International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 10 Issue 5 ǁ 2022 ǁ PP. 40-46

Ensuring Data Protection Using Hybrid Cryptography

Riyas j[1]
Master of Science in Information Technology
School of CS & IT-Bangalore.

Dr. Suchithra[2]
Jain University- School of CS & IT.
Bangalore.

ABSTRACT
Security is an important factor to ensure that the client data is placed in a secure place. We need to keep information about every aspect of our lives. In other words, information is an asset that has a key value like any other asset. As an asset, information needs to be secured from attacks. To be secured, information needs to be hidden from unauthorized access (confidentiality), protected from unauthorized change (integrity), and available to an authorized entity when it is needed (availability). It helps business to improves their organization by using the services the cloud provider offers such as shared network, valuable resources bandwidth, software and hardware in a cost-effective manner. In digital world, security works in a similar way. One concept is privacy, meaning that no one can break into files to read your sensitive data.
In this project, we are focusing on what encryption a client needed before choosing a cloud provider, because good encryption will help you protect your data when you share it or use it, but if it is not considered before, the client will hand up losing data, paying more money to cloud provider, because the encryption offering by the cloud doesn't much with his need.
Keywords: *Confidentiality – Cryptography -RSA – AES- SECURITY.*

Date of Submission: 13-05-2022 Date of acceptance: 27-05-2022

I. INTRODUCTION:

The information collected by an organization was stored on physical files. The confidentiality of the files was achieved by restricting the access to a few authorized and trusted people in the organization. In the same way, only a few authorized people were allowed to change the contents of the files in the organization.

There are a lot of advantages of cloud but one of the biggest concerns with data storage in cloud are data confidentiality. To secure the data and what encryption to just to make their data confidential because their data are not control by them, they live it to a provider to secure it for them, so the importance of knowing the best encryption it is very crucial to make sure every data are protected.

Our project will focus on encryption such as symmetric and asymmetric, it will be better for a new customer or company who wants to explore the benefit of cloud, to know what encryption to use for his data, so before deciding on which cloud provider to choose it will be better to know the encryption needed for your data then compare to what cloud provider offer, we know that all the data are not confidential so the client or company have to know which encryption to use for each type of data.

For your secrets to be secure, it may be necessary to add precautions not provided by our OS. The built-in protections may be adequate in some cases. If no one ever tries to break into or steal data from a particular computer, its data will be safe. Or if the intruder has not learned how to get around the simple default mechanisms, they're sufficient. But many attackers do have the skills and resources to break various security systems.

If you decide to do nothing and hope that no skilled cracker targets your information, you may get lucky, and nothing bad will happen. But most people aren't willing to take the risk. We are to compare two encryption methods; symmetric (AES) and asymmetric (RSA) algorithms. In addition to keep secrets, cryptography can add security to the process of authenticating people's identity. Because the password method used in almost all commercial operating systems is probably not very strong against a sophisticated attacker. It's important to add protection. The cryptographic techniques for providing data secrecy can be adapted to create strong digital identities. Cryptography is by no means the only tool needed to ensure data security, nor will it solve all security problems.

It is one instrument among many. Moreover, cryptography is not foolproof. All crypto can be broken, and more importantly, if it's implemented incorrectly, it adds no real security. It is found that the encryption needed will depend on the confidentiality of your data, if the data confidentiality is high as you will need a strong encryption such as RSA, if not you will need DES as encryption, so analyzing your data confidentiality is very important before deciding on which encryption to implement.

II. CRYPTOGRAPHY

Cryptography converts readable data to gibberish, with the ability to recovery the original data from that gibberish.

To get encrypted gibberish, sensitive data and a secret number is fed to the encryption machine. To recover the file the switch is flipped to 'decrypt'. In order to achieve this, encryption algorithms are used.

EX: Symmetric key, RSA Algorithm

Decryption is often categorized alongside encryption on the contrary decryption results from the encrypted data of the original data.

