the time of encryption.
- 2DES uses 112-bit key- two 56-bit keys are used; but gives security level of 256 and not 2112, thus because of a man-in-the-middle attack, breakthrough 2DES is possible.

The following figure depicts how Double DES works (Figure-6).

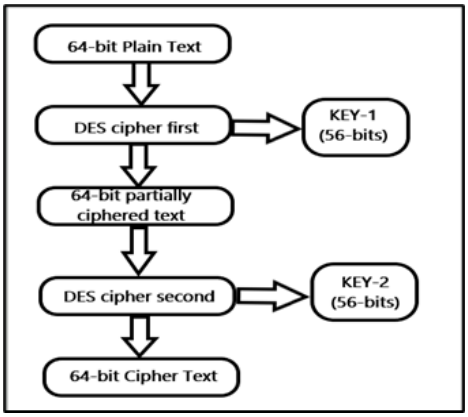

Fig.6. Double DES Algorithm

D. Triple-DES (3DES)

- Triple-DES (3-DES) uses three instances of DES on the original message.
- Three keys are used in this process. There are three ways of choosing these keys-
  a. All keys are different.
  b. Two keys are the same, one is different.
  c. All keys are the same.
- Just like 2DES, 3DES is also vulnerable to a man-in-the-middle attack, that is why it gives the security of 2112 instead of 2168 bits of the key.
- It is also vulnerable to block-collision attacks as it has a small block size and the same key is used for encrypting large plain text.

The following figure depicts how the Triple-DES algorithm works (Figure-7).

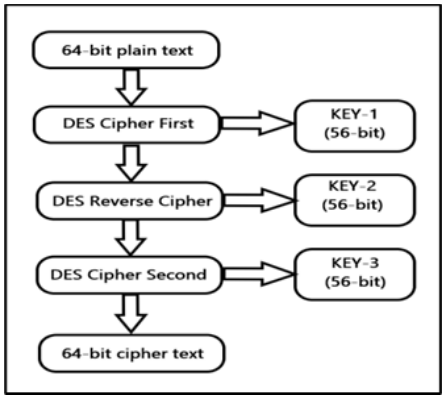

Fig.7. Triple-DES Algorithm

E. Advanced Encryption Standard (AES)

AES is a symmetric block cipher. It was picked up by the US government to ensure that the data is safe. It's used all over the world to secure unprotected information in software and hardware. AES uses 128-bit or 192-bit or 256-bit key length to encode and decode block of messages. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. As AES is symmetric, it uses the same key for encryption and decryption for data security. In one round of AES, it comprises some steps that incorporate confusion, diffusion, and mixing of the input of the original message to change it into the ciphertext. It should be kept in mind, that the key should be protected at all costs. If an attacker gains the key to the encrypted system, the most secure system can also become the most vulnerable system.

Algorithm for AES:

```
Cipher (byte [] input, byte [] output)
{
byte [4,4] State;
copy input [] into State [] AddRoundKey
for (round = 1; round < Nr-1; ++round)
{
SubBytesShiftRowsMixColumnsAddRoundKey
}
SubBytesShiftRowsAddRoundKey
copy State [] to output []}
```

F. Elliptic Curve Cryptography

Elliptic curve cryptography is public-key cryptography based on algebraic structures of elliptic curves. ECC provides small keys as compared to other algorithms and provides the same level of security. This algorithm can be used for key arrangements, digital signature, random number generator, and many more. This cryptographic algorithm came in use worldwide in 2004-2005. This algorithm has several benefits such as its key size is reduced, the storage area is reduced and it can provide the same level of security as compared to large values of any other algorithm.

Steps involved in ECC algorithm:

- Key generation:
  a. Here both the public and private keys are created. For the generation of a public key, the following formula is used T= r* p.
  b. Here, T is the public key; r is the private key and p is the point on the curve. The value of r should be selected at random and it should be in the range of (1 to n-1).
- Encryption:
  a. Let m be the message which is on the point j in the curve and w is randomly selected, we get two ciphertexts- C1 and C2. C1= w*p and C2= j+ w*T
- Decryption:

a. To get the original message, the following formula is applied j= C2-r*C1.

G. Homomorphic Encryption

Homomorphic encryption is a kind of encryption that allows the users to do complex mathematical calculations on the encrypted data without compromising it. When data is encrypted using this encryption, the ciphertext can be used as if it is the original text. The data in such encryption has the same structure and can have similar mathematical operations, so whether the data is encrypted or decrypted, it gives the same result. This has an important role in cloud computing as customers can freely share their encrypted data in the public cloud and then it's the responsibility of cloud service providers to secure it from any attacks [14].

