Journal of Research Proceedings

JRP

Under the delegate of "Journal of Research Proceedings," we anchor a bimonthly electronic journal enclosing the diverse realms of the educational research field. JRP is providing a platform for the researchers, academicians, professionals, practitioners, and students to impart and share knowledge in the form of high quality empirical and theoretical research papers, case studies, literature reviews, and book reviews.

JRP Publications
www.i-jrp.com
journalrp.editor@gmail.com
9353189468

Survey on cryptographic algorithms in cloud computing

Kota Anjani Vaibhavi[1], Dr.Nagaraj G Cholli [2]

Student, Dept of Information Science and Engineering, R.V. College of Engineering, Bengaluru, India[1]

Associate Professor , Dept of Information Science and Engineering, R.V. College of Engineering, Bengaluru, India [2]

ABSTRACT

In the modern world, many companies and organizations manage a lot of data and they require a platform to store this data. So to fulfill this purpose cloud computing is introduced. Cloud is a platform where we can store the data, files, media etc. in a way that we can access it at any time and perform modifications to it.

So when a user or any company stores its data in a trusted cloud , the main duty of the cloud service provider is to ensure the safety of the data. That is the data should be stored efficiently without any errors or discrepancies. It shouldn't be accessed by unauthorized users or any malicious attackers because that data in the wrong hands can cause a lot of damage.

To overcome the drawbacks in the cloud computing and make it more secure and efficient, we have come up with cloud cryptography. This is done to ensure that the data is properly stored and is safe inside the cloud. This paper gives the idea of what is cloud cryptography, why is it needed and its pros and cons.. It describes some of the different techniques of cryptography and compares them.

KEYWORDS: Cryptography, encryption, authorization, plain text, cipher text, misconfiguration, phishing, DDOS, malware, provenance, remanence, compliance, symmetric and asymmetric algorithms.

I. INTRODUCTION

A. Cloud Computing

The provision of various services over the Internet is cloud computing. Data storage, servers, databases, networking, and software are some of the tools or applications available [1-2]. The word cloud computing refers to the data accessed by distant means in the cloud or in a virtual environment. Cloud-based storage allows files to be saved and retrieved on request to a distant database. Types of cloud include public ,private and hybrid cloud models [3].

Public cloud is the cloud which allows all the users over the internet who has an account to access the information stored by the user in the public cloud. Private cloud is a space which can be used by a company or industry alone which handles the data and services. The cloud is particularly present at the data center or can be hosted by some third-party services [4]. Where as the hybrid cloud is a mix of a private cloud and public cloud services and a software to communicate between these individual services. Coming to the community cloud, the cloud infrastructure is pooled across a number of comparable companies. Because the expenditures are divided across the institutions, this may assist decrease the working capital expenses for its establishment. A third-party supplier or at one of the local firms might host the cloud platform [5-6].

Cloud services are divided into three categories: Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS). IaaS comprises the fundamental cloud IT building pieces. Typical networking characteristics, computers (virtual or real) and the storage capacity of data are available. The most flexible and controlled administration of resources is provided by IaaS [7].

The next stage is Platform-as-a-Service (PaaS) and the collection, network and virtual machines are underpinned This also contains equipment and techniques that developers must add to: middleware, database management, operating systems and development tools that may be used for developing apps [8]. Software as a service (SaaS) is the supply of cloud-based apps which are perhaps the most widely utilized kind of cloud-based computing on a daily basis. This is immaterial to the end user, who accesses the service through an app or a website [9].

B. Cloud cryptography

Cloud cryptography uses encryption techniques to safeguard the information that the cloud uses or saves in [10]. This technique allows to safeguard private data of the users without any delay in the

data exchange. Users can access the information safely and easily in the same way as they can access the unencrypted data before the encryption techniques have been applied [11].

It is an encoding technique that safeguards cloud-saved data. In exchange, it gives easy and safe access to the server by those having the cryptographic keys. Authentication is the fundamental rationale of this technique. This involves algorithms that are used to jumbled text into a mixed code, called ciphertext. The ciphertext can be decoded with a sequence of bits and converted to plaintext with the help of encryption key. Information at rest and information in transit are two forms of data that are secured via encryption [12].

Cloud cryptography uses encryption methods to link information which is used or stored in the cloud. It enables users to reach shared cloud administrations easily and securely, since encryption secures all data provided by the cloud providers. Cryptography is a technology which enables the client, with the support of codes, to protect information and its exchange. The advanced trading techniques employ cryptography to monitor the movement of resources, manage the production of additional units and trade of shields [13-15].

II. THREATS AND ISSUES IN CLOUD COMPUTING

The cloud computing has many benefits but with greater technology comes greater issues and so the cloud computing is associated with number of pitfalls. Cloud computing presents a variety of security problems. These challenges are- security problems encountered by cloud providers and also consumer's security problems [16-17]. In most circumstances, the supplier must provide safe architecture and safeguard consumer applications and data, whereas the user must maintain adequate security steps have been implemented by the supplier to protect their privacy. Some of the issues faced in cloud computing are:

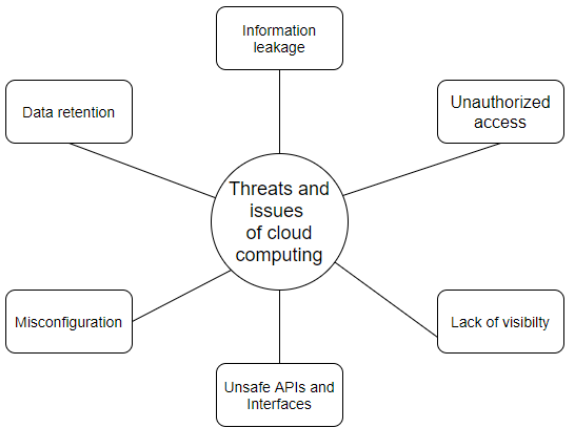

Fig 1. Cloud computing issues

A. Safety and unauthorized access

Neglect of personnel and unauthorized access by misuses of passwords of staff has become one of the major security dangers in cloud technology. The system might be made subject to several various attacks if modern staff check in to cloud platforms from their smart phones, laptop devices and personal computers.