Data Confidentiality, Data Integrity, authentication and non - repudiation are core principles of cryptography.

a) **Data Confidentiality**:

Designed to protect data from disclosure attack. The service as defined by X.800 is very broad and encompasses confidentiality of the whole message or part of a message.

b) **Data integrity**:

Designed to protect data from modification, insertion, deletion and replaying by an adversary and refers to maintaining and making sure that the data stays accurate and consistent over its entire life cycle.

c) **Authentication**:

This service provides the authentication of the party at the other end of the line.

d) **Non-repudiation**:

Protects against repudiation by either the sender or the receiver of the data.

HYBRID CRYPTOGRAPHY:

In cryptography, a hybrid cryptosystem is one which combines the convenience of a public-key cryptosystem with the efficiency of a symmetric-key cryptosystem.

Public-key cryptosystems are convenient in that they do not require the sender and receiver to share a common secret in order to communicate securely (among other useful properties).

However, they often rely on complicated mathematical computations and are thus generally much more inefficient than comparable symmetric-key cryptosystem.

In many applications, the high cost of encrypting long messages in a public-key cryptosystem can be prohibitive. This is addressed by hybrid systems by using a combination of both.

DATA SECURITY

Data security is the practice of protecting digital information from unauthorized access, corruption, or theft throughout its entire lifecycle.

It's a concept that encompasses every aspect of information security from the physical security of hardware and storage devices to administrative and access controls, as well as the logical security of software applications. It also includes organizational policies and procedures.

When properly implemented, robust data security strategies will protect an organization's information assets against cybercriminal activities, but they also guard against insider threats and human error, which remains among the leading causes of data breaches today.

Data security involves deploying tools and technologies that enhance the organization's visibility into where its critical data resides and how it is used.

Ideally, these tools should be able to apply protections like encryption, data masking, and redaction of sensitive files, and should automate reporting to streamline audits and adhering to regulatory requirements.

III. SECURITY GOALS

CONFIDENTIALITY

Confidentiality is probably the most common aspect of information security. We need to protect our confidential information. An organization needs to guard against those malicious actions that endanger the confidentiality of its information.

In military, concealment of sensitive information is the major concern. In industry, hiding some information from competitors is crucial to the operation of the organization. In banking, customers' accounts need to be kept secret.Confidentiality not only applies to the storage of the information, it also applies to the

storage of the information, it also applies to the transmission of information. When we send a piece of information to be stored in a remote computer or when we retrieve a piece of information from a remote computer, we need to conceal it during transmission.

INTEGRITY

Information needs to be changed constantly. In a bank, when a customer deposits or withdraws money, the balance of her account needs to be changed.

Integrity means that changes need to be done only by authorized entities and through authorized mechanisms.

Integrity violation is not necessary the result of a malicious act; an interruption in the system, such as a power surge, may also create unwanted changes in some information.

AVAILABILITY

The third component of information security is availability. The information created and stored by an organization needs to be available to authorized entities.

Information is useless if it is not available. Information needs to be constantly changed, which means it must be accessible to authorized entities.

IV. CRYPTOGRAPHIC ATTACKS

Cryptographic attacks can be categorized into two distinct types:

1) Cryptanalytic and
2) Non-cryptanalytic.

CRYPTANALYTIC ATTACK:

These attacks are combinations of statistical and algebraic techniques aimed at ascertaining the secret key of cipher. These methods inspect the mathematical properties of the cryptographic algorithms and aims at finding distinguishers of the output distribution of cryptographic algorithms from uniform distributions.

Ideally, all cryptographic algorithms act upon the message distribution and converts it using the key to a ciphertext distribution which looks random.

The objective of cryptanalysis is to find properties of the cipher which does not exist in a random function.

