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

A Survey: AN INFORMATION SECURITY USING SYMMETRIC KEY ALGORITHM

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

Final Year PG Student, School of Computer Science & Information Technology, Jain Deemed-to-be University, Bengaluru[1]
Professor, School of Computer Science & Information Technology, Jain Deemed-to-be University, Bengaluru[2]
Email: dishavasanthkumar@gmail.com[1], vijay.pattukkottai@gmail.com[2]

Abstract: Industries are increasingly dependent on dispersed systems and networks and communication facilities to transfer crucial and important information that must be kept safe. As a result, protecting corporate information becomes increasingly crucial, and maintaining information security is critical. Information security is described as ensuring the integrity, confidentiality, and availability of data and operating procedures by securing the information, the system, and the hardware that use, store, and transmit the information. In this paper, we show how numerous research have impacted information security in many sectors such as cyber security, Internet of Things, and network security, as well as the security requirements to mitigate this influence.

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

1. Introduction

The significance of data security has expanded because of the expanded usage of pcs and the web. Of course, there are presently a few diaries and countless yearly gatherings and studios committed to the security parts of data frameworks (is) and registering. These incorporate commitments by pc researchers, cryptologists, electrical and pc designs and is researchers. Notwithstanding, these givers regularly have altogether different perspectives on the key data security issues and their particular arrangements. Moreover, we see that researcher having a place with a specific discipline, for example, software engineering, cryptology, pc designing or is, frequently appear to have an unfortunate consciousness of the commitments made by specialists in different disciplines. This prompts fracture in the field of data security, which has two ramifications. To begin with, researchers in various disciplines might wind up attempting to waste time. Second, we can see that tending to security issues comprehensively requires interdisciplinary endeavours.

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 algorithm. Helping to accessing their information/images with safe and secure. Encryption method that employs 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. Before encryption and after decoding, the standard sign will appear. This study does not provide formal evidence that more computing complexity is a good thing.

2. Related Work

Anup and Suchitra,[2] have proposed the accompanying data and comments demonstrate that Triple-Des delivers a higher-quality encryption procedure than des better encryption and decryption performance process. When in a hurry, this becomes a major flaw. Using a network to execute several processes The moment has arrived will be enhanced in the future for the Triple-DES process task would also include a higher level of assurance for all sorts of multimedia, quality and performance are essential data. The latter would entail encrypting data with a cross-platform of video and audio files, various algorithms. Nandakumar Bhimnath et al. [3] has proposed that this method is most effective when applied at the organizational level. Because of the Triple DES approach employed, even if the data is hacked, the hacker will not be able to access the account. As a result, this tool is the best for security. To protect users of Gmail, Rapid Share, PayPal, eBay, and other services from being hacked. To prevent people from losing data on the internet. The use of two-factor authentication improves security. Murugan and Sriram V et al. [5] proposed Secure File Transfer Protocol (SFTP) is an intranet-based tool that allows for more secure file transfers. Encryption is performed by the software itself in this case. As a result, the client plays no part in encryption or decoding. SFTP encrypts the file during transmission and decrypts the encrypted data at the receiving end. The ability to encrypt keys is one of the most essential features of SFTP. The file is encrypted using a private key during encrypted file transfer. The SFTP generates the private key from the client's registration information. To decode the encrypted file, The key must be communicated by the sender to the recipient. As a result, the encrypted file is sent along with the private key. Encryption is used here to protect the private key. That is, a static software key encrypts the private key. As a result, with this key, the recipient can quickly decrypt the contents. As a result, the encrypted transfer is quicker than SSH FTP. To increase the security of a file, SFTP supports file locking and unlocking procedures. Cryptography is used to do this modification will not work on locked files. Screen sharing is yet another capability of SFTP. The term "screen share" refers to when two or more people share their screens remote systems. J. Guru Mohish Srivastava et al. [7] they all worked and explained the data is encrypted into cypher text using the Triple DES technique. They are given the data concealment key, which is used to disguise the data, and a new key is given to them as an image encryption key. One key is used to hide data, while the other is used to update the hidden information, and any new updated information is required to feature or delete some unnecessary information. If a person does not have the key or loses the key, they are unable to carry out any of the activities. They must obtain a new key from an authorized individual who is locked in; if they use an unauthorized key, they risk losing all of the hidden information. As a result, the information is preserved while converting them to photos, and they will be compressed to take up a little amount of storage space as new storage space is allocated to them because the data required a significant amount of space. The use of steganography techniques to disguise data with more security connections is more useful. V Goutham Bharadwaja et al. [10] proposed the AES algorithm and the chaotic sequence are used to encrypt and decrypt images in this research. The encryption and decryption processes are successfully implemented utilizing JAVA coding. To ensure the efficacy of the encryption method used, histogram analysis and adjacent pixel auto correlation are performed on the photos. As a result, the encryption approach can withstand a variety of attacks, including brute force, cypher, and plaintext attacks. Ibrahim Nadher et al. [11] their paper study uses a data encryption tool produced without any additional analytical expense to assist commercial organizations in selecting the most dependable International Journal of Advanced Science and encryption algorithms for their enterprises. Other parameters have been compared to each method.