Although this is a matter for on-site operations, Cloud computing also raises risks and security problems. Due to the type of cloud and the open Internet access to the technology, suspicious activities associated with malevolent insiders could be even more hard to identify. And a data violation might already be ongoing when any dangers are discovered. In order to identify suspicious insider behavior and limit vulnerabilities, organizations have to have appropriate safety measures in place prior business transactions have substantial effect [18].

B. Lack of visibility in cloud applications

The failure to see the public cloud leads to a threat to safety and may result in illegal access, inadequate management and the reproduction of private data from the cloud [19]. It can impede the organization's capacity to check the efficiency of its security checks. Implementing crisis management plans to identify odd patterns of usage that relate to safety (since they do not include full authority of cloud-based resources) and evaluate data, services and consumers. This is among the key issues to be addressed by a company [20-21].

Complete transparency in the cloud architecture is crucial for organizations. Cloud services are able to deliver business people, among some other groups, to enable fast detection and reaction to a risk in actual environments, reporting on networks and user activities [22].

C. Misconfiguration

Cloud computing misconfiguration is a largest source of data violations. If the cloud infrastructure of a company is not correctly designed, important corporate data and apps might be attack-prone [23].

Since the cloud architecture is built for easy information and data transfer, enterprises might find it challenging to ensure that their information is available only to authenticated parties. This problem might be compounded since an architecture is neither seen or controlled inside its cloud hosting platform [24].

D. Unsafe APIs and interfaces

Application Programming Interfaces (APIs) empower clients to personalize their environment on their chosen cloud. API itself may, however, become a cloud safety hazard. It not only provides enterprises the opportunity to tailor their cloud solutions' functionality to specific business demands as well as provide information identification, accessibility and efficient data encryption. The APIs can serve developers diverse goals, but may also leave numerous useful safety hazards that lead to a threatened infrastructure [25-26].

E. Information leakage

The easy transfer of information and the potential to work smoothly amongst coworkers and even outside persons is one of the key advantages of cloud computing. Nevertheless, as cloud storage shares often occur by direct e-mail invites or through an open link to certain users, possible security threats and cloud services obstacles might arise.

If you are aware of the data kept inside your cloud, you can visit the open link – or change the configuration of a cloud-based content to "open". Moreover, hackers use tools to scan the web continuously to find examples such as insecure cloud deployments [27].

If these assets include sensitive organization firm data and are in the hands of the incorrect or illegal people, a possible major security breach may threaten an organization immediately and this might have an influence [28].

F. Data Retention

Data retention has long been an issue of company executives but is still far vital as the intricacy and complexity of the cybersecurity keeps expanding. There are presently several data confidentiality rules that have been designed to secure consumer information, such as the EU GDPR, HIPAA, PCI DSS, and others [29].

Failure of the companies to comply these rules may result in severe consequences, including substantial fines, or the worse, a information infringement [30]. The compliance load is shared by a controlled cloud server. To ensure the continuous security of the company and its clients, organizations should pick a partner experienced with data privacy and regulatory requirements [31].

Due to all these vulnerabilities in the cloud computing, it gives hackers various opportunities to get a breach into the system and access private data and services of the cloud of a private organization. Following are some of the methods through which hackers can gain access into the system [32-35].

A. Phishing and Social engineering Attacks

Because cloud technology is public, it is prone to assaults on phishing and social engineering. Upon receipt or even other private data, a hostile person can access a service quickly, as the platform may be accessed from everywhere. Staff must be informed of phishing & social engineering in order to prevent such assaults.[36-38]

B. Accounts Hijacking

Hacking has been increased by the advent of cloud technology. Hackers can access confidential information saved in the cloud using worker credentials offsite. Furthermore, assailants may misrepresent and change data using hijacked authorizations. Scripting mistakes and overused

passwords let hackers to grab accounts without us knowing include other different hijacking practices.

C. Distributed-Denial-of-Service(DDOS) Attacks

When cloud technology became initially popular, DDoS assaults were inconceivable. Cloud services make the initiation of DDoS assaults exceedingly hard. However, DDoS assaults have gotten far more feasible with far too many digital networks, such as mobile phones as well as other communications systems.[39-40]

D. Injection of Malware

Malware injection is generally performed utilizing certain cloud-based scripts that operate on cloud-controlled servers as SaaS. Furthermore the cloud starts to work together when malware is inserted or uploaded to the cloud platform. Using such flaws, attackers may remove crucial data or jeopardize the authenticity and steal the information. In addition, a massive safety risk in cloud environment has been the attack by malware injection.This work, we have not to train a Bayesian network; however, a basic diagram is introduced that can be utilized for the prediction model.[40-42]

III. NEED FOR CLOUD SECURITY

Security in the cloud is crucial because most firms now use some sort of cloud technology. However, as corporations go farther data and cloud apps, IT experts stay worried about safety, management and governance when the company's material is kept on the cloud. Users are concerned that extremely private corporate data and intellectual property might be vulnerable to unintentional leaks or to ever more elaborate cyber attacks.

