Efficient Cryptographic Encryption Techniques for Data Privacy Preservation

Mangore Anirudh K, M Roberts Masillamani

Abstract: In present digital era, a remarkable development in the networking technology leads a process of interchanging of the digital information very often. The information in both the private ownership and public sectors are increased which needs Availability Authentication, Confidentiality, Integrity. The security of the confidential information from the unauthorized access can be done by numerous file encryption strategies. Security is the significant issue, when the delicate data is saved and moved throughout the web where the data is no longer secured by physical limits. Cryptography is an important, reliable and effective element to make sure the protected interaction between the various entities by moving muddled data and also only the authorized concern person can be able to retrieve the data. The security of communication is an essential concern on World Wide Web. It has to do with privacy, integrity, authentication throughout the access or modifying of secret internal credentials. This article will focus a few of the most fascinating algorithms of file encryption that are presently utilized. This paper emphasis primarily on existing various sort of file encryption strategies

I. INTRODUCTION

Security is the main concern to keep information safe and spread it throughout the unknown network source with safe way. Thus, the standard requirement of every deal is the safe interaction over networks. Cryptography is a necessary element for secured interaction and transmitted flow of details through secured unique services like privacy, information stability, gain access to non-repudiation ,control, authentication and. It supplies a method to secure delicate details by moving it into inarticulate and just the licensed person can gain access to this info by transforming into the initial text. The procedure to transform the general text into cipher text with the secret is called file encryption procedure. The reciprocal procedure of file encryption is otherwise known as decryption topology. The algorithms by using cryptography is safe and secure and effective, low expense, need little memory footprint, simple to carry out and used on numerous fields. The large variety of benefits is established to protect cryptographic algorithms by utilizing various mathematical procedures[24],[25]. It is rather hard to establish completely safe and secure algorithm for file encryption because of the obstacles by means of cryptanalysts , where they are continually trying to utilize any existing cryptographic systems [1] - [5] .To accomplish high-security requirements, the choice of best algorithm plays a crucial function which safeguard the cryptographic parts to cryptanalysis. The details is to be safe and secure when it is sent while secret information like ATM cards, charge card, banking deals and digital ideal management requirement to be safeguarded. To prevent details hacking from unapproved users file encryptions methods are utilized. For information security in cordless interaction file encryption strategies plays substantial function due to the fact that cordless interaction is utilized in online transmission. Varied file encryption methods are utilized to safeguard the personal information from unapproved usage. File encryption attains the information security better. The development of file encryption is moving towards a future of limitless possibilities. Daily brand-new approaches of file encryption strategies are found.

Revised Manuscript Received on May 05, 2019.

Mangore Anirudh K, Department of Computer science and Engineering, Bharath Institute of Higher Education and Research, Chennai, Tamilnadu, India.

M Roberts Masillamani, Department of Computer science and Engineering, Bharath Institute of Higher Education and Research, Chennai, Tamilnadu,India.

II. CLASSIFICATION OF CRYPTOGRAPHY

Symmetric Key Encryption

The symmetric (secret key) file encryption is using comparative trick for the file encryption and unscrambling of a sender message. Encrypted sender file and equating tricks are hiding and felt in one's bones by licensed sender and recipient who need to interact. The allotment of various tricks to the special occasions constructs the basic protection of the message. The encrypted symmetric file quality is relying on the trick of file encryption and equating tricks. The evaluations of encrypted symmetric file can be bought into square and stream figure based upon the occasion of message bits [14], [15],[22] In a square figure, an occasion of fixed size message characters (a square) is protected at the precise very same time and received by the recipient. Based upon the results of the message, tricks and cipher text the block cipher can be classified into binary and non-binary block cipher. The binary block cipher’s message bit is 64, 128, 192, and 256 and also undefined requirement of non-binary block cipher is relies on the cipher application

Asymmetric Key Encryption

The Asymmetric file encryption is generally suggested to as public, there are differed tricks are utilized for the message in both encryption and decryption.

The file encryption trick remains in addition specified as the public trick and can be made use of to encode the message with the trick.[22],[23],[24] The decryption trick is mentioned to as technique or individual trick and can be used to figure out the message. The quality of the unequal file encryption is used with ingenious mark then it can provide to the clients through message confirmation recommendation. The out of balance file encryption calculation consists of RSA [17], Diffie-Hellman evaluation [18], and so on

Data Encryption Standard (DES)

In 1972 B.DES was the earliest symmetric file encryption calculation which was established by IBM and gotten by National Bureau of Standard (NBS) in 1977 as Federal Information Processing Standard (FIPS). National Institute of Standards and Technology (NIST) is the present organization to perform the standard file encryption evaluation worldwide. It incorporates 64 bits vital which consists of 56 bits are lawfully used by the estimate as important bits and are haphazardly produced. The remaining of the 8 bits that are not taken into account, instead of that it is utilized for the mistake location as set to make an equality of every 8-bit byte [19], [20], [21] DES made use of the one trick for file encryption and unscrambling treatment and necessary 56bits length and plays out the message of the encrypted file utilizing the 64 bits square size. For that reason, the unscrambling treatment on a 64 bits figure message by incorporating the similar 56 bits necessary to gives the extremely first 64 bits square of the message [23]. The DES calculation forms the 64 bits contribution with a covert stage, 16 rounds of the trick and the last adjustment.