Other algorithms are superior in terms of speed and power usage. Hackers won't be able to quickly break the Blowfish algorithm unless they figure out the appropriate combinations. Making accurate lock combinations is more difficult. The number of rounds has increased thanks to the algorithm. Encryption and decryption of images and videos requires less time. Akshitha Vuppala et al. [12] explained how to improve the Key Schedule Method, a unique FORTIS algorithm is proposed in this research. When compared to the present Triple-DES, the Verilog code was simulated and the Physical design was created using Cadence Design Suite, with the power and area having a negligible effect. The algorithm's power traces were acquired using ChipwhispererR -Lite (CW1173) using the CW-305 Artix-7 FPGA board as the target to determine the algorithm's strength. The identification of operations from the power trace became more difficult with the introduction of the Comparator and flexible shifter in the Key Schedule Algorithm, as a result of which the PGE values were reduced and the algorithm was harmed.

3. Analysis: Technical Preliminaries

3.1 Information Security

Information security refers to the methods and process used to secure confidential, private, and sensitive information or data in print, electronic, or any other form against unauthorized access, use, misuse, disclosure, destruction, modification, or disruption.

- Confidentiality - implies data isn't unveiled to unapproved people, substances and interaction. For instance, assuming that we say I have a secret key for my Gmail account however somebody saw while I was doing a login into Gmail account. All things considered my secret key has been compromised and Privacy has been penetrated.

- Integrity - implies keeping up with precision and fulfilment of information. This implies information can't be altered in an unapproved way. For instance, in the event that a representative leaves an association, all things considered information for that worker in all offices like records, ought to be refreshed to reflect status to Occupation LEFT so information is finished and exact and notwithstanding this main approved individual ought to be permitted to alter worker information.

- Availability - implies data should be accessible when required. For instance, in the event that one necessity to get to data of a specific worker to check whether representative has outstood the quantity of leaves, all things considered it requires joint effort from various authoritative groups like organization activities, advancement tasks, episode reaction and strategy/change the executives.

- Non-repudiation - implies one party can't deny getting a message or an exchange nor would the other party be able to deny communicating something specific or an exchange. For instance, in cryptography, it is adequate to show that message coordinates the computerized signature endorsed with source's private key and that shipper might have a communicated something specific and no other person might have modified it on the way. Information Uprightness and Realness are pre-requirements for Non renouncement.

- Authenticity - implies checking that clients are who they say they are and that each info showing up at objective is from a confided in source. This rule assuming adhered to ensures the substantial and real message got from a confided in source through a legitimate transmission. For instance, on the off chance that take above model shipper sends the message alongside advanced signature which was created utilizing the hash worth of message and private key. Presently at the collector side this computerized mark is decoded utilizing the public key creating a hash worth and message is again hashed to produce the hash esteem. On the off chance that the 2 worth matches, it is known as legitimate transmission with the true or we say certified message got at the beneficiary side.

