Quality Analysis of Network Security using Cryptographic Techniques

Aniket Dalvi
Research Scholar, MCA
Thakur Institute of Management Studies, Career Development and Research (TIMSCDR), Mumbai India

Charul Dalvi
Research Scholar, MCA
Thakur Institute of Management Studies, Career Development and Research (TIMSCDR), Mumbai India

Rahul Deshmukh
Research Scholar, MCA
Thakur Institute of Management Studies, Career Development and Research (TIMSCDR), Mumbai India

ABSTRACT
Data or Information security is a testing issue today that requests a strong encryption which is exceptionally hard to break. System Security is the most fundamental part in data security in light of the fact that it is in charge of securing all data went through organized PCs. A considerable measure of examination has been carried out in cryptography such a large number of specialists have proposed diverse calculations for encryption. Data can be access by unapproved client for insidious reason. In this way, it is critical to actualize successful encryption/decoding calculations for more security. In this paper we have given an extensive mixture of different calculations and systems, for example, Triple DES, BREA, AES, Elliptic Curve Cryptography, CryptoStegnography, Dual RSA, Stream and Block figures, and Quantum Cryptography through which information will be secured. A definite examination is carried out to have an acceptable view about all the methods, nature of every strategy and will examine open key base, really great protection, computerized signature, private key encryption, piece shrewd parallel encryption.

Keywords
Elliptic Curve; Quantum Cryptography; Private Key Encryption

1. INTRODUCTION
Cryptography is presented in the field of Network security which makes the information more secured. Cryptography is an expression with a Greek beginning, signifies "mystery or concealed written work," which is utilized to scramble information utilizing a key. Every Technique is investigated in subtle element to view its quality regarding security. Each method has its detriments and preferences that are said in the paper. As innovation is quickly expanding, significance of security is additionally expanding. Security is a fundamental figure today's mechanical world. Unapproved access of information can be hurtful because of which information can be hacked and can be utilized for malignant reason. Cryptography gives distinctive procedures to assurance against unapproved access which is sufficiently secured that obliges and a lot of time to unscramble a message which either surpasses time or expense of data.

2. TYPES OF CRYPTOGRAPHIC ALGORITHMS
This survey provides the detail analysis on network security using evaluation criteria. Quality of cryptographic techniques is analyzed on the basis of parameters which are mentioned below:

2.1 Network Security Using Cryptographic Techniques
The research paper focuses on Crypto graphy. System Security is the most fundamental part in data security on the grounds that it is in charge of securing all data passed through arranged machines. System Security & Cryptography is an idea to ensure system and information transmission over remote system. System security includes the approval of access to information in a system, which is controlled by the system manager. System Security is the most basic part in data security in light of the fact that it is in charge of securing all data passed through organized machines. 105-107 machine system foundations, approaches embraced by the system director to ensure the system and the system open assets from unapproved access, and reliable and constant checking and estimation of its adequacy joined together.

2.2 Literature Review of Cryptography & Network Security
The research paper proposes that cryptography serves as the establishment for most IT security arrangements, which include: Digital marks that are utilized to check the realness of overhauls for machine working frameworks. The predominating myth that mystery is useful for security has been demonstrated off with the affiliation that cryptosystems give to a great degree solid security. When these frameworks use a Cryptography and Network Security 23 lopsided key administration framework process where people in general key is known to everybody and the mystery key is known just to the person who has it. Security is accomplished when cryptography depends on one of its most fundamental standards that the calculations stay open.

2.3 Cryptosteganography
Security Enhancement by Utilizing Efficient Data Hiding Techniques The research paper utilized Cryptography routines and Steganography procedures for secure and better correspondence. This make the message location handle much harder for the hackers who hides between the Sender and Receiver. The two layers of security which is Cryptosteganography are utilized which makes it hard to recognize the vicinity of hidden message. However if the hacker has assaulted the carrier of message then he won't have the capacity to get the first message as all the related information here is in encoded structure. The mix of Cryptosteganography system is used so hacker needs to invest a considerable measure of time and exertion for attempting a few assaults and getting the first message. Although both of these methods are not difficult to actualize yet there mix will give much productive and dependable security.

2.4 Encoding and Decoding of a Message in the Implementation of Elliptic Curve Cryptography using Koblitz's Method

This paper proposes that ECC (Elliptic Curve Cryptography) is perfect for obliged environment, for example, pager, PDAs, cellular phones and shrewd cards. The key functions in ECC are Encoding and Decoding. ECC is an open key cryptography that offers execution points of interest at higher security levels. Just the specific client knows the private key while the general population keys are dispersed to all clients tuning in the correspondence. The results of Koblitz's methods conclude that execution time for encoding is distinctive for diverse estimations of ECC domain parameters. The execution time taken for translating is consistent for distinctive estimations of space parameters. The execution time for decoding is insignificant contrasted with that of Encoding.

2.5 Hybrid Cryptography Algorithm

The research paper proposes Elliptic Curve Cryptography for encryption, Dual-RSA (Rivest Shamir and Adleman) calculation for verification and MD-5 (Message Digest) for uprightness. This new security convention has been intended for better security with uprightness utilizing a mix of both symmetric and asymmetric cryptographic strategies. The RSA encryption and unscrambling time is more prominent than Dual RSA on the grounds that Dual RSA performs the encryption and decoding operation for two blocks. Since, the message is scrambled with ECC (Elliptic Curve Cryptography) and key is encoded by utilizing Dual RSA. So, Dual RSA concludes two preferences one is the message can't be unscrambled and time needed to perform the encryption and decoding operation less contrast with RSA in light of the fact that Dual RSA perform encryption and unscrambling by two blocks at once.

