International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
https://www.ijcsjournal.com/ Volume 10, Issue 2, No 7, 2022. ISSN: 2348-6600
Reference ID: IJCS-454 PAGE NO: 3079-3085

Review of Secure Communication over the Public Network using Modern Techniques

[1] Dr. Ramesh Palanisamy, [2] Rehab khameis shanan AL-Zuwaydi,
[3] Manal Mohammed Humaid Al aamri
Department of Information Technology,
University of Technology and Applied Sciences – Ibra, Sultanate of Oman.
palanisamy@ict.edu.om, 36s1749@ict.edu.om, 36s1749@ict.edu.om

Abstract

At present, it can be said that data technology is developing quite quickly, especially with the widespread use of the Internet. As a result, one of the major problems we currently face is the security of organizational communications. This paper aims to address the problems with the security information encryption computations used by the current organization. We explore the effects of various encryption techniques on advancing organizational security, starting with the PC network correspondence security information encryption calculation. The analysis' findings demonstrate that it is understood that using a connection encryption calculation together with a network's correspondence security calculation can increase security. The start-to-finish encryption computation can enhance the security of digital transactions. The RSA and DES calculations are two extremely agent calculations; they address different encryption frameworks. According to the viewpoint of organization, information connect, three techniques are combined encryption calculation, hub encryption calculation, and start-to-finish encryption calculation.

1. Introduction

Since the beginning of the new century, with the rapid advancement of modern PC data innovation, PCs have gradually become a necessity for modern people to engage in open work like collaboration and business exchange, entertainment training and learning, and daily existence [1], even though PC network remote correspondence enjoys various benefits, such as instant, good, quick, no functioning time, and organization space limi Nevertheless, they frequently have benefits and drawbacks. While bringing about a great deal of comfort for people's lives and jobs, security-related problems, including organizational security flaws, infection programming interruptions, programmer weakness interruptions, and organizational server security data system leaks, often appeared [3, 4].

There are now real threats to the legitimate rights and interests of business clients and the security of residents' very own data [5] since the multicomputer network's distant communication

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
https://www.ijcsjournal.com/ Volume 10, Issue 2, No 7, 2022. ISSN: 2348-6600
Reference ID: IJCS-454 PAGE NO: 3079-3085

arrangement has been drastically reduced. As a result, a key area of academic research is minimizing security risks in PC network correspondence [6]. The practical use of information data encryption innovation [7] provides useful fictitious and specialist references [8].

Using particular encryption technology, information plaintext encryption converts such straightforward advanced plaintext data alterations into computerized cipher text that is difficult for regular people to decipher [9]. That means it cannot be decrypted. In this concept, the specialist staff first referred to the need to discern precisely the essential significance and significant disparity between the plaintext of the secret key and the cipher text [10]. The opposite is the cipher text, which changes handling [11] has used. The cipher text is difficult for ordinary people to decipher. When experts are preparing for network information security encryption, they could need to separately sort out the information source and information collector [12, 13].

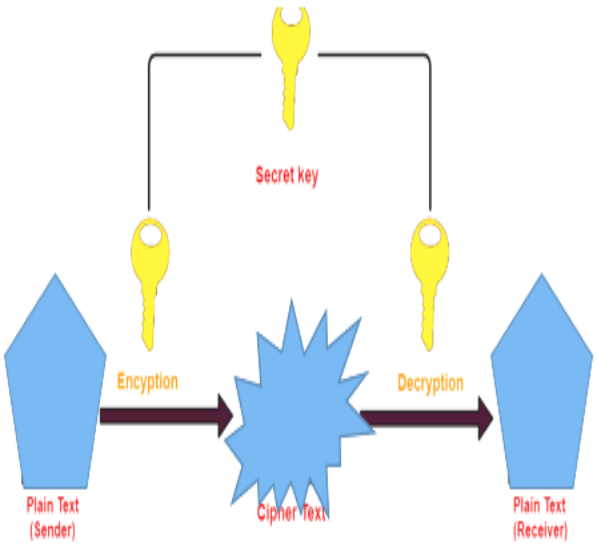
To discuss the function of the newest encryption breakthrough in network security protection. PC expert Liu provided a detailed introduction to the innovation and strategy standards for PC information encryption, broke down the problems in the PC industry into logical and mechanical flow obstructions, and explained relevant research approaches and advancements [14]. Wang et al. discussed the applicable specialized hypothetical presumption and recommended the investigation relevance and examination status of PC network security encryption calculations in their article. Additionally, it demonstrated the value and significance of innovation in personal safety throughout the organization activity stage [15]. Yang et al. discussed the use of information encryption innovation in the study and suggested the many advantages of this invention [16]. Ruslan and Tsouris said that information encryption innovation incredibly safeguards the protection of data and works on the secrecy of information transmission in an organized framework, which positively affects working on the security of PC network interchanges [17].