- Accountability - implies that it should be feasible to follow activities of an element extraordinarily to that substance. For instance, as we talked about in Trustworthiness area Few out of every odd worker ought to be permitted to do changes in different representatives' information. For this there is a different office in an association that is liable for rolling out such improvements and when they get demand for a change then that letter should be endorsed by more significant position for instance Overseer of school and individual that is dispensed that change will actually want to do change in the wake of checking his profile measurements, hence timestamp with the user (doing changes) subtleties get recorded. Accordingly, we can say in the event that a change goes this way, it will be feasible to follow the activities remarkably to a substance.

Types of Security

Data Security isn't just about getting data from unapproved access. Data Security is essentially the act of forestalling unapproved access, use, exposure, interruption, change, assessment, recording or obliteration of data. Data can be physical or electronic one. Data can be whatever like Your subtleties or we can say your profile via web-based media, your information in cell phone, your biometrics and so forth Along these lines Data Security ranges so many examination regions like Cryptography, Portable Processing, Digital Legal sciences, Online Web-based Media and so forth.

3.1.1 Cloud Security

Cloud security protects cloud or cloud-connected data and information in the same way as application and infrastructure security does. Cloud security focuses on the risks that arise from Internet-facing services and shared settings, such as public clouds, by providing additional protections and solutions. Interaction with cloud providers or third-party services is another component of cloud security. Because the infrastructure is often controlled, are often unable to fully control environments while using cloud-hosted resources and apps. As a result, cloud security procedures must account for limited control and include safeguards to prevent access and vulnerabilities caused by contractors or vendors.

3.1.2 Cryptography

Encryption: The method of encoding information is known as encryption. This procedure converts plaintext, or the original file of the data, into ciphertext, or an alternative representation of the data. Only authorized users are able to convert a ciphertext back to plaintext and access the original data.

Decryption: Decryption is the process of restoring encrypted data to its original state. In most cases, it's a reversal of the encryption process. Because decryption requires a secret key or password, it decodes the encrypted information so that only an authorized user can decrypt the data.

3.1.3 Application Security

A significant portion of application security is based on specialized tools for application shielding, scanning, and testing. These tools can assist in identifying vulnerabilities in applications and their associated components. When vulnerabilities are discovered, they can be fixed before applications are released or vulnerabilities are exploited. Application security applies to both the applications used and those may develop, as both must be secure.

3.1.4 Infrastructure Security

Networks, servers, client devices, mobile devices, and data centers are among the infrastructure components that are protected by infrastructure security techniques. Without sufficient protections, the increased interconnectedness between these and other infrastructure components puts information at risk.

This risk arises from the fact that connectivity spreads vulnerabilities throughout the systems. If one component of infrastructure fails or is compromised, it affects all dependent components. As a result, minimizing dependencies and isolating components while still allowing intercommunications is an important goal of infrastructure security.

3.1.5 Disaster Recovery

Unexpected circumstances might cause the company to lose money or suffer damage, thus disaster recovery plans are essential. Ransomware, natural disasters, and single points of failure are some examples. The recovery of information, the restoration of systems, and the resuming of operations are all part of most disaster recovery plans. These measures are frequently included in a business continuity management (BCM) plan, which is aimed to help firms sustain operations with the least amount of downtime possible.

3.1.6 Incident Response

A combination of protocols and measures for identifying, investigating, and responding to threats or destructive occurrences is known as incident response. It prevents or minimizes system damage caused by attacks, natural disasters, system failures, or human mistake. Any harm to information, such as any damage or theft, is included in this damage.

An incident response plan is a regularly used tool for incident response (IRP). The duties and responsibilities for responding to occurrences are outlined in IRPs. These plans also help to define security strategy, give recommendations or procedures for action, and guarantee that incident information is used to improve security.

