I J R B A T, Issue (XI) Vol (II) May 2023 : 27-33
A Double-Blind Peer Reviewed & Refereed Journal
OPEN ACCESS
e-ISSN 2347 – 517X
Original Article
INTERNATIONAL JOURNAL OF RESEARCHES IN BIOSCIENCES, AGRICULTURE AND TECHNOLOGY
 www.ijrbat.in

SYMMETRIC ENCRYPTION: COUNTERING DATA PROTECTION AND DATA SECURITY IN CLOUD CRYPTOGRAPHY

Amruta J.Thakur[1] and R. N. Jugele[2]

[1,2]Department of Computer, Science,ScienceCollege, Nagpur
Corresponding Email: amrutajthakur@gmail.com, rn_jugele@yahoo.com

Communicated : 12.01.2023 | Revision : 16.02.2023 & 23.02.2023 Accepted : 22.03.2023 | Published : 30.05.2023

ABSTRACT:
Cloud computing has become the ideal way to deliver enterprise applications and the preferred solution for companies extending their infrastructure or launching new innovations. Data security is the most important aspects in cloud platform. Many researchers have addressed this issue by Cryptography with different encryption schemes that provides secure data sharing without delaying data transmission on cloud. Modern cryptography concerns itself with Confidentiality, Integrity, Non-repudiation and Authentication. Ensured cloud data protection is an important part of the cloud computing environment because customers often store sensitive information with cloud storage services but these are not secure services. So it remains a challenge to exchange data in a safe way while storing data from an unconfident cloud. This paper addresses the fundamentals of cloud cryptography that is the encryption of data stored in the cloud which adds a strong layer of protection and avoids a data breach, hacked or malware. Paper concludes by urging further study into the proposed cryptography algorithms to keep a balance between security and efficiency to reduce cybercrimes.

Keywords :- Cryptography, cloud computing, encryption, decryption, data security, data transmission, cybercrimes.

INTRODUCTION :

Cloud computing is the delivery of computing services including servers, storage, databases, networking, software, analytics, and intelligence over the Internet ("the cloud") to offer faster innovation, flexible resources, and economies of scale. Most cloud computing services fall into four broad categories: infrastructure as a service (IaaS), platform as a service (PaaS), server less and software as a service (SaaS). These are sometimes called the cloud computing stack because they build on top of one another. Knowing what they are and how they are different makes it easier to accomplish your business goals.

The main concern in the cloud computing industry is security. Countering data protection and data security in cloud is a major concern. Perhaps the most dangerous types of malware creators are the hackers and groups of hackers that create malicious software programs.

Cloud encryption is a simple yet effective method to prevent sensitive cloud data from being accessed in the event of a breach. Even if the data ends up being stolen; cybercriminals fail to read the content of the encrypted files. Many experts regard encryption as a successful and effective approach to robust data security [1].

Countering data protection and data security in cloud by cryptography

Data should always be protected, which means it has encryption and passwords in place to keep unwanted people from accessing the data. Unauthorized access is a security breach or data breach, whether the person who accesses it does anything with the information they find or not.Cloud storage solution providers encrypt information and pass the encryption keys to their client companies. When the data needs to be decrypted, these keys can be used to safely access the information and pass it along as required. Decryption keys transform the

http://doi.org/10.29369/ijrbat.2023.02.1.0006

encrypted data into readable form [2].Cryptography is the practice and study of techniques for secure communication in the presence of adversarial behavior. More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages. Cryptography is the technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix "crypt" means "hidden" and suffix graphy means "writing"[2]. Encryption is a process of encoding a message, Decryption is the reverse process. Encoding: the process of translating entire words or phrases to other words or phrases. Enciphering: translating letters or symbols individually encryption: the group term that covers both encoding and [1].Basic operations – plaintext to cipher text:

Encryption: C = E(P) – cipher text to plaintext:

Decryption: P = D(C) – requirement:

P = D(E(P))

P is for Plain text, C is for Cipher text.

Defining some terms used in Cryptography:

- Plaintext is the original intelligible source information or data that is input to algorithms.
- Cipher text is the scrambled message output as random stream of unintelligible data.
- Encryption Algorithm substitutes and performs permutations on plain text to cipher text.
- Decryption Algorithm is encryption run in reverse by taking the secret key and transforming the cipher text to produce the original plain text.
- Keys are used as input for encryption or decryption and determine the transformation.
- Sender and Recipients are persons who are communication and sharing the plain text[8].

Security and Privacy Algorithms

There are several data encryption algorithms available:

i) Triple DES

ii) Blowfish encryption algorithm

iii) Twofish encryption algorithm

iv) Advanced Encryption Standard (AES)

i) Triple Data Encryption Standard (TripleDES):

This form of data encryption algorithm applies block cipher algorithms thrice to all the data blocks individually.