For a very long time, and amongst numerous people, "secret code making" and DES have actually been associated. This treatment can keep running in a couple of modes and consists of 16 rounds. In spite of the truth that this is thought about "strong" file encryption, many companies utilize "triple DES", which uses 3 types in development. It is not always the case that a DES-scrambled message can't be "broken.".

Triple Data Encryption Standard (3DES)

Triple Data Encryption Standard (3DES) is developed by IBM in 1998 as Triple Data Encryption Algorithm (TDEA) and institutionalized in ANSI X9.17 and ISO 8732. 3DES was shown as the source of alternative for DES, but because of the enhancement in the essential length and utilize the DES algorithm to the 3 more times in each information block. The 56 bits essential length of DES estimation was typically adequate prior to when the computation prepared nevertheless as the calculation power is hiked then the strength attack is possible. However, 3DES provides a fundamental technique by the addition of essential length instead of structure an overall square figure and it makes sure versus the savage power attack. A savage power attack regularly trying each plausibility of getting to secrets up until the very first message is gotten.

RSA (Rivest Shamir and Adleman) Algorithm

RSA is an estimation for public crucial cryptography that depends upon the assumed problem of factoring big integers, the factoring issue [10] RSA represents Ron Rivest, Adi Shamir and Leonard Adleman, who initially publically depicted the algorithm in 1977. In RSA, user right off the bat makes and after that disperses the outcome of 2 comprehensive prime numbers and their open secret as an assistant esteem [11] These prime numbers should be remained discreet. Public secret can be used by anyone to rush a message. The RSA estimation consists of 3 phases:

- Key age
- Encryption and
- Decryption

Advanced Signature Algorithm

A digital signature is a mathematical plan for showing the credibility of a digital message or file. A legitimate digital signature offers a recipient factor to trust that the message was made and sent out by a recognized sender; with completion objective that the sender can't reject having actually sent out the message (verification and non-renouncement) which the message was not customized in transmission (stability) [12] Digital signatures are generally used for monetary exchanges, configuring dispersion, and in various circumstances where it is necessary to identify bogus or changing. Digital signatures are often utilized to actualize electronic marks, which mention any electronic details that communicate the objective of a mark. It isn't legitimate that each and every single electronic mark makes use of sophisticated marks.

Digital signature uses a different sort of balance cryptography. For messages sent out through a non safe and secure channel, a properly actualized innovative mark offers the collector inspiration to rely on the message was sent out by the asserted sender [13] Digital signatures are proportional to traditional composed by hand marks in many relates to, nevertheless properly carried out innovative marks are more difficult to style than the handwritten kind. Digital signature plots in the sense used here are cryptographically based, and ought to be actualized legally to be effective. Digital signature can also offer non-disavowal, suggesting that the underwriter can't successfully ensure they didn't sign a message, while in addition asserting their personal essential stays trick; even more, some non-renouncement strategies use a duration stamp for the Digital signature, so that no matter whether the personal secret is exposed, the mark stands. Thoroughly significant messages may be anything representable as a bit string: precedents include e-mail, or a message sent out through some other cryptographic convention.

Diffie– Hellman Algorithm

Diffie-- Hellman essential trade is a specific method for trading cryptographic secrets [14] it is among the most prompt affordable circumstances of essential trade actualized inside the field of cryptography. The Diffie-- Hellman essential trade method allows 2 unknown events to equally develop a typical trick key over an unpredictable interchanges channel [15] this secret can be then utilized to encode resulting interchanges making use of a symmetric essential cipher.

The method was pursued immediately a while later on by RSA, a use of open crucial cryptography making use of deviated computations.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

AES (Advanced Encryption Standard)

The Advanced Encryption Standard (AES) is file encryption estimation for protecting delicate however uncategorized product by U.S. Government companies and, as a possible result, might in the end becomes the accepted file encryption requirement for service exchanges in the personal department. It is energetic trade for the Data Encryption Standard (DES) and to a lower degree Triple DES. The information needed a symmetric computation making use of square file encryption of 128 bits in size, supporting crucial sizes of 128, 192 and 256 bits, as a base. The algorithm was needed to be royalty-free for usage make use of around the world and deal security of an appropriate measurement to make sure details for the following 20 to 30 years. Their hardware program executions are basic even in limited regulations (for example, in a smart card) and additionally produce terrific security versus different attack techniques.

III. CONCLUSION

Cryptography presumes considerable task in broadening advancement of innovative details data storage and correspondence. It is used to achieve the mains of security goals like personal privacy, respectability, verification, non-disavowal. It is broke down that in Diffie-Hellman essential trade cryptography algorithm, secret keys are traded in between 2 customers. While a digital signature used by receiver in digital signature algorithm to validate that the flag got isn't altered. It is furthermore presumed that each of the systems is important for constant file encryption. Every treatment is remarkable in its own particular way, which might be suitable for different applications. Many brand-new file encryption techniques growing in this method fast and protected basic file encryption systems will reliably exercise with high rate of security.