3.2 Vulnerabilities in Information Sharing

Vulnerabilities are flaws in a system that allow threats to gain access to valuable assets. There are flaws in every system. Even as technology advances, the number of vulnerabilities grows, such as tens of millions of lines of code, numerous developers, human flaws, and so on. Hardware, software, network, and procedural vulnerabilities were the most common causes of vulnerabilities.

Types of Vulnerabilities

3.2.1 Hardware Vulnerabilities

A hardware vulnerability is a flaw in a computer system that can be exploited by gaining remote or physical access to the system's hardware. It's a weakness in the system's operation that lets attackers to take control of the system by elevating privileges or running code. Instead of requiring physical access, these vulnerabilities can occasionally be exploited remotely. These are more commonly exploited in focused assaults on known high-value systems and organisations, rather than in random hacking attempts. Traditional malware prevention plus a locked door is sufficient for the majority of users.

3.2.2 Software Vulnerabilities

A software vulnerability is a flaw in software that allows an attacker to take control of a computer system. These flaws can be caused by a weakness in the way the software is designed or coded. It scans a system to see if it contains a software vulnerability. The scan can inform the attacker about the kinds of software installed on the system, whether it is updated, and whether any of the software packages are susceptible. When the attacker realises this, he or she will be better prepared to conduct attacks against the system. If the attack is successful, the attacker will be able to execute malicious commands on the target system. It can use a software flaw to steal or alter sensitive data, join a botnet, install a backdoor, or infect a system with additional malware. In addition, once an attacker has gained access to one network host, they can utilise that host to gain access to other hosts on the same network.

3.2.3 Network Vulnerabilities

Network vulnerabilities are continually changing, leading in the loss of important data and income for enterprises. Despite the fact that threat entities are always discovering new vulnerabilities, some of their tactics remain the same. Hackers have tried-and-true methods for breaking into what appears to be a secure network, and they use a variety of tricks, gadgets, and information to accomplish it. Some companies do not provide proper security for their network systems, either because their executives do not implement robust security policies or because they do not fully grasp how to safeguard their systems. Exploitable vulnerabilities and holes exist in all networks, but understanding how hackers exploit them provides businesses a better idea of what they need to do to prevent authorised people from accessing any important digital asset.

3.2.4 Procedural Vulnerabilities

Procedure vulnerabilities contribute to policy failure, and in Australian contexts, they raise the risk of conceiving climate change vulnerability solutions that involve moving people out of the way of environmental risks as they are conceived within colonial traditions, and into the way of risks as conceived through the eyes of remote Indigenous communities.[15]

3.3 Cryptography

The Block Cipher was the first of many cyphers used in cryptography. In comparison to modern cryptographic techniques, cyphers were much easier to decipher, although they both needed keys and plaintext. Crypts from the past were the first kinds of encryption, notwithstanding their simplicity. Algorithms and cryptosystems today are far more sophisticated. To provide the most secure data transit and storage, they use numerous rounds of cyphers and encrypt the ciphertext of communications. There are now ways of encryption that are irreversible, ensuring the message's security indefinitely.[16]

The requirement for data to be safeguarded more and more securely is driving the development of more complex cryptography solutions. The majority of cyphers and algorithms employed in the early days of cryptography have been cracked, rendering them ineffective for data security. Today's algorithms can be decrypted, but deciphering the meaning of a single message would take years, if not decades. As a result, the competition to develop newer, more powerful cryptography algorithms is still on.[16]

Types of Cryptography

3.3.1 Secret Key Cryptography

Secret key cryptography, also renowned as symmetric cryptography, encrypts data with a single key. Symmetric cryptography employs the same key for both encryption and decryption, making it the simplest type of cryptography. The cryptographic algorithm encrypts the data with the use of key in a cypher, and when the data has to be accessed again, only someone with the secret key may decrypt. Secret Key Cryptography can be used on both in-transit and at-rest data, but it is more usually used on the latter because disclosing the secret to the message's recipient can lead to compromise.

