JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

IMAGE BASED INFORMATION SECURITY USING TRIPLE DATA ENCRYPTION STANDARD

Disha V Gowda[1], Vijayakumar A[2]

Final Year PG Student, School of CS & IT, Jain Deemed-to-be University, Bengaluru[1]

Professor, School of CS & IT, Jain Deemed-to-be University, Bengaluru[2]

Email: dishavasanthkumar@gmail.com[1], vijay.pattukkottai@gmail.com[2]

Abstract: In modern environment, almost all digital services, such as internet communication, medical and military imaging systems, and multimedia systems, require a high level of security and protection. In order to safely store and transmit digital images containing critical information, a high level of security is required. This is due to the rapid advancement of multimedia technology, the internet, and cell phones. As a result, image encryption techniques are required to protect images from such attacks. To hide the image in the system, we use Triple DES (Data Encryption Standard). This type of encryption technique helps prevent both active and passive attacks. It therefore has the advantage of proven reliability as well as a longer key length, which eliminates many shortcut attacks that can be used to reduce the time to crack DES.

Keywords: Decryption, Encryption, Keys, Path, Triple Des.

1. Introduction

Cryptography is the take a look at of steady communications strategies that permit simplest the sender and meant recipient of a message to view its contents. The time period is derived from the Greek phrase kryptos, this means that hidden. It is intently related to encryption, that is the act of scrambling everyday textual content into what`s called ciphertext after which again once more upon arrival. In addition, cryptography additionally covers the obfuscation of statistics in snap shots the use of strategies which include microdots or merging. When transmitting digital facts, the maximum not unusual place use of cryptography is to encrypt and decrypt e-mail and different plain-textual content messages. The best technique makes uses of the symmetric or "mystery key" system. Here, facts are encrypted the use of a mystery key, after which each the encoded message and mystery key are despatched to the recipient for decryption. The problem? If the message is intercepted, a 3rd birthday celebration has the whole lot they want to decrypt and examine the message. To deal with this issue, cryptologists devised the uneven or "public key" system. In this case, each person has keys: one public and one non-public. Senders request the general public key in their meant recipient, encrypt the message and ship it along. When the message arrives, simplest the recipient's non-public key will decode it — which means robbery is of little need without the corresponding non-public key.

Assuring and delivering 100 percent security is always tough to do. There will always be a flaw or vulnerability that needs to be fixed. It is possible, however, to make it harder for a hostile attacker. The scope of the project is to give the maximum security for the images using the encryption and decryption key between the user and the receiver. Securing through the Triple DES Algorithm. Helping to accessing their information/images with safe and secure. Triple DES is an encryption method that employs three DES instances on the same plaintext.

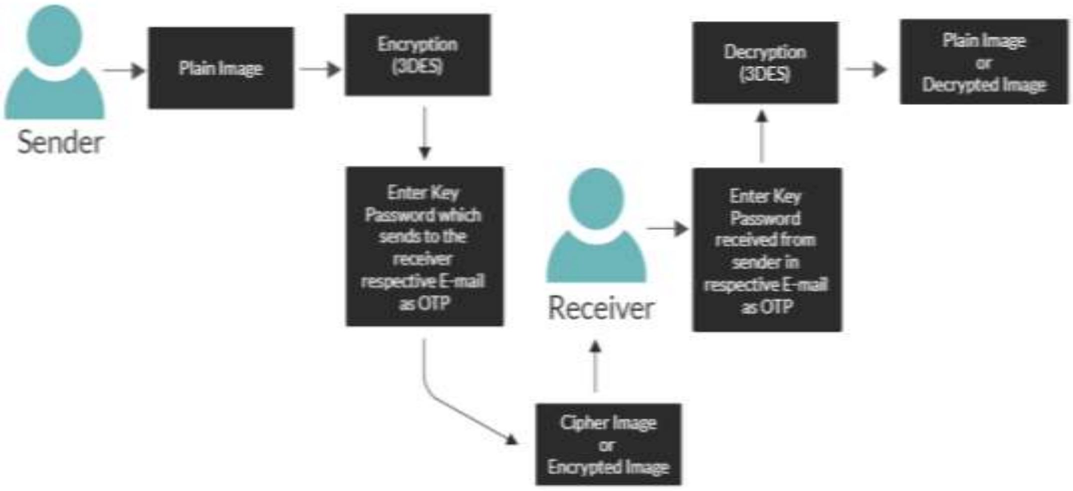
It employs a variety of key selection techniques: in the first, all keys are different, in the second, two keys are the same and one is different, and in the third, all keys are the same. The security partitions will be easily broken by unapproved people thanks to this rapid growth in technology. As a result, by leveraging private insurance to create a profitable and effective Data assurance.