The magnitude of the key is enlarged to provide extra protection by increasing the encryption ability.

Every individual block constitutes of 64 bit data. In this encryption algorithm, three keys are used where each key constitutes of 56 bits.

A total of three key permutations are provided under this standard:

Option a: the three keys are independent

Option b: keys 1 and 2 are independent

Option c: the three keys are similar

Most importantly, we call triple DES whose key length consists of (3*56 bits = 168 bits) whereas key security consists of (2*56 bits = 112 bits).

The substantially longer key length of this type of encryption algorithms overpowers other encryption techniques.

Nevertheless, after the development of the advanced encryption standard (AES), TripleDES has been rendered old-fashioned[3].

ii) Blowfish Encryption Algorithm:

Developed in 1993, the Blowfish encryption algorithm is an alternative for Data Encryption Standard (DES).

Before its creation, encryptions were performed by patents and intellectual properties of firms. The developer placed the protocol to the public to make it readily available for any interested user. Compared to DES, it is substantially faster and offers better encryption security[5]. It is an asymmetric type of encryption protocol uses a single key for both encryption and decryption. It

http://doi.org/10.29369/ijrbat.2023.02.1.0006

is a block cipher and its block size is 64 bit and the key size lies anywhere between 32 – 448 bits. It features 18 sub keys, sixteen rounds and has four S-boxes. Its protection capability has been examined and proved. Considering blowfish standard is regarded as a Feistel cipher, a single structure is used to encrypt and decrypt data provided that the reverse direction of the round keys is considered.

It is a significantly fast operation because it involves a relatively small number of rounds as well as its clarity of functionality.

Nevertheless, its key-scheduling consumes a lot of time, although it has an upper hand when it comes to protecting brute-force threats.

Also, its 64-bit block length (size) is rather small making it endangered by birthday attacks compared to AES whose block size is 128 bits and above.

iii) Twofish Encryption Algorithm:

This form of the encryption algorithm is a symmetric key block cipher which is characterized by 128 bit block size and whose key size can run up to 256 bits. This protocol uses one key for encryption and decryption. It is a fast and flexible standard for eight-bit and thirty two-bit CPUs, and small smart cards. The protocol works exemplarily in hardware and has numerous functionality commutations between the speed of encryption and the setup time making it distinctive amongst other protocols. The standard shares some features with its predecessor, blowfish Encryption Algorithm and AES. At one time, this encryption algorithm was a real contestant for the best encryption standard, but the present AES beat it out. This algorithm bears several peculiar characteristics that distinguish it from other standards. This cryptographic protocol applies substitution-boxes, S-boxes that are pre-computed and key-reliant. This implies that despite the provision of the S-box, it relies on the cipher key for the decryption of the encrypted data.

The significance of the S-box is to conceal the key connection with the cipher text. The Twofish encryption standard is accepted as a substantially secure alternative. Encryption protocols whose keys have 128 bits and above are regarded as safe from attacks: Twofish has a block size of 128 bits.

Twofish protocol comes with several options. To execute fast encryption, the key setup time can be made longer; this is done when the amount of data (plaintext) to be encrypted is relatively large.The encryption can be made slower by setting a shorter key setup time when short blocks with constantly alternating keys are to be encrypted. For some PC users, Twofish is regarded as the best AES protocol due to its peculiar amalgamation of design, resilience, and speed.

iv) Advanced Encryption Standard (AES):

AES is the most popular and broadly used symmetric encryption standard today. Due to the DES's small key size and low computing capability, a replacement was required which led to the development of AES. Compared with TripleDES, it has been proved to be more than six times faster.

Concerning cyber security, the AES acronym, in particular, keeps popping up on all computer screens as it is the world's most accepted encryption standard. It is seen while using messaging applications such as Signal and Whatsapp, computer platforms such as VeraCrypt and other technologies commonly used. The AES standard constitutes 3 block ciphers where each block cipher uses cryptographic keys to perform data encryption and decryption in a 128-bit block.

A single key is used for encryption and decryption thus both the sender and receiver have the same key. The sizes of the keys are considered adequate to secure the classified data to a satisfactory secret level[4].

http://doi.org/10.29369/ijrbat.2023.02.1.0006

Cryptography Goals

This section explains the five main goals behind using Cryptography.

Every security system must provide a bundle of security functions that can assure the secrecy of the system. These functions are usually referred to as the goals of the security system. These goals can be listed under the following five main categories [12].

Authentication: This means that before sending and receiving data using the system, the receiver and sender identity should be verified.

Secrecy or Confidentiality: Usually this function (feature) is how most people identify a secure system. It means that only the authenticated people are able to interpret the message (date) content and no one else.