Difference Table of Security Algorithms

Below is a table (Table-1) which depicts differences between different security algorithms discussed in the previous section. This table differentiates the algorithms based on their block size, key size, time complexity, kind of security they provide, and the speed [15].

Table 1. Comparison of various Security Algorithms

S. No	Algorithms	Developed (year)	Block size (bits)	Key size (bits)	Time complexity	Security	Speed
1.	RSA	1977	128	1024-4096	O (n^2.b) or O(log(n^2). log(b))	Considered secure	Very slow
2.	DES	1997	64	56	O (2^{39-43})	Not secure	Very slow
3.	2DES	1998	64	56,112	O (2^{2k})	Not secure	Slow
4.	3DES	1998	64	112, 168	O (2^{39-43})	Secure	Slow
5.	AES	2000	128, 192 or 256	128, 192, 256	O (2^{48})	Highly secured	Very fast
6.	ECC	2002	-	Relatively less	O (n^k) or O (n^{k+1})	Highly secured	Very fast
7.	Homomorphic encryption	1978	-	-	T.polylog(k)	Highly secured	Fast

Cloud Security

When cloud computing is adopted by an organization, security is one of the most critical issues. Cloud security also called distributed computing security, is a lot of control, strategies, methods, and innovation intended to ensure information and cloud arrangement of the association. These safety measures are designed to ensure customer's private information is safe and secure in the cloud. The way cloud security is delivered to the customer by the cloud service provider will depend on the cloud supplier and the security arrangements set by them. However, cloud security procedures should be a joint responsibility between the user and the supplier. There are many cloud service providers such as Amazon Web Services, Microsoft Azure, Google Cloud Platform, IBM Cloud Services, Adobe Creative Cloud, Oracle Cloud, Dropbox, and many more. The cloud service providers provide their customer with only those service which they ask for and pay only for those services [16].

Security Issues in Storing Data in Cloud

There are many issues related to the organization's data security present in the cloud. Following are some common security issues:

- **Data breaches:** In this, unauthorized access to your private/confidential information takes place by a cybercriminal, where he tries to steal your data. Although such acts can be intentional or unintentional.
- **The hijacking of accounts:** In this, a hacker uses an undermined email account to impersonate the account owner. It is a kind of identity theft that can steal the user's information. Account hijacking can be done by phishing or password guessing or sending spoofed emails to the user.
- **Insider threat:** This is a malicious threat to any user's data that comes from inside the organization of the user, like former employees, contractors, business partners, etc. this threat can negatively impact the reputation of an organization.
- **Malware Injection:** In this, the attacker tries to inject a harmful software or a virtual machine into the cloud system of the intended person.
- **Data loss:** It is a condition in which the data of an organization- whether small or large is accidentally deleted or corrupted or is made unreadable by a software or a user for the organization itself.
- **Shared vulnerabilities:** Security of cloud is a mutual responsibility of the cloud service provider and the user or organization. The vulnerabilities in the cloud can be exploited by the hacker for his gain. Weakness can be in any of the software, application, network, etc.
- **Denial of Service (DOS) attack:** This type of attack makes the resources present in the cloud unavailable for legitimate users. DOS attack makes use of cloud data unavailable for legitimate users by flooding them with connection requests.

Conclusion and Future Scope

As the security of cloud data is of prime importance, thus organizations should choose their cloud service provider according to their needs and the services they provide. Though cloud computing has several advantages that are not provided by any other means, several challenges should be kept in mind related to cloud computing. Data should not be leaked to any non-trustworthy third party as this can make the data vulnerable. Many algorithms are used for the protection of data which are adopted by many cloud service providers. As an attack on data can occur on any layer of the network, the multi-level security architecture should be adopted by the organizations for the security of information present on their cloud. Also, Homomorphic Encryption and Elliptic Curve Cryptography (ECC) provides high security and safety as compared to any other algorithm such as RSA, DES, AES and we would consider working on these algorithms for securing cloud data soon.