2. Cryptographic Algorithms

In a cryptographic framework, cryptographic computations are collections of cycles or rules that are used to encrypt and decrypt communications. In plain English, they are procedures that protect information by preventing access by unauthorized parties. These computations serve various functions, including ensuring safe and accurate financial transactions. Most cryptography computations use encryption, which allows two groups to communicate while preventing unauthorized outsiders from reading such exchanges. Cipher text sometimes called jumbled Text, is created from understandable plaintext through encryption. After being encrypted, the information is decrypted to restore it and make it understandable to the intended person. Both encryption and decryption rely on computations to function. Calculations used in cryptography come in many different forms. But many fall into one of two categories: symmetric or asymmetrical configurations.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
https://www.ijcsjournal.com/ Volume 10, Issue 2, No 7, 2022. ISSN: 2348-6600
Reference ID: IJCS-454 PAGE NO: 3079-3085

Nevertheless, some structures mix the two classes equally. Symmetric calculations, also known as symmetric or shared-key calculations, operate by using a key only known to the two people who have given their approval. While they can be implemented as square codes or stream figures, the Message is encoded and decoded using the same key. The Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are the most well-known applications of symmetric cryptography computations. Calculations in lopsided cryptography require two keys: a public key and a private key. Although the private key should be concealed to protect the data, the public key can be discovered. One of the most well-known applications of this computation is RSA. In general, symmetric computations happen far more quickly than kilter ones. This is typically related to the fact that just one key is needed. In any instance, the drawback of shared-key frameworks is that both parties are aware of the secret key. Furthermore, access to the information is controlled by the key as the computation used is in a public space. To ensure security, the keys should be protected and replaced reasonably frequently.



3. Algorithm Types

The data that has been shared between the partners has added security features thanks to an encryption algorithm that has been developed. Depending on the security requirements, numerous computations can be used with the code suite. The standard encryption algorithms include the following as a component.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
https://www.ijcsjournal.com/ Volume 10, Issue 2, No 7, 2022. ISSN: 2348-6600
Reference ID: IJCS-454 PAGE NO: 3079-3085

• IDEA Algorithm
• MD5 Algorithm
• Symmetric Algorithms
• Diffie Hellman Key Exchange Algorithm
• Digital Signature Algorithm
• Encryption Algorithm
• Advanced Encryption Standard
• Asymmetric Encryption
• ElGamal Encryption
• HMAC, Certificate Revocation, RC5
• DES Algorithm
• Brute Force Algorithm
• SHA Algorithm, RSA Algorithm
• What Is Digital Certificate?