The information and picture will be scrambled and converted into garbled data. Before encryption and after decoding, the standard sign will appear. If decoding an image with different permutations than those used for encryption is needed while keeping all other fixed parameters, such as 56 bits keys, the complexity is benefited, the original image is not obtained. This study does not provide formal evidence that more computing complexity is a good thing.

2. Related Work

The accompanying statistics and feedback reveal that Triple-Des grants a better-nice encryption method than des higher encryption and decryption overall performance method. Using a community to execute numerous approaches The second has arrived might be superior withinside the destiny for the Triple-DES method undertaking could additionally encompass a better stage of warranty for all forms of multimedia, nice and overall performance are difficult statistics. The latter could entail encrypting statistics with a cross-platform of video and audio files, diverse algorithms [3] this technique is handiest whilst implemented on the organisational stage. Because of the Triple DES method employed, even though the statistics is hacked, the hacker will now no longer be capable of get entry to the account. SFTP encrypts the record at some stage in transmission and decrypts the encrypted statistics on the receiving end. The cap potential to encrypt keys is one of the maximum crucial functions of SFTP. The record is encrypted the use of a non-public key at some stage in encrypted record switch. The SFTP generates the non-public key from the customer`s registration statistics. To decode the encrypted record, The key should be communicated via way of means of the sender to the recipient. As a result, the encrypted record is despatched at the side of the non-public key. Encryption is used right here to defend the non-public key. That is, a static software program key encrypts the non-public key. As a result, with this key, the recipient can speedily decrypt the contents. [7] all of it laboured and defined the statistics is encrypted into cypher textual content the use of the Triple DES technique. They should achieve a brand-new key from a permitted character who's locked in; in the event that they use an unauthorised key, they chance dropping all the hidden statistics. The AES set of rules and the chaotic series are used to encrypt and decrypt on this research. [11] makes use of a statistics encryption device produced with none extra analytical price to help industrial companies in deciding on the maximum reliable International Journal of Advanced Science and encryption algorithms for his or her enterprises. [12] it defined the way to enhance the Key Schedule Method, a completely unique FORTIS set of rules is proposed on this research. The identity of operations from the electricity hint have become extra hard with the creation of the Comparator and bendy shifter withinside the Key Schedule Algorithm, due to which the PGE values have been decreased and the set of rules become harmed.

3. PROPOSED SYSTEM


Sender
Plain Image
Encryption (3DES)
Enter Key Password which sends to the receiver respective E-mail as OTP
Cipher Image or Encrypted Image
Receiver
Enter Key Password received from sender in respective E-mail as OTP
Decryption (3DES)
Plain Image or Decrypted Image

4. Technical Background

4.1Cryptography

Cryptography is the process of altering messages so that their meaning is hidden from an enemy or opponent who may seize them. Cryptography is the science of secret writing that employs a variety of techniques to protect information that is stored in an unreadable format. This unreadable format can only be converted into a readable format by the designated recipients. Cryptographic techniques are used to secure E-mail messages, credit card information, audio/video broadcasting, storage media, and other sensitive information in secure electronic transactions. Using cryptographic systems, the sender can encrypt a message before sending it over the network. The receiver, on the other hand, has the ability to decrypt the message and restore its original content.

Components of Cryptography

- Plain Text

Plain text is an image that needs to be converted to text, binary code, or images that anyone needs to be converted to an easy-to-read form, except for those with a secret to unlock secrets. It refers to an unsent message or unencrypted message that the sender wants to send.

- Cipher Text

During the encryption process, plain text is rushed and converted to format and the result format is called cryptographic text. It is for encrypted messages and receives receiver. However, text is like plain text operated by the encryption process to reproduce the end output. However, this final output contains the original message of the format that the original message cannot be used unless the formal means knows that the code is not cracked.

- Encryption

Encryption takes information and converts it to unread format that can reverse it. It is the process of encrypting plain text to provide Cipher text. Encryption requires an algorithm called encryption and secret key. You cannot decrypt the most important information about encrypted messages without knowing the secret key. Clear text is converted to encryption of cryptographic text.