References

1. Pearson, S., Benameur, A., Privacy, Security, and Trust Issues Arises from Cloud Computing, Cloud Computing Technology and Science (CloudCom), IEEE Second International Conference 2010, On page(s): 693-702.
2. Wang C, Wang Q, Ren K, Lou W (2009) Ensuring Data Storage Security in Cloud Computing. In: The 17th International workshop on quality of service. IEEE Computer Society, Washington, DC, USA, pp 1–9.
3. Jaeger T, Schiffman J (2010) Outlook: cloudy with a chance of Security challenges and improvements. IEEE Security Privacy 8(1):77–80.
4. Devi T, "Data Security Frameworks in Cloud", School of Computing Sciences and Engineering International Conference on Science, Engineering and Management Research (ICSEMR 2014) 978-1-4799-7613-3/14/ ©2014 IEEE.
5. Rachna Arora, Anshu Parashar, "Secure User Data in Cloud Computing Using Encryption Algorithm", IJERA, vol 3, Issue 4, Jul-Aug 2013, pp. 1922-1926.
6. Dr. A. Padmapriya, P. Subhasri, "Cloud Computing: Security Challenges and Encryption Practices", IJARCSSE, vol 3, Issue 3, March 2013.
7. M. Vijaypriya, "Security Algorithm in Cloud Computing: Overview".
8. Dr. Rajamohan Parthasarthy, Ms. Haw Wai Yee, Mr. Seow Seon Loong, Dr. Leelavathi Rajamanickam, Ms. Preethy Ayyapan, "Implementation of RSA Algorithm to Secure Data in Cloud Computing", IJISET, vol 6, Issue 4, April 2019.
9. Martan van Dijk, Craig Gentry, Shai Haleri, Vinod Vaikuntanathan, "Fully Homomorphic Encryption over the Integers".
10. Mr. Manish M Potey, Dr. C A Dhote, Mr. Deepak H Sharma," Homomorphic Encryption for Security of Cloud Data", ScienceDirect, 2016.
11. Nasarul Islam, Mohamed Riyas, "Analysis of Various Encryption Algorithms in Cloud Computing", IJCSMC, Vol 6, Issue 7, July- 2017, pg-90-97.
12. R. Gowthami Saranya, A. Kausalya, "A Comparative Analysis of Security Algorithms using Cryptographic Techniques in Cloud Computing", IJCSIT, Vol8(2), 2017, pg-306-310.
13. Gurpreet Singh, Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES, and AES) for Information Security", International Journal of Computer Applications (0975–8887) Volume 67–No.19, April 2013.
14. Ramaiah, Y. Govinda, and G. Vijaya Kumari. "Efficient public key homomorphic encryption over integer plaintexts." Information Security and Intelligence Control (ISIC), 2012 International Conference on. IEEE, 2012.
15. Keiko Hashizume1, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez "An analysis of security issues for cloud computing", Springer, 2013, 4:5.
16. Jensen M, Schwenk J, Gruschka N, Iacono LL (2009) On technical Security issues in Cloud Computing. In: IEEE International Conference on Cloud Computing (CLOUD'09). 116, 116, pp 109–116.

Authors Profile

Srishti Varma is currently pursuing B.Tech in Information Technology from Amity School of Engineering and Technology, Amity University, Uttar Pradesh. Her interests include Cyber Security, Algorithms and Artificial Intelligence.

Ritu Gupta is currently working as an Assistant Professor in Amity School of Engineering and technology, Amity University, Uttar Pradesh. She has completed her Ph. D from Amity University in the area of Image Processing. She received her M. Tech in Information Technology from MDU, Rohtak, Haryana, India. Her research interest includes Digital Image Processing, Image Security and Cryptography. She has co-authored 25 peer-reviewed research papers in international journals and conferences.

Priya Verma is currently pursing B.Tech in Information Technology from Amity School of Engineering and Technology, Amity University, Uttar Pradesh. Her interests lie in web development, machine learning and artificial intelligence.

Abhilasha Singh is currently working as an Assistant Professor in Amity School of Engineering and technology, Amity University, Uttar Pradesh. She has completed her Ph. D from Amity University in the area of Image Processing. She received her M. Tech in Information Technology from Banasthali University, Rajasthan, India. Her research interest includes Digital Image Watermarking Techniques, Medical Image Watermarking and Bio-Medical Signal Processing. She has co-authored 20 peer-reviewed research papers in international journals and conferences.

Arun Kumar is currently working as an Assistant Professor in SRMIST, Ghaziabad. He has completed his M. Tech in VLSI from SRM University, Chennai, India. His research interest includes Medical Image Processing, Machine Learning and Deep Learning. He has many research papers in international journals and conferences.