3.3.2 Public Key Cryptography

Asymmetric cryptography, often known as public key cryptography, encrypting data using two keys. One key is used to encrypt the message, while the other decrypt it. In contrast to symmetric cryptography, if one key is used to encrypt, the message cannot be decrypted with the same key; instead, the other key must be utilised. The private key cannot be deduced from the public key due to the mathematical relationship between the keys, while the public key can be derived from the private. The private key should not be shared and should only be kept by the owner. Any other entity can be granted the public key.

3.3.3 Hash Functions

Hash functions are one-way, irreversible functions that safeguard data while preventing recovery of the original message. Hashing is a method of converting a variable length string into a fixed length string. For each input, a good hashing algorithm will generate distinct outputs. The only method to crack a hash is to attempt every potential input until you obtain the same hash every time. A hash can be used to hash data (like passwords) and to create certificates.

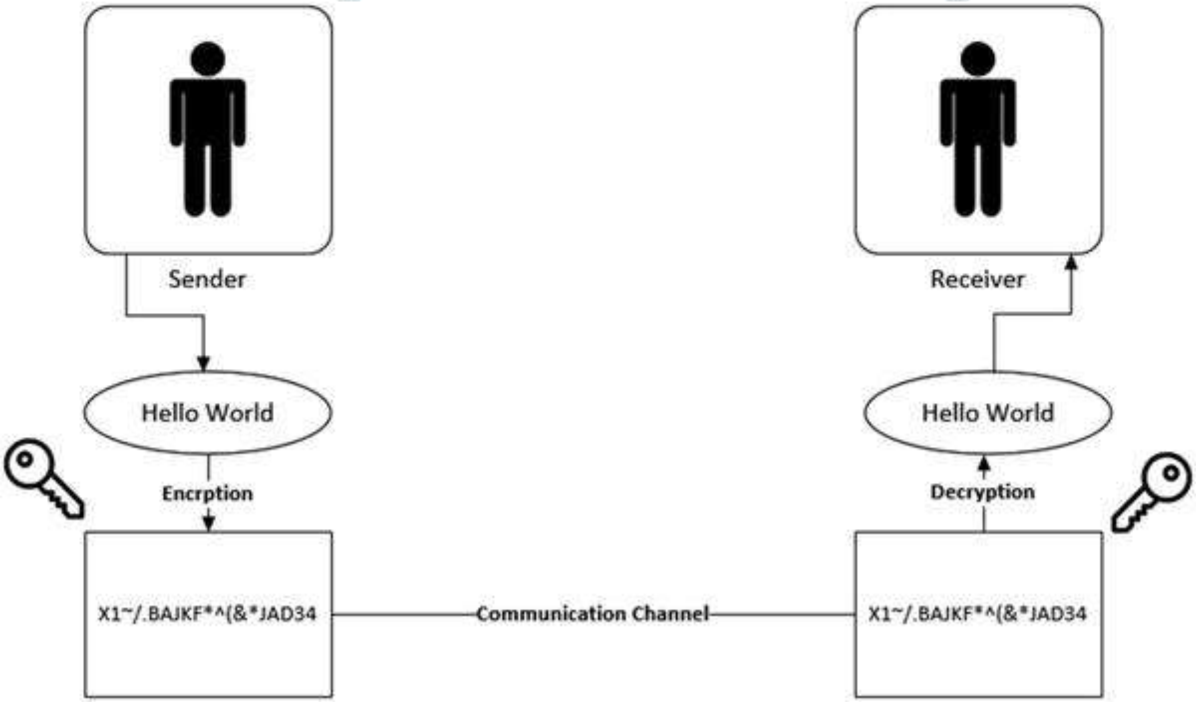
3.4 Digital Password

A digital password is a string of random characters that is used to restrict access to a digital device or software by requiring the user to show authorization through the secret password. Password phishing and hacking have become more common as the number of digital devices and systems that use passwords has grown. This entry discusses the various types and systems of authentication, including digital passwords; reveals the vulnerabilities in digital password systems; considers some notable corporate password thefts; and concludes with recommendations for how users and administrators can combat password hacking.