NON-CRYPTANALYTIC ATTACKS

The other types of attacks are non-cryptanalytic attacks, which do not exploit the mathematical weakness of the cryptographic algorithm. However, the three goals of security, namely confidentiality, integrity, and availability can be very much threatened by this class of attacks.

Our three goals of security can be threatened by security attacks. Although the literature uses different approaches to categorizing the attacks.

V. TYPES OF DATA SECURITY

ENCRYTPTION

Using an algorithm to transform normal text characters into an unreadable format, encryption keys scramble data so that only authorized users can read it.

File and database encryption solutions serve as a final line of defense for sensitive volumes by obscuring their contents through encryption.

Most solutions also include security key management capabilities.

Encryption is the principal application of cryptography; it makes data incomprehensible in order to ensure its confidentiality.

Encryption uses an algorithm called a cipher and a secret value called the key; if you don't know the secret key, you can't decrypt, nor can you learn any bit of information on the encrypted message—and neither can any attacker.

There are two types:

1)Public key (Asymmetric) - It is just like your bank account number. You can share this with anyone.

2) Private key (Symmetric)- It is like our ATM PIN. That we should not share this with anyone.

SYMMETRIC ENCRYPTION

Symmetrical encryption is a type of encryption that is used for encryption and decryption of electronic data by just one key (a secret key). Substitution ciphers are symmetrical encryption techniques, but modern symmetric encryption can be much more complicated.

Data are converted to a method that anyone cannot understand without a secret key to decrypt it using symmetrical encryption algorithms.Symmetric encryption is an old algorithm, but it is faster and efficient than

asymmetric encryption. Because of great performance and fast speed of symmetric as compare to asymmetric encryption.
Whereas Symmetric key cryptography involves the usage of the same key for encryption and decryption. At the same time, Asymmetric key cryptography involves using one key for encryption and another different key for decryption.Symmetric encryption is typical for big quantities of information.
EXAMPLE: for database encryption, in bulk encryption. In the case of a database, the secret key can only be encrypted or decrypted by the database itself.

ASYMMETRIC ENCRYPTION

This is based on substitution and premutation of symbols (characters or bits). asymmetric encryption is also called public-key cryptography. Asymmetric key encryption helps to resolve a key exchange problem of symmetric key Cryptography. In Asymmetric encryption, two keys are used to encrypt plain text in asymmetrical encryption.

It is based on applying mathematical functions to numbers. anyone who wishes to send you a message will have a public key freely accessible, but the second private key is held the secret for you to understand you only.

This uses two separate keys: one private and one public. If encryption and decryption are thought of as locking and unlocking padlocks with keys, then the padlock that is locked with a public key can be unlocked only with corresponding private key. A message encrypted with a public key can be decoded with a private key. A message encrypted with a private key can also be decrypted with a public key.

VI. ALGORITHMS:

ADVANCED STANDARD ENCRYPTION (AES)

The advanced encryption standard (AES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST) in December 2001.
The AES Encryption algorithm (also known as the Rijndael algorithm) is a symmetric block cipher algorithm with a block/chunk size of 128 bits. It converts these individual blocks using keys of 128, 192, and 256 bits. Once it encrypts these blocks, it joins them together to form the ciphertext.

CRITERIA

The criteria defined by NIST for selecting AES fall into three areas:
a) Security
b) Cost
c) Implementation
At the end, Rijndael was judged the best at meeting the combination of these criteria.

SECURITY

The main emphasis was on security. Because NIST explicitly demanded a 128-bit key, this criterion focused on resistance to cryptanalysis attacks other than brute-force attack.

COST

The second criterion was cost, which covers the computational efficiency and storage requirement for different implementation such as hardware, software, or smart cards.

IMPLEMENTATION

This criterion included the requirement that the algorithm must have flexibility and simplicity.