- Decryption

This is the inversion of the encryption process that restores the secret text to the plain text with the decryption algorithm and private key. In symmetric encryption, the key used for decryption is the same as the key used for encryption. On the other hand, asymmetric encryption or encryption, the key used for decryption is different from the key used for encryption.

- Keys

Encryption and decryption algorithms are known to each other as a diameter. Encryption and decryption algorithms require this key to encrypt or decrypt messages. The sender uses the encryption algorithm and the Secret key to convert plain text into encrypted text. On the other hand, the receiver uses the same decryption algorithm and private key to reinstall the ciphertext into plain text. The longer the secret key, the more difficult attackers can decrypt messages.

4.2 Methodology

- Secret (symmetric) key

The secret key cryptography, a single key is used for both encryption and decryption. The sender uses the key to encrypt the plaintext and send the ciphertext to the receiver. The receiver applies the exact key to decrypt the message and recover the plaintext. Since a single key is used for both functions, secret key cryptography is also known as symmetric encryption.

- Public Key

Public key cryptography has been considered the most important new development in cryptography in the last 300 to 400 years. Modern public key cryptography was publicly first described by Professor Martin Hellman and Stanford University graduate student Whitfield Diffie in 1976. The research describes a two-key encryption system in which Two parties can engage in secure communication over an insecure communication channel without having to sharing a key secrecy.

- Digital Password

Digital passwords are random strings used to restrict access to software by requiring users to provide authentication via secret passwords. Digital passwords are a form of authentication. The various authentication types include those digital users know (passwords, signatures, etc.), those digital users have (physical tokens, one-time passwords, etc.), and those digital users have (fingerprints, voiceprints, etc.) It is included. Biometric data). Digital security experts have criticized digital systems that rely on one-factor authentication. B. Only one digital password is required before granting a user access to a resource. Digital passwords are considered an effective digital security measure when required in combination with other authentication layers.

4.3 Significance

It is an integrated defence layer within all digital transformation initiatives, nowadays collectively referred to as the Digital Business. As the foundation of modern security systems, encryption is used to protect transactions and communications, protect personal information (PII) and other sensitive data, authenticate identities, prevent document tampering, and establish trust between servers increased. Cryptography is one of the most important tools companies use to protect systems that contain data, which is their most important asset, whether it is stationary or transferring. Data is important information in the form of customer PII, employee PII, intellectual property, business plans, and other sensitive information. Therefore, encryption is an important infrastructure as the security of sensitive data becomes increasingly dependent on the encryption solution.

Weak or ambiguous encryption can expose critical infrastructure to vulnerabilities. Public attention to published data leads to brand erosion. In this modern environment, organizations need to be aware of how encryption is implemented and managed throughout the enterprise. When embedded in the invisible layer of encryption, sensitive data cannot be read and modified, preventing malicious attackers from performing malicious activities.

4.4 Triple-DES Algorithm

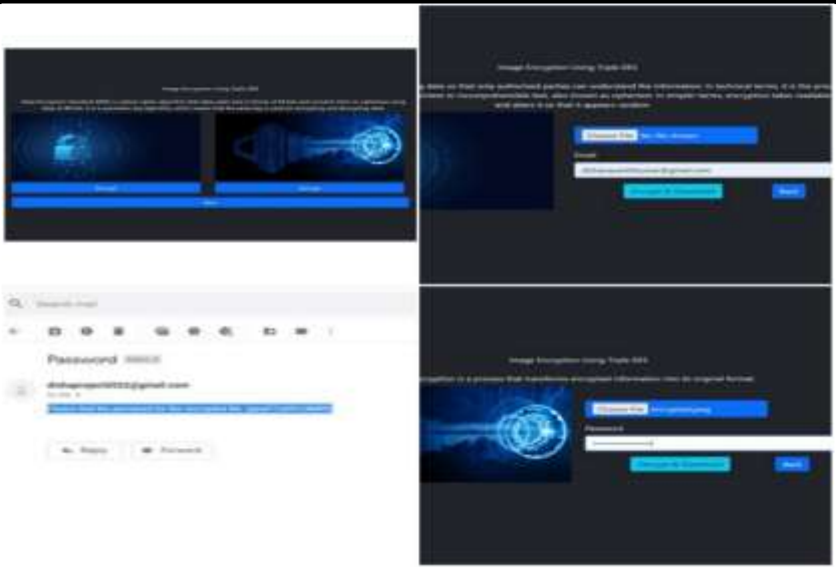
The method of encrypting a picture, text, or video utilising 56 bit two keys or 128-bit keys is known as Triple-DES. Although this method is secure, it is not without problems. To go around this problem, we used three 56-bit keys instead of two to encrypt our information. As a result, it is more secure. For the encryption process in the previously mentioned case study, just two keys were needed. This is followed by the triple-DES procedure. To perform the encryption procedure, the EDE model stipulates that each file or text must be encrypted twice and decrypted once in a sequential order.