A key element of cloud security is analysis and business material protection, including client orders, confidential design papers and financial information. To maintain oneself, avoiding leaks and data breaches is vital.

The maintenance of a robust cloud security posture will enable enterprises realize the already generally acknowledged advantages of Cloud Computing- decreased upfront expenses, reduction in continuing operational expenses as well as the managerial costs.

The primary goal is to safeguard and preserve private data, when it is sent via the Web as well as other communications systems and for this Cloud cryptography is required. The greatest technique to assess the safety and confidentiality of an organization is by use of the CIA trinity. This refers to privacy, completeness and accessibility.

The discipline of IT puts an emphasis on the accessibility and consistency of the data. Sufficient attention is not given to the confidentiality of data . Therefore, any firm ought to adopt cloud cryptography.

In addition, encryption isn't only applied for data protection and privacy. In its essence, digital information is to be sent and encrypted through a secure method to send. Users want the guarantee that their information is protected when sent to a different source and that the sent person only needs to get the data and not to hostile invaders.

IV. TYPES OF DATA IN CLOUD COMPUTING

Cloud encryption is the method by which data can be encoded or transformed before it is sent to the cloud. Encryption employs data transformation by mathematical procedures (plaintext) and it converts data into unreadable (ciphertext) to hide text, file, program or picture from non-authorized and hostile users. This is the most easy and important approach to ensure that cloud information can not be broken, hijacked, or accessed by an abnormal person.

Providers of cloud storage encode information and transfer user encryption keys. These keys will be used when it is necessary to securely decode data. Decryption converts the hidden data to previous user sent data.

So it is important to know about the different types of data and as to know which data type is being used-

1. **Data at rest:**

   The data which is kept someplace and not transmitted to anybody else, including people, 3rd parties, programs, etc. It is possible to keep the data in some devices which are also easily available . This comprises servers for the database, system directories, smart phones, USBs, Network Attached Storage and local hard drives.

2. **Data in transit**

   The data which is sent from point to point is called data in transit. It is necessary to remember that the transmission of the data is not from the sender to recipient . For instance, the transmission of data with one lone party when we transmit any information from our computer or Laptop across our Network. Instead we carry out information exchange between unidentified entities when we have a transfer with a distributed database. This data is often called "in motion".

3. **Data in use/ provenance**

   This data is generally used when the data is not saved in an external storage or on a hard disk and when it is being handled by some application. In other words, it is being deleted, attached, changed, read or produced. In general, data in use is vulnerable to various types of risks and problems based on who may acquire it or where the network is situated. This type of data is challenging to encrypt since the program that has accessibility may crash.

   - Data quality: lineage may be applied on the basis of original data and modifications to evaluate data quality and accuracy. It can also offer evidence on the origin of data.
   - Audit trail: Data audition trail tracking, resource consumption detection and data creation mistake detection may take place using the provenance.
   - Informational : A lineage common usage is used to query information for data identification depending on lineage info. It is also possible to explore to create a framework for interpreting data.

4. **Data Lineage**

   As the phrase itself explains, the data lineage contains the data record and is preserved in data storage. By this, it is easy to track the changes to data in order to keep companies happy.

5. **Data remanence**

   Pushing a file into the garbage and then clearing the trash does not truly delete the item. It only tells the storage device that the item is removed, but the item data remains on the hard disc until the file system finally replaces the item. You must next follow a step in deleting the part of your disc, maybe by deliberately overwriting the original file, if you desire the real removal of deleted files. Due to the magnetic characteristics of the storage medium, it might be also feasible to recover fragments of the original file. This is known as data remanence.

V. CLOUD CRYPTOGRAPHY TECHNIQUES

Many cloud safety strategies employ different encryption mechanisms. For cloud security, cryptographic technology has become critical. Cryptography refers to the approach commonly utilized for the security of information and messages transmitted across the network in communications systems. The plain text messages are encoded in the form of "cipher text" and then transmitted through the network with a cryptographic technique. At the receiving end, the cypher text message will be decoded again with a decoding method in the original plain text. Thus, the information can only be read by the transmitter and recipient.

Below are some of the terms used and their meanings:

Plain-text : The original input text sent.
Cipher-text : The output after the application of encryption technique.
Encryption algorithm : Used by sender of the plaintext to convert it to cipher text.
Decryption algorithm : Used by receiver of the ciphertext to convert it back to plain text.
Key: A key is a number (or set of numbers) that the cipher, as an algorithm, operates on it.

1. **Private-Key or Symmetric Algorithms**
   - In this type of encryption, the sender and receiver of the data the data have a key which is always hidden from others.
   - For both encryption and data decoding, Symmetric methods employ one key.

- There is little computing power needed and the encryption functionality is really good.
- These systems give users with a two-way system and guarantee authenticity and authority until the user is able to interpret the key, the encoded data stored on cloud.
- Some examples of symmetric algorithms are DES, AES, 3DES.

  AES:

  - 128 bit block encryption
  - Takes plains text as input and has a secret key(128, 192, 256bits).
  - On implementing the algorithm ,cipher text comes as an output.
  - Decryption is done using the same key to get the plain text.