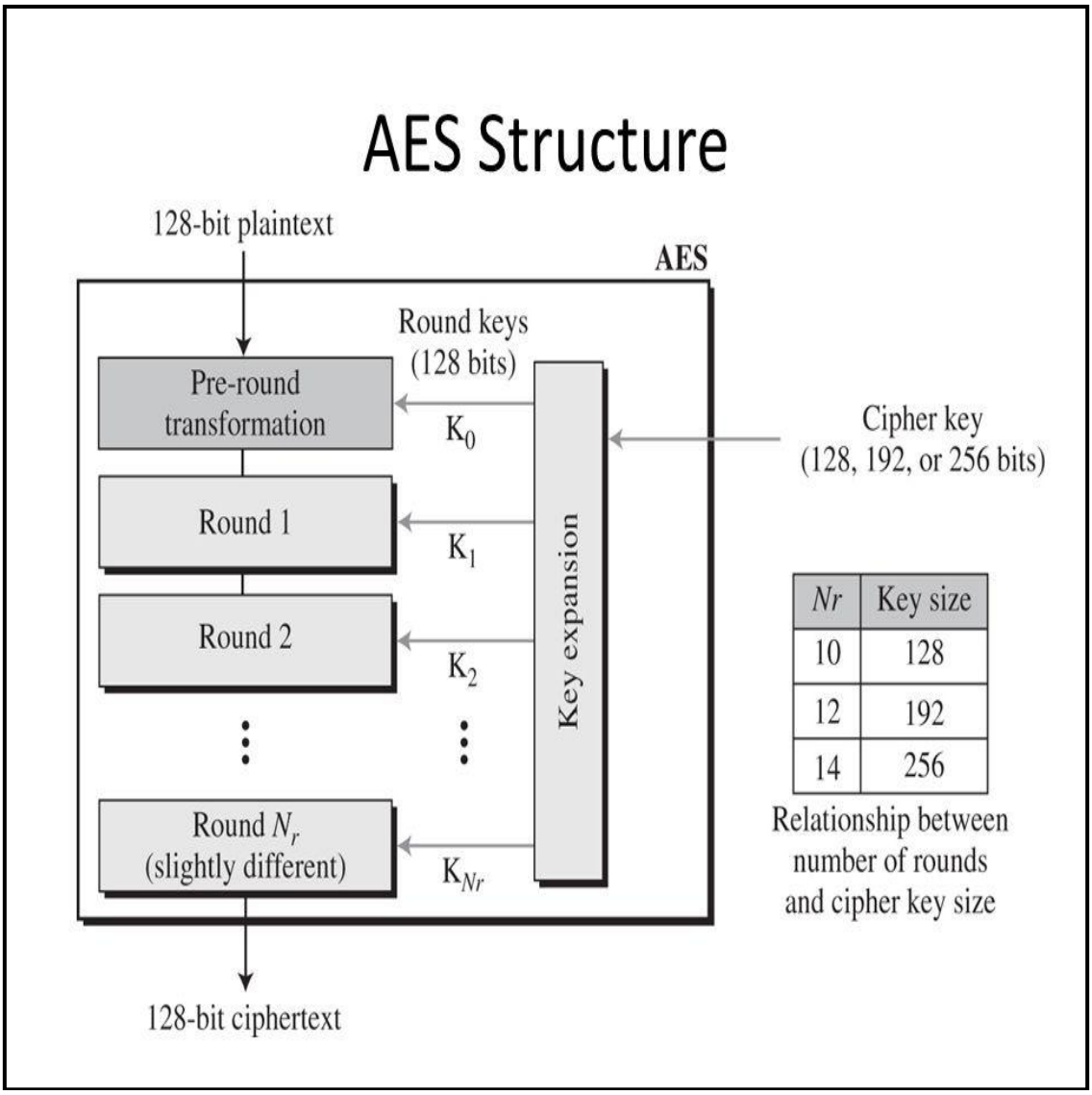

FIG: GENERAL DESIGN OF AES ENCRYPTION CIPHER

RIVEST, SHAMIR AND ADLEMAN (RSA)

RSA set of rules is asymmetric cryptography set of rules. Asymmetric surely approach that it works on unique keys i.e., Public Key and Private Key. As the call describes that the Public Key is given to each person and Private secret is kept private.