REFERENCES

1. K. Mandal, C. Parakash, and A. Tiwari, “Performance evaluation of cryptographic algorithms: DES and AES,” in Proceeding of the IEEE Students' Conference on Electrical, Electronics and Computer Science: Innovation for Humanity (SCEECS), 2012.
2. M. Ebrahim, S. Khan, and U. bin Khalid, “Symmetric algorithm survey: A comparative analysis,” International Journal of Computer Applications, vol. 61, no. 20, pp. 12–19, 2013.
3. N. Kumar and P. Chaudhary, “Performance evaluation of encryption/decryption mechanisms to enhance data security,” Indian Journal of Science and Technology, vol. 9, no. 20, 2016.
4. Disina, A. H., Pindar, Z. A., & Jamel, S., “Enhanced caeser cipher to exclude repetition and withstand frequency cryptanalysis,” Journal of Network and Information Security, 2015.
5. V. V Palagushin and A. D. Khomonenko, “Evaluation of cryptographic primitives security based on proximity to the latin square,” in
6. Proceeding of the IEEE 18th conference of fruct association, pp. 266–271, 2016.
7. S. H. Jamel and M. M. Deris, “Diffusive primitives in the design of modern cryptographic algorithms,” in proceedings of the International Conference on Computer and Communication Engineering (ICCCE08): Global Links for Human Development, pp. 707–710, 2008.
8. S. Goldwasser and M. Bellare, Lecture Notes on Cryptography, Cambridge, Massachusetts, 2008.
9. A.Kaushik, M. Barnela, and A. Kumar, “Keyless user defined optimal security encryption,” International Journal of Computer and Electrical Engineering, vol. 4, no. 2, pp. 2–6, 2012.
10. W. Stallings, Cryptography and network security: principles and practices. Prentice Hall, 2005.
11. M. Stamp, Information Security: Principles and Practice. John Wiley & Sons, 2011.
12. F.Maqsood, M. M. Ali, M. Ahmed, and M. A. Shah, “Cryptography: A comparative analysis for modern techniques,” International Journal of Advanced Computer Science and Applications, vol. 8, no. 6, pp. 442–448, 2017.
13. S. Ahmad, K. M. R. Alam, H. Rahman, and S. Tamura, “A comparison between symmetric and asymmetric key encryption algorithm based decryption mixnets,” in Proceedings of the IEEE International Conference on Networking Systems and Security, 2015.

A. M. Alshahrani and S. Walker, “Implement a novel symmetric block cipher algorithm,” International Journal on Cryptography and Information Security, vol. 4, no. 4, pp. 1–11, 2014.

14. M. Dworkin, “Recommendation for block cipher modes of operation,” NIST Spec. Publ. 800-38B, 2005.
15. T. Nie and T. Zhang, “A study of DES and Blowfish encryption algorithm,” in Proceedings of 10th IEEE Region Annual International Conference TENCON, pp. 1–4, 2009.
16. M. E. Smid and D. K. Branstad, “Data Encryption Standard: past and future,” Proceedings of the IEEE, vol. 76, no. 5, pp. 550–559, 1988.
17. J. Daemen, V. Rijmen, and K. U. Leuven, AES Proposal: Rijndael. (NIST), National Institute of Standards, 1999.
18. N. I. of Standards-(NIST), Advanced Encryption Standard (AES). Federal Information Processing Standards Publication197, 2001.
19. B. Schneier, “Description of a new variable-length key, 64-bit block cipher (Blowfish),” in Proceedings of the Fast Software Encryption: Cambridge Security Workshop Cambridge, U. K., pp. 191–204, 1994.
20. S. Jamel, M. M. Deris, I. T. R. Yanto, and T. Herawan, “The hybrid cubes encryption algorithm (HiSea),” Communications in Computer and Information Science, Springer-Verlag Berlin Heidelberg, vol. 154, pp. 191–200, 2011.
21. W. Stallings, “The RC4 stream encryption algorithm,” in Cryptography and network security, 2005.
22. MangoreAnirudh K 1, M Roberts Masillamani, Privacy Of Big Data In Healthcare Monitoring System, Journal of Adv Research in Dynamical & Control Systems, Vol. 10, 02-Special Issue, 2018.
23. MangoreAnirudh K 1, M Roberts Masillamani, Big Data Encryption In Healthcare Monitoring System, Journal of Adv Research in Dynamical & Control Systems, Vol. 10, 02-Special Issue, 2018.
24. ShwetambariKharabe, C. Nalini,” Robust ROI Localization Based Finger Vein Authentication Using Adaptive Thresholding Extraction with Deep Learning Technique”, Journal of Advanced Research in Dynamical & Control Systems, Vol. 10, 07-Special Issue, 2018.
25. ShwetambariKharabe, C. Nalini,” Using Adaptive Thresholding Extraction - Robust ROI Localization Based Finger Vein Authentication”, Journal of Advanced Research in Dynamical & Control Systems, Jour of Adv Research in Dynamical & Control Systems, Vol. 10, 02-Special Issue, 2018.