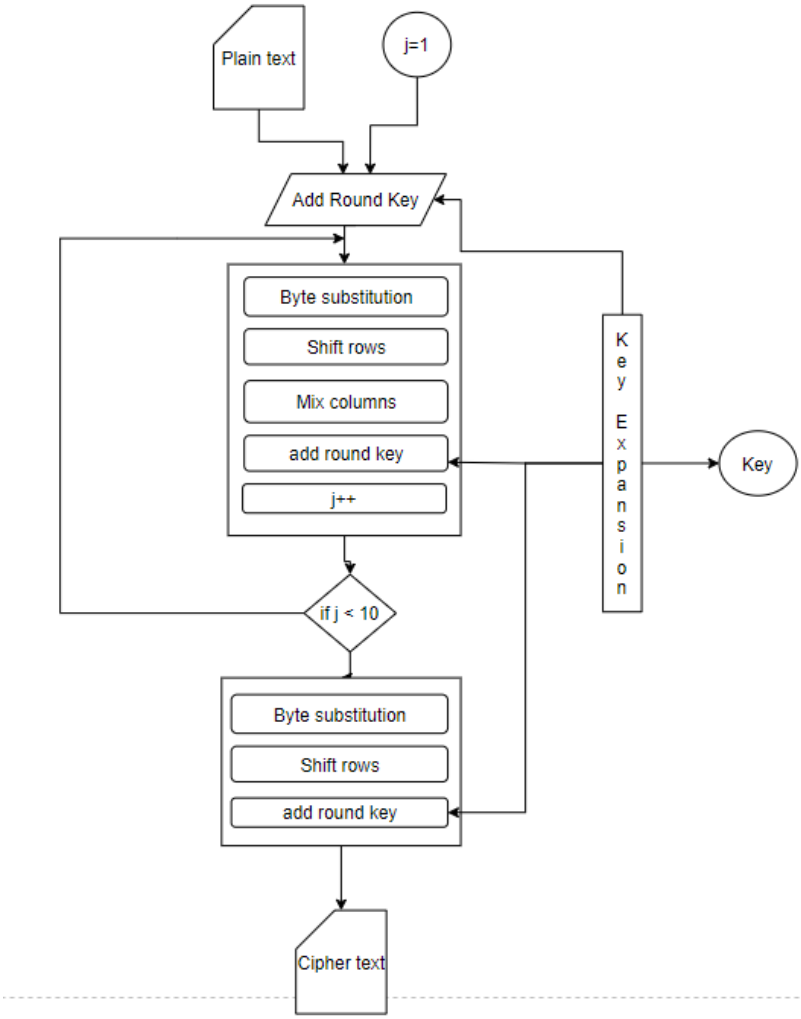

Fig 2. AES process(128-bit key)

DES:

- 64 bit block encryption
- Takes plains text as input and has a secret key(56 bits).
- On implementing the algorithm cipher text comes as an output.
- Decryption is done using the same key to get the plain text.

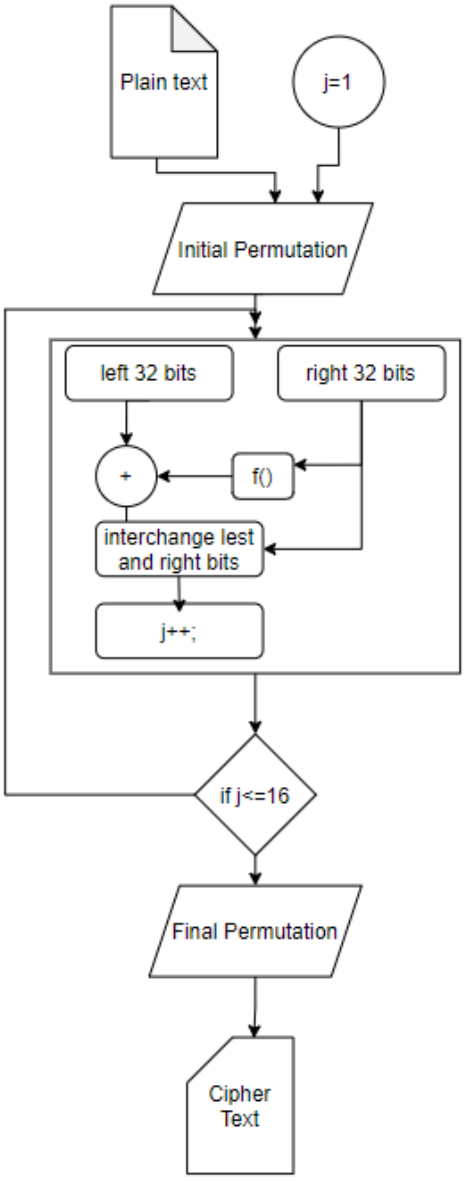

Fig 3. DES process

AES	DES
128- bit input	64-bit input
Allows 3 types of keys (128 / 192 / 256 bit key)	56 bit key
Number of rounds depends on key length 128 bits – 10 rounds 192 bits – 12 rounds 256 bits – 14 rounds	16 rounds
Operations – Byte substitution, Shift Row, Mix Column and Key Addition.	Operations - Expansion, XOR operation with round key, Substitution and Permutation.
Derived from Square cipher.	Derived from Lucifer cipher.
More secure	Less secure

Table 1. Comparison between AES & DES

Comparison between AES and DES :

- AES allows the user with 3 key length options i.e. 128 or 192 or 256 bits where as DES allows only one 56 bit key.

- The number of rounds of operations increases with increase in key length in AES but the number of rounds is fixed in DES.

- The operations in AES makes the encryption much stronger than that of DES and this makes the decryption harder for the person without the key.

- The initial and final permutation process in DES has no importance in cryptography as they both complement themselves.