The RSA cryptosystem, named after its inventors Ron Rivest, Adi Shamir and Leonard Adleman, is the maximum well known and extensively used public-key cryptosystem in the international today.

For example, as one of the public-key cryptosystems used within the Transport Layer Security (TLS) protocol and its predecessor, the Secure Sockets Layer (SSL) protocol, the RSA cryptosystem is used thousands and thousands of times every day at the Internet. Essentially, RSA is used to transmit a session key for a symmetric cryptosystem that's then used to make certain the safety of a communique**.**

HYBRID ENCRYPTION:

The idea of hybrid encryption is quite simple. Instead of using AES to encrypt the text, we use AES to encrypt the message. Then, maintain the secret of the key, and we encrypt the key using RSA.

The steps of hybrid encryption are:

1.Generate a symmetric key. The symmetric key needs to be kept a secret.
2. Encrypt the data using the secret symmetric key.
3. The person to whom we wish to send a message will share the public key and keep the private key a secret.
4. Encrypt the symmetric key using the public key of the receiver.
5. Send the encrypted symmetric key to the receiver.
6. Send the encrypted message text.

7. The receiver decrypts the encrypted symmetric key using her private key and gets the symmetric key needed for decryption.
8. The receiver uses the decrypted symmetric key to decrypt the message, getting the original message.

```
**********************************************************************
**********************************************************************
Welcome...
We're going to encrypt and decrypt a message using AES and RSA
**********************************************************************
**********************************************************************
Genering RSA public and Privite keys......
Genering AES symmetric key......
Enter the message: Hello
Hello
Encrypting the message with AES......
Upload Done
Encrypting the AES symmetric key with RSA......
Mail Sent
```

```
Welcome to Sefy
# Press 1 to upload file
# Press 2 to download file
# other key to exit
1
Enter file name with path: (with \) C:\\Users\\KABIR\\Desktop\\projects\\sefy\\first.txt
Enter the bucket name: sefy0
Enter the object name: first.txt
**********************************************************
**********************************************************
Welcome...
We're going to encrypt and decrypt a message using AES and RSA
**********************************************************
**********************************************************
Genering RSA public and Privite keys......
Genering AES symmetric key......
Enter the message: hello bro
Encrypting the message with AES......
Upload Done
[50995, 49572, 40973, 16636, 52917, 7267, 13382, 7267, 49572, 16636, 7087, 16636, 16636, 50995, 49572, 4646, 52917, 5115, 7267, 4646, 40947, 42726, 40947, 4646, 13382, 38783, 49572, 50995, 50995,
 23920, 14801, 38783]
Encrypting the AES symmetric key with RSA......
Mail Sent
DONE!
```

```
Welcome...
We're going to encrypt and decrypt a message using AES and RSA
**********************************************************************
**********************************************************************
Enter the message: Hello
[5548, 12897, 5548, 5548, 9052, 9052, 10255, 3144, 1584, 7671, 12897, 7671, 23398, 55
48, 12897, 7671, 20191, 12897, 5548, 5548, 1209, 1209, 23398, 23398, 12897, 12537, 12
537, 5548, 3144, 13560, 7671, 1584]

Cipher Text:  b'\x8d\xa8P\xc3,'

AES Key:  [5548, 12897, 5548, 5548, 9052, 9052, 10255, 3144, 1584, 7671, 12897, 7671,
23398, 5548, 12897, 7671, 20191, 12897, 5548, 5548, 1209, 1209, 23398, 23398, 12897,
12537, 12537, 5548, 3144, 13560, 7671, 1584]

Private Key:  (457, 25159)



decrypted message:  Hello
```

FUTURE ENHANCEMENT

Data security is always been an important aspect of data. Here RSA and AES algorithm has been implemented for the data protection (Encryption and Decryption). In the future, to secure the data we can use algorithms like Two fish encryption algorithm and with the combination of Blowfish algorithm.