4. Essential Terms of Cryptography

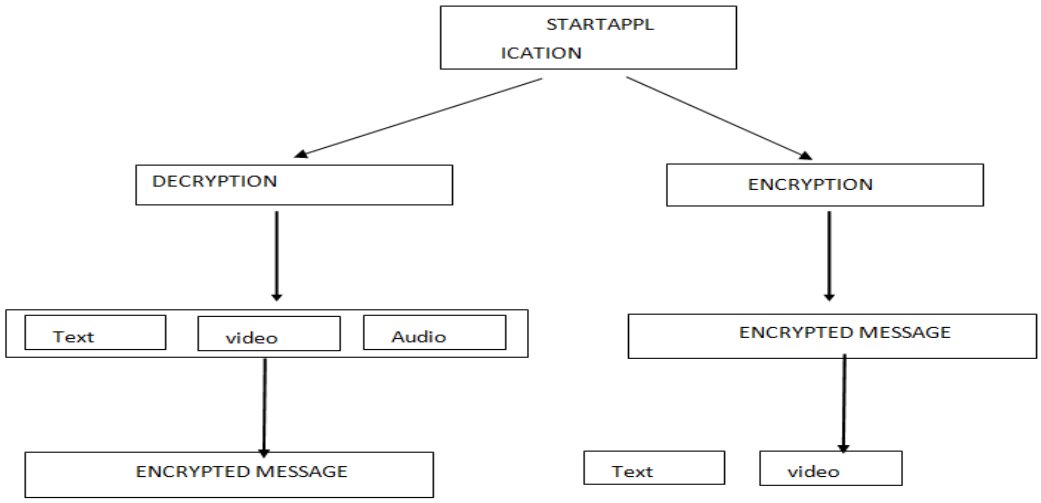
The act of clouding a communication by obscuring its content is called encryption. To validate a unique assertion, it may also be used to produce advanced markings.

Decoding is the encryption process in reverse. In most cases, the cipher text or computation used for encryption is also used for decryption. The illustration represents a method, computational capability, or interaction for encoding or unscrambling. A code is a series of simple cut advancements that may be used to encrypt data. Data might be in plaintext before encoded or in its original, undisturbed structure.

Cipher text is the outcome of plain text encryption and is an incomprehensible code. Without knowledge of the underlying keys or the calculations used during encryption, cryptanalysis is the demonstration of deciphering an encoded communication. The cryptanalyst could already know a portion of the plaintext but wants the remaining amount to be in the cipher text. They may also need to be familiar with the key and calculations that were used.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
https://www.ijcsjournal.com/ Volume 10, Issue 2, No 7, 2022. ISSN: 2348-6600
Reference ID: IJCS-454 PAGE NO: 3079-3085

5. Proposed System



Our input is first converted to Base-64 before the cryptography is applied. And we store the Text we acquired in a text file. We next go on to cryptography.

Sender Side

Cryptographic steps make up the sender side. This approach begins with cryptography.

Cryptography Stage

The Advanced Encryption Standard (AES) algorithm is used during the encryption step, and AES uses the same key to encrypt and decode data as a symmetric encryption technique. The SPN (substitution permutation network) approach, which uses multiple rounds, is also used to encrypt data. What makes AES so powerful is the enormous quantity of encryption rounds it employs.

Key + Message equals input. The output is an encrypted message.

Receiver side

The decoding stage is on the receiver side, and the Message will be decrypted on the receiving side.

Decryption Stage

We use the data that was taken from the encryption step in the decryption stage and employ AES. The Encrypted Message and the key can be used to do the decryption.
Key + Encrypted Message is the input. Plain Text is the output.

The Plain Text is currently in Base-64 format. Apply Base-64 conversion after receiving the plain Text to convert it to the specified input: Text, an image, a video, or an audio file.

6. Cryptographic

- Passive attack
- Active Attack

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
https://www.ijcsjournal.com/ Volume 10, Issue 2, No 7, 2022. ISSN: 2348-6600
Reference ID: IJCS-454 PAGE NO: 3079-3085

7. Cryptanalytic Technique

- Cypher Text
- Plaintext Attack
- Man-in-the-Middle Attack
- Correlation
- Attack Against or Using the Underlying Hardware
- Faults in the Crypto system our

8. Data Security Protocol

- IPSec protocol
- SSL Secure Shell (SSH
- Hyper Text Transfer Protocol Secure (HTTPS
- Kerberos

9. Conclusion

We have looked at particular encryption computations in this study. Due to correlations conducted on numerous cryptographic computations, such as AES, DES, RSA, and others, we have discovered that each measure has its benefits, expressed by employing number bounds. As data and correspondences are regularly overlooked by open agencies in today's internet-based society, we learned that records security has become increasingly important. We will implement the first stage this Semester, which consists of the following steps: Planning, which entails choosing an appropriate application title, language, and algorithm and accurately defining the application's purpose, how to graph it, its goals, and its advantages and disadvantages.