- Conclusion : AES is more secure than DES and is used in a wide range if a proper key employment is done.

2. . Public-Key Or Asymmetric Algorithms

- This contains 2 keys, one public which is used for encryption and the other is private, used for decryption.
  - Some examples of symmetric algorithms are RSA, Diffie-hellman, ECC etc

RSA:

- Choose two distinct prime numbers p and q. Compute n = pq.
- Compute $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1) = n - (p + q - 1)$, where φ is Euler's totient function.
- Choose e such that $1<e<\varphi(n)$ and $\gcd(e, \varphi(n)) = 1$.
- Determine d as $d \equiv e^{-1} \pmod{\varphi(n)}$, d is kept as the private key.
- Encryption : c= m^e (mod n)
- Decryption : m= c^d (mod n)

Diffie-hellman:

- Alice and bob choose two same public keys(P,Q) and different private key each.(a),(b)
- They each generate key using
  x= Q^a (mod P)
  y= Q^b (mod P)
  and these are interchanged.
- They each generate secret key using the above shared keys
  ka= y^a (mod P)
  kb= x^b (mod P)

- Ka=kb, is the symmetric key to encrypt.

Comparison between RSA and Diffie-hellman :

- The process of the key exchange across Diffie- Hellman leaves it open to middle-man assaults, because it will not verify any of the interchange parties involved.

- Since the Diffie-Hellman Key Transfer doesn't verify a person, an attacker can send fake messages to any one of the sides.

- Therefore, in Diffie-Hellman, often digital signatures, is employed in conjunction with a further authentication mechanism.

- The RSA technique may not be used like Diffie-Hellman to sign digital signatures and symmetric key exchanges, but needs a public key transfer in advance.

- Also in the Diffie-Hellman technique, every side produces a public and private key but only the public key is communicated. Once the customer has validated the public key of the other individual, the exchange will be communicated on either end which is not the case in RSA.

- While both the Diffie-Hellman Key Exchange and RSA are the most used asymmetric encryption techniques, RSA is often more prominent for internet-based information securement.

Other encryption algorithms :

1. **Identity based encryption**

   - The knowledge of the user plays an important part in identity-based encryption (IBE).
   - In IBE, the user's public key is some unique user identify information. This enables any user to construct an ASCII text for a public key based on a known identification value.

- The matching private keys are created by a reliable 3rd party called the Private Key General (PKG).
- This encryption decreases both user and administrator's complexity of the encryption procedure.
- Email Encryption is one of the actual Identity Based Encryption applications.

2. Attribute Based Encryption

- It is the sort of encryption in which a control authority creates a user's private key (such as IBE), depending on each user's attributes/policy.
- Data owner employs a range of qualities to encode the data and the data may only be decrypted by authorized users that have or have expected attributes.
- This system of cryptography makes the cloud infrastructure more protected.

3. Homomorphic encryption

- A significant innovation in cryptography, known as homomorphic encryption, was made to keep the information encrypted but accessible at the very same time.
- The homomorphic encryption approach can do out operations without decoding on encrypted files.
- Homogeneous encryption methods are used to conduct encrypted information activities without revealing the private key, the user is really the only one person holding the private key.
- This can be broken down into 3 parts –
  - Integer division
  - Modular Arithmetic
  - Modulo 2 Arithmetic and Binary Operations
- Fully homomorphic encryption allows a person to calculate data results if he does not have a hidden decryption key.

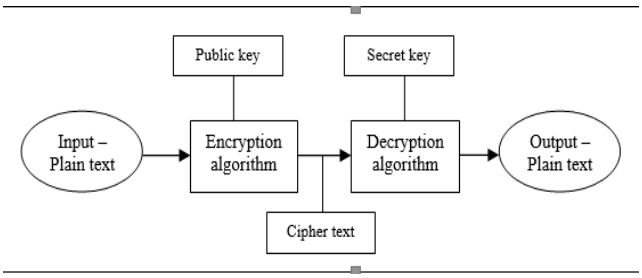

Fig 4. Cryptography process

Below are some on the ways in which data encryption can be done:

A. Full disk encryption :

That is the basic approach to protect machine's hard drives. It is instantly encrypted whenever an item is stored on an external disc.

B. End to end Encryption:

Senders and recipients transmit messages that are the only people who are able to read them. For instance, any chat platform uses end-to-end encryption.

C. File Encryption:

It is the process of data being encrypted at rest so that if an unauthorised person attempts to steal a file, he or she cannot obtain the data that the user has.

D. Pre-Encryption :

Before the data reaches the cloud, it can be pre-encrypted by software, which makes it difficult for anybody trying to access it.

VI. USES AND BENEFITS OF CLOUD CRYPTOGRAPHY

As the world is transitioning to a technological era, the data provided by business is becoming digitalized. In the cloud cryptography, certain procedures are designed to ensure that the data is not pirated, violated or impacted by virus, with a robust protective layer. Some of the benefits of cloud cryptography is:

1. **Privacy –**

   The data is always confidential to customers as the content is sensitive and decreases the risk of unlawful uses being fraudulent.

2. **Improved security of information –**

   When information is sent from device to device, data transmission is at stake and cryptography keeps the content from being susceptible.

3. **Users –**

   Because cloud cryptography is using stringent safety protocols, companies are promptly notified if an unauthorized party is trying to make modifications. The only persons who have secret key are able to view them.