VII. CONCLUSION

The growing concern over the lack of data security in companies has found its way into a new product that provides the ability to delete data over the Internet. The crytography makes the data more secured in manner and confidentiality is high. Encoding critical information can make it unreadable and useless for malicious actors. Software-based data encryption is performed by a software solution to secure the digital data before it is written to the SSD. In hardware-based encryption, a separate processor is dedicated to encryption and decryption for safeguarding sensitive data on a portable device, such as a laptop or USB drive.

In today's technology-dependent world, data security is absolutely necessary. Improved data security methods are constantly being developed to protect important databases, and it's likely that data security will only rise in importance as our technology increases.

REFERENCES:

[1]. Mollin, R. , A. (2002). RSA and Public-Key Cryptography. CRC Press.
[2]. Hinek, M. , Jason. (2009). Cryptanalysis of RSA and Its Variants. CRC Press.
[3]. Stallings, W. (2006). Cryptography and Network Security. Prentice Hall.
[4]. Burnett, S., & Paine, S. (2001). RSA Security's Official Guide to Cryptography. McGraw Hill Professional.
[5]. Simrandeep Singh Thapar, Himali Sarangal, "A Study of Data Threats and the Role of Cryptography Algorithms" 2018 IEEE
[6]. Abdalbasit Mohammed Qadir, Nurhayat Varol," A Review Paper on Cryptography" 2019 IEEE
[7]. Mark A. Will, Ryan K. L. Ko," Anonymous Data Sharing Between Organisations with Elliptic Curve Cryptography" 2017 IEEE
[8]. Anuj Kumar, vinod Jain, Anupam Yadav," A New Approach for Security in Cloud Data Storage for IOT Applications Using Hybrid Cryptography Technique" 2020 IEEE
[9]. Marek R. Ogiela, Lidia Ogiela," Cognitive cryptography techniques for intelligent information management" 2018 Elsevier
[10]. Sattar B.Sadkhan, Akbal O. Salman," A Survey on Lightweight-Cryptography Status and Future Challenges" 2018 IEEE
[11]. Je SenTeh, MoatsumAlawida, You ChengSii," Implementation and practical problems of chaos-based cryptography" 2020 Elsevier
[12]. M Elhoseny, K Shankar, SK Lakshmanaprabu," Hybrid optimization with cryptography encryption for medical image security in Internet of Things" 2018 Springer
[13]. MS Taha, MSM Rahim, SA Lafta," Combination of steganography and cryptography: A short survey" 2019 IOPScience
[14]. S Padhye, RA Sahu, V Saraswat," Introduction to cryptography" 2018 TaylorFrancis.
[15]. S. Murphy, "The Advanced Encryption Standard (AES)," information Security Technical Report, Vol. 4, No. 4, PP.12-17, 1999.
[16]. I. A. Sada, "Hiding Data Using LSB-3", J.basrah researches (sciences), vol. 33. No. 4, pp. 81-88, Dec. 2007.
[17]. M. Juneja, and P. S. Sandhu, "Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption," International Conference on Advances in Recent Technologies in Communication and Computing, PP. 302-305, 2009.
[18]. Dutta et al, "New Data Hiding Algorithm in MATLAB using Encrypted secret message," International Conference on Communication Systems and Network Technologies, PP. 262-267, 2011.
[19]. W. Stallings, "Cryptography and Network Security Principles and Practices, Fourth Edition," Prentice Hall, PP.1-663 November 16, 2005.
[20]. R.O. El Safy, H. H. Zayed, and A. El Dessouki, "An adaptive steganography technique based on integer wavelet transform," ICNM International Conference on Networking and Media Convergence, PP. 111-117, (2009).