Digital passwords are a random sequence of computer characters (numbers, letters, symbols, etc.) with no spaces to limit access to digital devices and software applications by letting the user know the secret password for authentication. Created to do. Digital passwords are a form of so-called 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. 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. Analysis: Significance of Cryptography

The selected papers fundamental value is that they provide knowledge about various encryption and decryption methods in order to secure photographs that are regularly downloaded and transmitted across social media and networks.



Working of Cryptography

4.1 Types of Cryptographic Algorithm

4.1.1 DES Algorithm

Data encryption standard (DES) has been found to be vulnerable to very powerful attacks, and as a result, DES's popularity has been found to be on the decline. DES is a block cypher that encrypts data in 64-bit blocks. This means that 64 bits of plain text are fed into DES, which produces 64 bits of ciphertext. With minor variations, the same algorithm and key are used for encryption and decryption. The length of the key is 56 bits.

4.1.2 AES Algorithm

The Advanced Encryption Algorithm (AES) is a symmetric block cypher algorithm with a 128-bit block/chunk size. It converts these individual blocks using 128-, 192-, and 256-bit keys. It encrypts these blocks and then joins them to form the ciphertext. It is built on a substitution-permutation network, or SP network. It is made up of a series of linked operations, such as replacing inputs with specific outputs and bit shuffling. [16].

4.1.3 3 DES Algorithm

DES is a Feistel network-based symmetric-key algorithm. As a symmetric key cypher, it employs the same key for both encryption and decryption. The Feistel network makes both of these processes nearly identical, resulting in a more efficient algorithm to implement. Although DES has a 64-bit block and key size, the key only offers 56 bits of security in practice. Because of the short key length of DES, 3DES was created as a more secure alternative. The DES algorithm is run three times with three keys in 3DES; however, it is only considered secure if three distinct keys are used. [6]

4.1.4 Blowfish Algorithm

Blowfish is a symmetric encryption algorithm, which means that it encrypts and decrypts messages with the same secret key. Blowfish is also a block cypher, which means that during encryption and decryption, it divides a message into fixed length blocks. [13]

4.1.5 RSA Algorithm

The RSA algorithm is an asymmetric cryptography algorithm, which means it employs both a public and private key. A public key, as the name implies, is shared publicly, whereas a private key is private and must not be shared with anyone. Ron Rivest, Adi Shamir, and Leonard Adleman are the inventor names given to the RSA algorithm.

4.1.6 Diffie-Hellman

The Diffie–Hellman (DH) Algorithm is a key-exchange protocol that allows two parties communicating over a public channel to establish a mutual secret without exposing it to the Internet. DH allows the two to use symmetric cryptography to encrypt and decrypt their conversation or data using a public key. [16]

5. Conclusion

This is being written in order to provide a project information on the triple Data Encryption standard for image encryption. The triple data encryption standard is an improved version of the data encryption method 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. 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.

6. Reference

[1] Somya Garg Tarun Garg Bhawna Mallick "Secure Message Transfer Using Triple Des" International Journal of Computer Applications (0975 – 8887) Volume 165 – No.8, May 2017

[2] Anup & Suchithra" Image Encryption Using Triple Des Algorithm" Imperial Journal of Interdisciplinary Research (Ijir) Vol-3, Issue-5, 2017 Issn: 2454-1362, Http://Www.Onlinejournal.In Imperial Journal of Interdisciplinary Research (Ijir)

[3] Nandkumar Bhimnath, Rohan Yemul, Manisha K. M "A Survey Paper on Secured Email Server using 3DES" International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 06 Issue: 03 | Mar 2019 www.irjet.net p-ISSN: 2395-0072 © 2019, IRJET | Impact Factor value: 7.211 | ISO 9001:2008 Certified Journal

[4] M.R.M Veeramanickam Varsha Khenat, Puja Dhalpe Navin Dube "Securing Digital Images Using Watermarking Technique and Triple des Algorithm" Journal for Research| Volume 02| Issue 02 | April 2016 Issn: 2395-7549 All Rights Reserved by Www.Journalforresearch.