In this paper, we have examined unique encryption calculations. We have located that every measure has its advantages, as indicated by using number boundaries, due to the correlations made on several cryptographic calculations, for example, AES, DES, RSA, ETC. We discovered that in this net world, records safety assumes a critical phase as data and correspondences are frequently neglected through open agencies. This Semester, we will put into effect The first stage, which includes: Planning, which consists of selecting a suitable title, language, and algorithm for the application, as correctly as clarifying the thought of the application, how to graph it, its objectives, its professionals and cons. We will implement the last phase in the next Semester, which entails developing the program, testing it, and ensuring it functions properly.

10. References

[1] Mitali, Kumar Manoj, Sharma Arvind, "A Survey in various cryptography techniques", IJETTCS, volume 3, Issues 4, July August 2014, ISSN2278-6856.

[2] Ritu Tripathi, Sanjay Agrawal, "Comparative Study of Symmetric and Asymmetric Cryptography Techniques", International Journal of Advance Foundation and Research in Computer (IJAFRC), volume 1, issue 6, June 2014, ISSN 2348 – 4853.

[3] Apoorva, Yogesh Kumar," Comparative Study of Different Symmetric Key Cryptography Algorithms", International Journal of Application or Innovation in Engineering

[4] & Management (IJAIEM),volume 2,issue 7,July 2013, ISSN 2319 –4847.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
https://www.ijcsjournal.com/ Volume 10, Issue 2, No 7, 2022. ISSN: 2348-6600
Reference ID: IJCS-454 PAGE NO: 3079-3085

[5] Mohit Marwaha, Rajeev Bedi, Amritpal Singh, Tejinder Singh "Comparative Analysis of Cryptographic Algorithms", International Journal of Advanced Engineering Technology, EISSN 0976-3945.

[6] Ms Ankita Umale, Ms Priyanka Fulare, "Comparative Study of Symmetric Encryption techniques for Mobile Data Caching in WMN", The InternationalJournal Of Engineering And Science (IJES).

[7] Monika Agrawal, Pradeep Mishra," A Comparative Survey on Symmetric Key Encryption Techniques", International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 05 May 2012, PP877-882.

[8] An overview of Cryptography www.graykessler.net/library/crypto.html.

[9] What is symmetric Key Cryptography? Webopedia http://www.webopedia.com/terms/symmetric-keycryptography.html.

[10] Symmetric-key – How Stuff Works htttp://computer.howstuffwork.com/encryption2.htm.

M. Kumar and E. G. Dharma, "A comparative analysis of symmetric key encryption algorithm", IJARCET, vol. 3, no. 2, (2014).

[11] O.P Verma, Ritu Agarwal, Dhiraj Dafouti and Shobha Tyagi, "Performance Analysis of Data Encryption Algorithms", IEEE Delhi Technological University, India, 2011.

[12] Brown Lawrie, Steflik Dick, "Symmetric Encryption Algorithm", CS-480b, Lecture slide (ppt).

[13] MajdiAl-qdah& Lin Yi Hui "simple Encryption/Decryption Application" published in

[14] International Journal of computer science and security, volume(1): Issues(1).

[15] Cryptanalysis of a computer cryptography scheme based on a filter bank David Arroyo a,_, Chengqing Li b, Shujun Li c and Gonzalo Alvarez.

[16] Cryptanalysis of an image encryption scheme based on a new total shuffling algorithm David Arroyo a,∗, Chengqing Li b, Shujun Li c, Gonzalo Alvarez a and Wolfgang A. Halang c.

[17] 18Oracevic, A., Dilek, S., & Özdemir, S. (2017). Security in Internet of things: A survey. 2017 International Symposium on Networks, Computers and Communications (ISNCC), (June), 1--6.

[18] Borgohain, T., Kumar, U., & Sanyal, S. (2015). Survey of Security and Privacy Issues of Internet of Things. arXiv Preprint arXiv:1501.02211, 7. Retrieved from http://arxiv.org/abs/1501.02211.

[19] Suo, H., Wan, J., Zou, C., & Liu, J. (2012). Security in the Internet of things: A review. Proceedings - 2012 International Conference on Computer Science and Electronics Engineering, ICCSEE 2012, 3, 648--651.

[20] Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani, "New Comparative Study Between DES, 3DES and AES within Nine Factors", Journal Of Computing, ISSN 2151-9617.