Integrity: Integrity means that the content of the communicated data is assured to be free from any type of modification between the end points (sender and receiver). The basic form of integrity is packet check sum in IPv4 packets.

Non-Repudiation: This function implies that neither the sender nor the receiver can falsely deny that they have sent a certain message.

Service Reliability and Availability: Since secure systems usually get attacked by intruders, which may affect their availability and type of service to their users. Such systems should provide a way to grant their users the quality of service they expect.

Types of cybercrimes:

1) Hacking: It is an illegal practice by which a hacker breaches the computer's security system of someone for personal interest.

2) Unwarranted Mass-surveillance: Mass surveillance means surveillance of a substantial fraction of a group of people by the authority especially for the security purpose, but if someone does it for personal interest, it is considered as cybercrime.

3) Child Pornography: It is one of the most heinous crimes that is brazenly practiced across the world. Children are sexually abused and videos are being made and uploaded on the Internet.

4) Copyright Infringement: If someone infringes someone's protected copyright without permission and publishes that with his own name it is known as copyright infringement.

5) Money Laundering: Illegal possession of money by an individual or an organization is known as money laundering. It typically involves transfers of money through foreign banks and/or legitimate business. In other words, it is the practice of transforming illegitimately earned money into the legitimate financial system.

6) Cyber-Extortion: When a hacker hacks someone's email server or computer system and demands money to reinstate the system, it is known as cyber-extortion [7].

Cloud attack

Any cyber attack that targets off-site service platforms that offer storage, computing, or hosting services via their cloud infrastructure can be classified as a cloud cyber attack. This can include attacks on service platforms that utilise service delivery models like SaaS, IaaS, and PaaS. According to McAfee, data in the cloud may just be more vulnerable **than data on on-site servers. These Vulnerabilities are compounded by lapses across** both Cloud Service Providers (CSPs) and end-users.[7]

1) Misconfiguration: CSPs provide different tiers of service depending on how much control an organisation needs over their cloud deployment. These offerings include Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Organisations have to configure these deployments according to their requirements to ensure more robust cyber security. Unfortunately, most companies do not have an adequate cloud security posture to ensure the safety of these services, leading to vulnerabilities in deployment. According to IBM, mis configured servers are responsible for 86%

http://doi.org/10.29369/ijrbat.2023.02.1.0006

of compromised records. Knowledge of the specific deployment you're using will help you configure it according to your security needs with the security tools provided by CSPs [6].

2) Compromised user accounts. Weak password protocols are a leading cause of compromised user accounts. Many users who work with cloud services do not have strong password protection, as they either use weak passwords, reuse older passwords or don't change their passwords regularly .As cyber security professionals, we encourage users to change their passwords regularly, at least once every 60–90 days[6].

3) API vulnerability: CSPs provide application programming interfaces that allow users to interact and work with their cloud computing service. These APIs include extensive documentation to allow users to understand and use them effectively. This documentation, however, can be obtained by hackers too and can be used to exploit the APIs to gain access and exfiltrate sensitive data stored in the cloud. Also, any vulnerabilities in the integration and configuration of these APIs will leave a backdoor open for cyber criminals to exploit. Eliminating security oversights in the implementation and configuration of APIs can be done by sticking to the documentation. Organisations also need to strictly monitor the functioning of the API's to identify any vulnerabilities.

Malicious insider activity: Even if organizations implement the most secure cyber ecosystem, a malicious user can negate these security protocols and leak critical information. The activities of malicious insiders are often hard to detect as they might already have access to critical information.In fact, over the last few years, the number of security breaches as a result of insider threats has seen a sharp upturn.To negate insider threats, organisations can implement stringent access controls to limit the amount of information accessed by individuals inside your organisation.Prevent cloud cyber attacks by implementing powerful cloud security measuresEvery day, a greater number of organisations adopt cloud services to facilitate their move to a remote work environment and increase collaboration between global team members.As adoption increases, so do the vulnerabilities. By understanding cloud security basics and some of the most common vulnerabilities that occur therein, we can limit our risk of becoming a target of cloud cyber attacks[7].

Study to find proposed algorithm:

The study of proposed algorithm is for encrypting data at the client-side before transmitting it for storage in the cloud environment. Plain text is converted into cipher text that prevent from cybercrimes [11].

1. Convert the character to its ASCII code
2. Convert the ASCII code to its equivalent 8-bit binary number. If it is not equal to 8 bits, add preceding 0s.
3. Find the 1s complement of the last 4 bits.
4. Convert the generated binary code to an ASCII character and transmit it to the cloud.