It encrypts with one secret key, then decrypts with another secret key, and lastly encrypts with the same encrypt key.

We use three separate keys for each EDE process to circumvent this problem. EDE employs 192-bit keys, with only 168 bits used in the encryption process. Even if we don't use the last eight bits, this is still a highly strong algorithm. As a result, it's more secure over a network.

5. Results

As the DES algorithm, which was devised in the early 1970s, used a 56-bit key, 3DES was constructed. Due to meet-in-the-middle attacks, the effective security provided by 3DES is only 112 bits. Triple DES is three times slower than DES, but when implemented correctly, it is substantially more secure. The technique for decrypting anything is the same as the procedure for encrypting it, only it is carried out in the other direction. Data is encrypted and decrypted in 64-bit chunks with DES. The DES input key is 64 bits long, whereas the actual DES key is just 56 bits long.



6. Conclusion

The paper is being written in order to provide a project proposal on the triple Data Encryption standard for image encryption. The triple data encryption standard is an improved version of the data encryption standard that performs all decryption and encryption processes three times instead of only once. It has been determined that a significant number of resources will be necessary to continue with the experimental analysis and settings for implementing the triple Data Encryption standard. However, due to its linear cryptanalysis, the implementation of the triple Data Encryption standard technique may encounter difficulties.

7. Future enhancement

Because of the above research paper, it will be possible to view photographs that are encrypted so well that no one will be able to crack or decrypt them quickly in the future. Adaptation to other services such as Facebook and linkedin, among others More coverage and scalability. The project is created in a flexible way, more work can be done to improve the application in response to new modifications and versions. This can be done on the Internet by purchasing network space and setting up a website. When used on the internet, the current application necessitates the use of a huge database as a backend.

References

1. International journal of computer applications (0975 – 8887) volume 165 – no.8, may 2017 1 secure message transfer use triple des somya garg computer tarun garg bhawna mallick.
2. Imperial journal of interdisciplinary research (ijir) vol-3, issue-5, 2017 issn: 2454-1362, http://www.onlinejournal.in imperial journal of interdisciplinary research (ijir) page 969 image encryption using triple des algorithm anup r1 & suchithra r2

3. Journal for research| volume 02| issue 02 | april 2016 issn: 2395-7549 all rights reserved by www.journalforresearch.org 8 securing digital images using watermarking technique and triple des algorithm m.r.m veeramanickam varsha khenat, puja dhalpe navin dube.
4. International journal of scientific engineering and research (ijser) www.ijser.in issn (online): 2347-3878 volume 2 issue 11, november 2014 licensed under creative commons attribution cc by data encryption and decryption by using triple des and performance analysis of crypto system karthik. S, muruganandam. A
5. International journal of advanced science and technology vol. 29, no. 3, (2020), pp. 10549 – 10559 implementations of triple des algorithm in data hiding and image encryption techniques j. Guru mohish srivatsav, mrs. R. Sheeja
6. International mathematical forum, vol. 7, 2012, no. 59, 2929 - 2942 image encryption based on the modified tripledes cryptosystem v. M. Silva-garcía 1, r. Flores-carapia, i. López-yañez and c. Rentería-márquez
7. International journal of computer applications (0975 – 8887) volume 104 – no.2, october 2014 38 image encryption using simplified data encryption standard (s-des) sanjay kumar,sandeep Srivastava
8. International journal of advanced science and technology vol. 29, no. 3s, (2020), pp. 109-121 109 issn: 2005-4238 ijast copyright ⓒ 2020 sersc comparative analysis & implementation of image encryption & decryption for mobile cloud security ibraheem nadher ibraheem, saad mohsen hassan, suaad ali abead