2.6 Encryption Using Different Techniques: A Review

The review paper investigated distinctive lopsided cryptography systems, that includes RSA (Rivest Shamir and Adleman), Diffie- Hellman, DSA (Digital Signature Algorithm). The results demonstrates that in Diffie-Hellman cryptography calculation mystery keys are traded between two client whereas an advanced mark is utilized by receiver as a part of DSA to affirm that the sign got is unaltered. It is likewise inferred that all the strategies are valuable for ongoing encryption. Every system is special in its own specific way, which may be suitable for distinctive applications. Regular new encryption system is developing consequently quick and secure traditional encryption methods will dependably work out with high rate of security.

2.7 Timing Evaluation of Known Cryptographic Algorithms

The research paper proposes another timing assessment model focused around arbitrary number to analyze the time consumption of the known cryptographic calculations: Triple-DES (Data Encryption Standard), AES (Advanced Encryption Standard) and RSA (Rivest-Shamir- Adleman). Model for assessment consist of two assessing modes: Diverse Plaintexts in the Same Key (DPSK), the Same Plaintext in Diverse Keys (SPDK). As the premise of the assessing model, the plaintext and the relating key are both created by arbitrary numbers. The results demonstrate that under the same key length and for the same size of the prepared information, RSA is about a few hundred times slower than AES, triple-DES is around three times slower than AES. The drawback is in scrambling huge size plaintext is its computational overhead. Therefore, assessment model focused around the arbitrary number creating system may be helpful for examining new and more powerful calculations.

2.8 Stream and Block Cipher Algorithms

The research paper proposes the correlation in the Block and Stream cipher algorithms, utilizing distinctive information sizes and key sizes. The result demonstrates the prevalence of RC4 (Rivest Cipher) calculation over different calculations as far as preparing time and throughput. Then again, the IDEA (International Data Encryption Algorithm) create the most noticeably awful comes about out of every last one of calculations actualize here. There is likewise great clear that stream figure calculations as a rule scramble quicker than the piece figure calculations. Nothing but the impact of changing the key size on encryption time was likewise considered, and the results demonstrate that growing the key size could decrease the encryption time on some calculation that have settled round number.

2.9 Quantum Cryptography

This research paper focuses on quantum cryptography, and how this engineering helps the system security. The quantum cryptography system joins a variety of QKD (Quantum Key Distribution) strategies to entrenched web innovation to build a protected system. The security of quantum cryptography depends on the sacred laws of quantum mechanics, and the incomprehensibility of impeccable cloning of non- orthogonal states suggests the security of this convention. The quantum cryptography depends on two imperative components of quantum mechanics-the Heisenberg Uncertainty standard and the rule of Photon Polarization. The security of quantum cryptography relies on upon the establishment of quantum mechanics, and that can alter the system security. The advances in machine handling force and the risk of restriction throughout today's cryptography frameworks will remain a main thrust in the proceeded with innovative work of quantum cryptography.

2.10 Multiphase Encryption:A New Concept in Modern Cryptography

This article revolves around the new encryption techniques. Multiple Encryption is the method of encrypting an already encrypted text one or more sentence, either using the same or different algorithms. Encryption is done through cryptographic algorithms coded on plaintext. Diffie and Hellman have argued that 56 –bit key used in First State (Data Encryption Touchstone) is too small then a new approach is used which is Triple DES that comprises three Key each of 56 bit. This idea improves the strength of algorithm. Through this complexity may occur but it enhances more security over data transmission. It provides better security even if some element zero is damage, the savvy of original data can still be maintained by multiple encryptions. The disadvantage is that it affects the performance and speed of the scheme.

3. CONCLUSION

This paper explains that key conception is the symmetric Francis Scott Key conception where field text edition dual matter is converting into encrypted text known as naught text using common soldier key where cipher text decrypted by same private key into plain text. The encryption key is trivially related to the decryption key, in that they may be identical or there is a simple transform to go between the two keys. In each cycle, same plaintexts are respectively encrypted by "A new Symmetric key Coding Algorithmic rule is program using extended MSA method: DJSA symmetric key algorithm". This

result clear that proposed technique is better result producing as compared "DJSA symmetric key algorithm" and "Effect of Security Increment to Symmetric Data Encryption through AES Methodology".

Each and every calculation having its own particular preferences and inconveniences, this paper gives a general depiction of different cryptographic methods with parameters. Each method and calculation is novel in its own particular terms. In any case Private Key encryption, quantum cryptography and crypto steganography are the best in light of the fact that these are so fiery and quick that they can't be delicate effectively. In this examination paper distinctive methodologies have exhibited through which the level of security increments.

4. FUTURE ENHANCEMENT

In future, the developing innovation that is quantum cryptography can be utilized to give a profoundly secure correspondence. The Quantum Cryptography can possibly make a significant commitment to the system security among government, organizations, and scholastic environment.

5. REFERENCES

[1] https://en.wikipedia.org/wiki/Cryptography .

[2] https://en.wikipedia.org/wiki/Public- key_cryptography.

[3] fttps://www.researchgate.net/publication/283770069_Byte_Rotation_Encryption_Algorithm_through_parallel_processing_and_multi-core_utilization.

[4] http://science.howstuffworks.com/science-vs-myth/everyday-myths/quantum-cryptology.html.