[13]The original character or plaintext is the character that matches the ASCII code generated. Balancing the security of the proposed algorithm with usability, efficiency and testing its compatibility with the various cloud platforms is the concern with above algorithms. In recent years, the number of attacks on these platforms has increased rapidly. Incidentally, cloud cyber attacks accounted for 20% of all cyber attacks in 2020, making cloud computing platforms the third most-targeted cyber environment[10].

CONCLUSION:

In this paper, various cryptographic algorithms used in cloud computing were discussed. TripleDES applies block cipher algorithms thrice to all the data blocks individually. The Blowfish

http://doi.org/10.29369/ijrbat.2023.02.1.0006

encryption algorithm is an alternative for Data Encryption Standard (DES) It is a block cipher and its block size is 64 bit and the key size lies anywhere between 32 – 448 bits. **Twofish Encryption Algorithm** is the form of the encryption algorithm, it is a symmetric key block cipher which is characterized by 128-bit block size and whose key size can run up to 256 bits. The AES standard constitutes 3 block ciphers where each block cipher uses cryptographic keys to perform data encryption and decryption in a 128-bit block. Technology experts have unveiled numerous forms of securing data transfer, but data encryption is the commonest and easiest method that every PC user should be aware of and able to use. By encryption, the data is "scrambled" such that an unintended person cannot read it. When the algorithms are used for transfers, the information is initially transformed into an unreadable cipher text and sent in this format, upon which the receiver uses a secret key or a password to decode the cipher text into its initial format. The paper concludes by urging further study into the proposed cryptography algorithms to keep a balance between security and efficiency to reduce cybercrimes.

REFERENCES:

Daniel Slamanig, Stefan Rass -Cryptography for Security and Privacy in Cloud Computing (Information Security and Privacy)

Maryann Thomas, S. V. Athawale -Study of Cloud Computing Security Methods: Cryptography International Journal of Computer Science and Engineering.

https://www.baeldung.com/cs/des-vs-3des-vs-blowfish-vs-aes

Velte, T. A, Velte, T. J., Elsenpeter, R. Cloud Computing: A Practical Approach.

P Agarwal -Journal of Advanced Research in Computer,Cryptography Based Security

VJR Winkler -Securing the Cloud: Cloud computer Security techniques and tactics- 2011 - books

Cyber Chief Magazine, Cybersecurity 2020 Top Trends Shaping Management Priorities, Ed

Stallings, William. Cryptography and Network Security (6th Edition). Pearson, 2014

https://www.geeksforgeeks.org/an-overview-of-cloud-cryptography/

Google Platform Encryption Whitepaper. Encryption at Rest in Google Cloud Platform. Retrieved.

https://cloud.google.com/security/encryptionat-rest/default- encryption

https://www.triskelelabs.com/blog/cloud-cyber-attacks-the-latest-cloud-computing-security-issues#:~:text=Any%20cyber%20attack%20that%20targets,SaaS%2C%20IaaS%2C%20and%20PaaS.

https://www.cse.wustl.edu/~jain/cse567-06/ftp/encryption_perf/

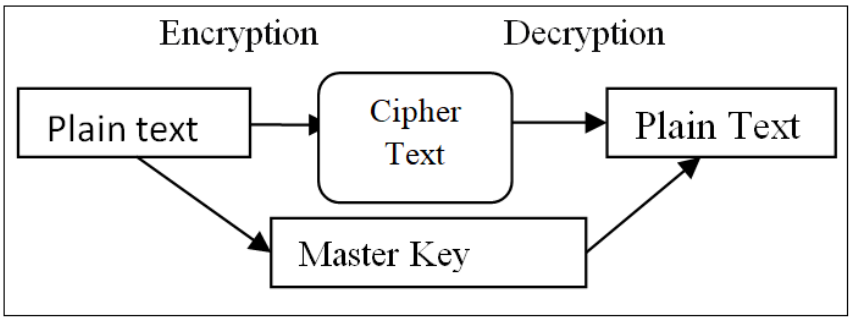
Felix Bentil,Department of Computer Applications, Lovely Professional University, LPU, Jalandhar, India, Cloud cryptography-A security Aspect.

http://doi.org/10.29369/ijrbat.2023.02.1.0006

Table-1: Symmetric encryption Protocol distribution

Algorithm	**Type**	**Method**	**Key Size**
3DES	Symmetric encryption	64-bit block cipher	56-, 112-, or 168-bit key
Blowfish	Symmetric encryption	64-bit block cipher	32-to 448 bit key
Twofish	Symmetric encryption	128-bit block cipher	128-, 192-, or 256-bit key
AES	Symmetric encryption	128-bit block cipher	128-bit block cipher

Fig1.Crypting Process



http://doi.org/10.29369/ijrbat.2023.02.1.0006