Cloud cryptography's primary advantage would be the same in all encryption implementation: only authorized parties who have possession to the secret key may read cipher text. Encrypting information guarantees it stays safe, even if the information falls into the incorrect hands. This is particularly useful when data is kept in the cloud, which safeguards sensitive content mostly in case of a breach between a source, an account or a platform.

Encryption is not that complicated if performed correctly. Instead, encryption might be useful in order for any firm to be flexible, data protection and comply. Below are some of the benefits of the cloud cryptography:

1. **Data Security every instant**

   This happens when data is being encrypted before sending to the storage. This is a great option regardless of how the data is being used.

   Traditionally, when transmitted from elsewhere, data will be most fragile and feeble. During this procedure, encryption maintains security.

2. **Part of compliance**

Encryption is among the most reliable technologies for data sharing and storage as it meets the institution's limitations.
These guidelines include, among other things, FIPS, FISMA, HIPPA and PCI/DSS.

3. **Maintaining Integrity**

Hackers gain from changing information, not only stealing data, to conduct theft. You may update and manipulate encrypted message from these attackers. However, the data receivers are able to detect whether it is damaged, so that the assault is immediately answered and resolved.

4. **Privacy protection**

Confidential material, such as sensitive information of specific customers, are protected by encryption. This provides safety and confidentiality, reducing the odds of federal agencies, cybercriminals and hackers from monitoring.

5. **Safeguarding multiple systems**

A lot of types of communication gadgets are essential components of our life. Data transmission from machine to machine has a significant risk and susceptibility, which is why cryptography can assist to safeguard data across numerous systems.

VII. DRAWBACKS OF CLOUD CRYPTOGRAPHY

The cloud computing's safe information storage drawback may be resolved somewhat by using the cryptographic techniques to perform the information storage and access from cloud servers upon this source document. By employing the various encryption / decryption methods, cryptographic algorithms boost information confidentiality. Cloud computing is a rapidly increasing sector with the highest benefits, although cloud computing also has it’s inconvenience.

- The main drawback of cloud computing is that there is no standardization, i.e. only certain suppliers of cloud services provide edge encryption technology, not all servers offer end-to-end cryptography.

- Costs - The encryption of data may also be expensive, as modern systems must be managed and modified.

- Losing information by the cloud services when data is moving through one network infrastructure to the other network infrastructure leading to deterioration of data, i.e. cloud services cannot use an extra protocol stack while moving information about the users from one center to the next.

- Glitches - Every IT expert is well known that the information cannot be transferred from one server to some other, although it is safe. A system bug may still be available.

- The other main drawback of cloud computing is that data confidentiality and security are not easy to achieve, i.e. the current cloud servers don't really give privacy capabilities against suppliers of malevolent cloud services. Many unreliable cloud services steal users of their personal information that leads to data breaches and confidentiality issues.

- Recovery of data - It is always pleasant to have your data safeguarded. The recovery of information might pose problems to the company through overbearing procedures. So the greater number of keys we possess, the harder it is to get into your system to explain.

- The other main downside of the cloud system is that the user must simply believe the cloud platform suppliers; nevertheless, this can prevent the danger of cyber criminals, who are able to use web servers administrators effortlessly, i.e. any malicious attacker existing in the cloud platform supplier organization may have access to all the information that is available or saved or have accessibility to it.

- Key rotating and deletion can get more complicated whenever an enterprise manages its own keys, he observes. A 3rd party proxy source may provide a protective barrier by storing the keys apart from the ciphertext in a cloud platform, and this also brings further degree of meaning and added expenses to that organization from another source.

VIII. CONCLUSION

Cloud computing is very beneficial in its own ways but also comes with some issues and threats making it vulnerable. Cloud cryptography is used to overcome most of these threats and ensures that the data is stored inside the cloud safely. It encrypts the data to be stored using a suitable encryption algorithm according to the data and stores it into the cloud.

This paper discusses about the different cryptographic techniques for the encryption and decryption of the data in cloud. In symmetric algorithms, AES and DES have been described and compared. Data encrypted using the AES algorithm is observed to be more secured than that of DES because of the complexity and adjustable key size.

Where as in the asymmetric cryptographic techniques, both the discussed algorithms are used widely but RSA is comparably better than Diffie-hellman because it does not allow the chance of a man-in-the-middle(MITM) attack. Also Diffie-hellman needs an additional digital signature authentication to keep it safe.

Cloud cryptography has its pros as well as cons, the pros are providing data privacy, maintaining integrity and improving security and coming to the cons – being expensive, glitches, sharing a lot of keys, and recovery of the data might be hard. In the future, there is a scope of implementing more number of cryptography techniques which give more efficiency in the safe data storage and transmission.

REFERENCES

[1] Rachana, C.R., Banu, R., Ahammed, G.A. and Parameshachari, B.D., 2017, August. Cloud Computing–A Unified Approach for Surveillance Issues. In IOP Conference Series: Materials Science and Engineering (Vol. 225, No. 1, p. 012073). IOP Publishing.

[2] Kelsey Rauber, "Cloud Cryptography", Mathematics Department New York City College of Technology 300, Jay Street, Brooklyn, NY 11201, USA, 2013.

[3] Chakraborty, C., Roy, S., Sharma, S., Tran, T., Dwivedi, P. and Singha, M., 2021. IoT Based Wearable Healthcare System: Post COVID-19. The Impact of the COVID-19 Pandemic on Green Societiesenvironmental Sustainability, pp.305-321.

[4] Seyhan, K., Nguyen, T.N., Akleylek, S., Cengiz, K. and Islam, S.H., 2021. Bi-GISIS KE: Modified key exchange protocol with reusable keys for IoT security. Journal of Information Security and Applications, 58, p.102788.