[5] Murugan G, Sriram V.P, Ambika M, Kolla Bhanu Prakash, Sudhakar Sengan, Priya V, Pankaj Dadheech, "Implementation of New Secure File Transfer Protocol Using Triple-DES and MD5", *IJAST*, vol. 29, no. 06, pp. 4156 - 4170, May 2020.

[6] Karthik. S, Muruganandam. "Data Encryption and Decryption by Using Triple Des and Performance Analysis of Crypto System" An International Journal of Scientific Engineering and Research 2347-3878 Volume 2 Issue 11, November 2014 Licensed Under Creative Commons Attribution

[7] J. Guru Mohish Srivatsav, Mrs. R. Sheeja "Implementation of Triple Des Algorithm in Data Hiding and Image Encryption Techniques" International Journal of Advanced Science and Technology Vol. 29, No. 3, (2020), Pp. 10549 – 10559

[8] V. M. Silva-García 1, R. Flores-Carapia, I. López-Yañez and C. Rentería-Márquez "Image Encryption Based on The Modified Tripledes Cryptosystem" International Mathematical Forum, Vol. 7, 2012, No. 59, 2929 - 2942

[9] Sanjay Kumar, Sandeep Srivastava "Image Encryption Using Simplified Data Encryption Standard (S-Des)" International Journal of Computer Applications (0975 – 8887) Volume 104 – No.2, October 2014 38

[10] V Goutham Bharadwaja, Yashas, Yathendra Yadav T V, Gelvesh G "Image Encryption for Secure Internet Transfer" International Journal of Engineering Applied Sciences and Technology, 2021 Vol. 6, Issue 1, Issn No. 2455-2143 Published Online May 2021 in Ijeast (Http://Www.Ijeast.Com)

[11] Ibraheem Nadher Ibraheem, Saad Mohsen Hassan, Suaad Ali Abead "Comparative Analysis & Implementation of Image Encryption & Decryption for Mobile Cloud Security"n International Journal of Advanced Science and Technology Vol. 29, No. 3s, (2020)

[12] Akshitha Vuppala, R Sai Roshan, Shaik Nawaz, JVR Ravindra "An Efficient Optimization and Secured Triple Data Encryption Standard Using Enhanced Key Scheduling Algorithm" Center for Advanced Computing and Research Laboratory (2020) 1054–1063 1877-0509 © 2020 The Authors. Published by Elsevier B.V.

[13] Kenneth J. Knapp, Thomas E. Marshall, R. Kelly Rainer, F. Nelson Ford "Information Security: Management's Effect on Culture and Policy Information Management & Computer Security" Issn: 0968-5227 Article Publication Date: 1 January 2006

[14] Omar G. Abood, Shawkat K. Guirguis "A Survey on Cryptography Algorithms" International Journal of Scientific and Research Publications, Volume 8, Issue 7, July 2018 ISSN 2250-3153 http://dx.doi.org/10.29322/IJSRP.8.7.2018.p7978 www.ijsrp.org

[15] Siri Velnad , Richard Howitt, DaleDominey-Howes FrankThomalla, DonnaHouston "Procedural vulnerability: Understanding environmental change in a remote indigenous Global Environmental Change Volume 23, Issue 1, February 2013

[16] Author Panelj.H.P. Eloffm.M.Eloff "Information Security Architecture" Computer Fraud & Security Volume 2005, Issue 11, November 2005, Https://Doi.Org/10.1016/S1361-3723(05)70275-X

[17] Abdalbasit Mohammed Nurhayat Varol "A Review Paper on Cryptography" June2019 DOI:10.1109/ISDFS.2019.8757514
https://www.researchgate.net/publication/334418542_A_Review_Paper_on_Cryptography