[5] Hashem H. Ramadan, Moussa Adamou Djamilou, "Using Cryptography Algorithms to Secure Cloud Computing Data and Services", American Journal of Engineering Research (AJER), 2017.

[6] Fathima, N., Ahammed, A., Banu, R., Parameshachari, B.D. and Naik, N.M., 2017, December. Optimized neighbor discovery in Internet of Things (IoT). In 2017 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT) (pp. 1-5). IEEE.

[7] Naeem, M.A., Nguyen, T.N., Ali, R., Cengiz, K., Meng, Y. and Khurshaid, T., 2021. Hybrid Cache Management in IoT-based Named Data Networking. IEEE Internet of Things Journal.

[8]Deepanshi Nanda, Sonia Sharma, "Security in Cloud Computing using Cryptographic Techniques", IJCST Vol. 8, Issue 2, April - June 2017

[9] Isaac Kofi Nti , Ghana Eric Gyamfi, Marvin Appiah Osei, "Effective Cryptographic Technique for Securing Cloud Storage Systems", Foundation of Computer Science FCS, New York, USA Volume 12 – No. 4, July 2017

[10] Boregowda, S.B., Babu Prasad, N.V., Puttamadappa, C. and Mruthyunjaya, H.S., 2015. Energy Balanced Fixed Clustering protocol for Wireless Sensor Networks. International Journal of Computer Science and Network Security, 11(8), pp.166-172.

[11]Amandeep Verma and Sakshi Kaushal , "Cloud Computing Security Issues and Challenges: A Survey", U.I.E.T, Panjab University, Chandigarh, India, 2011.

[12] Sreevathsa, C.V., Daina, K.K., Hemalatha, K.L. and Manjula, K., 2016, July. Increasing the performance of the firewall by providing customized policies. In 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT) (pp. 561-564). IEEE.

[13] Priya Mathur, Prateek Vashistha, Amit Kumar Gupta , "Comparative Study of Cryptography for Cloud Computing for Data Security", computer science and engineering, Poornima Institute of Engineering & Technology Jaipur,India, 2019.

[14] Arun, M., Baraneetharan, E., Kanchana, A. and Prabu, S., 2020. Detection and monitoring of the asymptotic COVID-19 patients using IoT devices and sensors. International Journal of Pervasive Computing and Communications.

[15] Waseem Akram, "A study on Role and Applications of Cryptography Techniques in Cloud Computing (Cloud Cryptography)" , International Journal of Advanced Scientific Research and Management, Volume 4 Issue 1, Jan 2019.

[16] Nguyen, Tu N., Bing-Hong Liu, and Shih-Yuan Wang. "On new approaches of maximum weighted target coverage and sensor connectivity: Hardness and approximation." IEEE Transactions on Network Science and Engineering 7, no. 3 (2019): 1736-1751.

[17] Rajendrakumar, Shiny, and V. K. Parvati. "Automation of irrigation system through embedded computing technology." In Proceedings of the 3rd International Conference on Cryptography, Security and Privacy, pp. 289-293. 2019.

[18] Le, Ngoc Tuyen, Jing-Wein Wang, Duc Huy Le, Chih-Chiang Wang, and Tu N. Nguyen. "Fingerprint enhancement based on tensor of wavelet subbands for classification." IEEE Access 8 (2020): 6602-6615.

[19] Parameshachari, B. D., H. T. Panduranga, and Silvia liberata Ullo. "Analysis and computation of encryption technique to enhance security of medical images." In IOP Conference Series: Materials Science and Engineering, vol. 925, no. 1, p. 012028. IOP Publishing, 2020.

[20] Hemalatha, K. L., SUNILKUMAR MANVI, and HN SURESH. "ADAPTIVE WEIGHTED-COVARIANCE REGULARIZED KERNEL FUZZY C MEANS ALGORITHM FOR MEDICAL IMAGE SEGMENTATION." Journal of Theoretical & Applied Information Technology 95, no. 14 (2017).

[21] Bhuvaneswary, N., S. Prabu, K. Tamilselvan, and K. G. Parthiban. "Efficient Implementation of Multiply Accumulate Operation Unit Using an Interlaced Partition Multiplier." Journal of Computational and Theoretical Nanoscience 18, no. 4 (2021): 1321-1326.

[22] Lingappa, H., H. Suresh, and S. Manvi. "Medical image segmentation based on extreme learning machine algorithm in kernel fuzzy c-means using artificial bee colony method." Int. J. Intell. Eng. Syst 11 (2018): 128-136.

[23] Bhuvaneswary, N., S. Prabu, S. Karthikeyan, R. Kathirvel, and T. Saraswathi. "Low Power Reversible Parallel and Serial Binary Adder/Subtractor." Further Advances in Internet of Things in Biomedical and Cyber Physical Systems (2021): 151.

[24] Do, Dinh-Thuan, Tu Anh Le, Tu N. Nguyen, Xingwang Li, and Khaled M. Rabie. "Joint impacts of imperfect CSI and imperfect SIC in cognitive radio-assisted NOMA-V2X communications." IEEE Access 8 (2020): 128629-128645.

[25] Rajendran, Ganesh B., Uma M. Kumarasamy, Chiara Zarro, Parameshachari B. Divakarachari, and Silvia L. Ullo. "Land-use and land-cover classification using a human group-based particle swarm optimization algorithm with an LSTM Classifier on hybrid pre-processing remote-sensing images." Remote Sensing 12, no. 24 (2020): 4135.

[26] Bhuvaneswary, N., S. Prabu, K. Tamilselvan, and K. G. Parthiban. "Efficient Implementation of Multiply Accumulate Operation Unit Using an Interlaced Partition Multiplier." Journal of Computational and Theoretical Nanoscience 18, no. 4 (2021): 1321-1326.

[27] Parameshachari, B. D., Rashmi P. Kiran, P. Rashmi, M. C. Supriya, Rajashekarappa, and H. T. Panduranga. "Controlled partial image encryption based on LSIC and chaotic map." In ICCSP, pp. 60-63. 2019.

[28] Subramani, Prabu, Ganesh Babu Rajendran, Jewel Sengupta, Rocío Pérez de Prado, and Parameshachari Bidare Divakarachari. "A block bi-diagonalization-based pre-coding for indoor multiple-input-multiple-output-visible light communication system." Energies 13, no. 13 (2020): 3466.

[29] Nguyen, Ngoc-Tu, Bing-Hong Liu, Shao-I. Chu, and Hao-Zhe Weng. "Challenges, designs, and performances of a distributed algorithm for minimum-latency of data-aggregation in multi-channel WSNs." IEEE Transactions on Network and Service Management 16, no. 1 (2018): 192-205.

[30] Shahriar, Md Rakib, SM Nahian Al Sunny, Xiaoqing Liu, Ming C. Leu, Liwen Hu, and Ngoc-Tu Nguyen. "MTComm based virtualization and integration of physical machine operations with digital-twins in cyber-physical manufacturing cloud." In 2018 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), pp. 46-51. IEEE, 2018.

[31] Puttamadappa, C., and B. D. Parameshachari. "Demand side management of small scale loads in a smart grid using glow-worm swarm optimization technique." Microprocessors and Microsystems 71 (2019): 102886.

[32] Hu, Liwen, Ngoc-Tu Nguyen, Wenjin Tao, Ming C. Leu, Xiaoqing Frank Liu, Md Rakib Shahriar, and SM Nahian Al Sunny. "Modeling of cloud-based digital twins for smart manufacturing with MT connect." Procedia manufacturing 26 (2018): 1193-1203.

[33] Chakraborty, C., Roy, S., Sharma, S., Tran, T., Adhimoorthy, P., Rajagopalan, K. and Jebaranjitham, N., 2021. Impact of Biomedical Waste Management System on Infection Control in the Midst of COVID-19 Pandemic. The Impact of the COVID-19 Pandemic on Green Societiesenvironmental Sustainability, pp.235-262.

[34]K. Yu, L. Tan, S. Mumtaz, S. Al-Rubaye, A. Al-Dulaimi, A. K. Bashir, F. A. Khan, “Securing Critical Infrastructures: Deep Learning-based Threat Detection in the IIoT”, IEEE Communications Magazine, 2021.

[35] K. Yu, Z. Guo, Y. Shen, W. Wang, J. C. Lin, T. Sato, “Secure Artificial Intelligence of Things for Implicit Group Recommendations”, IEEE Internet of Things Journal, 2021, doi: 10.1109/JIOT.2021.3079574.

[36] H. Li, K. Yu, B. Liu, C. Feng, Z. Qin and G. Srivastava, "An Efficient Ciphertext-Policy Weighted Attribute-Based Encryption for the Internet of Health Things," IEEE Journal of Biomedical and Health Informatics, 2021, doi: 10.1109/JBHI.2021.3075995.

[37] K. Yu, L. Tan, M. Aloqaily, H. Yang, and Y. Jararweh, "Blockchain-Enhanced Data Sharing with Traceable and Direct Revocation in IIoT", IEEE Transactions on Industrial Informatics, doi: 10.1109/TII.2021.3049141.

[38] K. Yu, L. Lin, M. Alazab, L. Tan, B. Gu, "Deep Learning-Based Traffic Safety Solution for a Mixture of Autonomous and Manual Vehicles in a 5G-Enabled Intelligent Transportation System", IEEE Transactions on Intelligent Transportation Systems, doi: 10.1109/TITS.2020.3042504.

[39] K. Yu, M. Arifuzzaman, Z. Wen, D. Zhang and T. Sato, "A Key Management Scheme for Secure Communications of Information Centric Advanced Metering Infrastructure in Smart Grid," IEEE Transactions on Instrumentation and Measurement, vol. 64, no. 8, pp. 2072-2085, August 2015.

[40] Y. Gong, L. Zhang, R. Liu, K. Yu and G. Srivastava, "Nonlinear MIMO for Industrial Internet of Things in Cyber–Physical Systems," IEEE Transactions on Industrial Informatics, vol. 17, no. 8, pp. 5533-5541, Aug. 2021, doi: 10.1109/TII.2020.3024631.

[41] C. Feng, K. Yu, M. Aloqaily, M. Alazab, Z. Lv and S. Mumtaz, "Attribute-Based Encryption with Parallel Outsourced Decryption for Edge Intelligent IoV," IEEE Transactions on Vehicular Technology, vol. 69, no. 11, pp. 13784-13795, Nov. 2020, doi: 10.1109/TVT.2020.3027568.

[42] S. Chen, L. Zhang, Y. Tang, C. Shen, R. Kumar, K. Yu, U. Tariq, and A. K. Bashir, "Indoor Temperature Monitoring Using Wireless Sensor Networks: A SMAC Application in Smart Cities", Sustainable Cities and Society, vol. 61, p. 102333, July 2020.