iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** IX **Month of publication:** September 2021

DOI: https://doi.org/10.22214/ijraset.2021.38339

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue IX Sep 2021- Available at www.ijraset.com

A Synoptic View on Network Security and Cryptography

Divya J Nair
Finance Professional, Europcar, Doha, Qatar

Abstract: ***Cryptography is a tool that guards a network and data transmission over a network. Data Security is the core aspect of secure data transmission over untrustworthy network. Network security encompasses the authorization of access to data in a network, which is organized by the network administrator. Users select or are assigned an ID and password or other authenticating information that permits them access to information and programs within their control. Network security covers a wide range of computer networks, both public and private, that are used in ordinary jobs performing transactions and communications among businesses, government agencies and individuals. Networks may be private, such as within a company, or private which allow access to the public. Network security is involved in every type of institutions. In this article we concisely outlined Network security and cryptography along with its basic principles.***
Keywords: Network, Network Security, Cryptography, Asymmetric Cryptosystems, Symmetric Cryptosystems

I. INTRODUCTION

Network Security is a vital element in information security because it is responsible for safeguarding all information passing through networked computers. Network Security refers to all hardware and software functions, characteristics, features, operational procedures, accountability, measures, access control, and administrative and management policy needed to give a standard level of protection for both Hardware and Software , and information in a network. Network security problems can be studied roughly into four closely intertwined areas: Confidentiality, Authentication, Nonrepudiation, and Integrity control.

1) *Confidentiality:* Has to deals with keeping information out of the purview of unauthorized users.
2) Authentication: Deals with defining whom you are talking to, before revealing sensitive information.
3) *Nonrepudiation:* Deals with signatures.
4) *Message Integrity:* Even if the sender and receiver are able to authenticate each other, they also want to insure that the content of their communication is not altered, either deliberately or by accident, in transmission.

In order to prevent the attack of outsiders from the data intrusion, different measures have been adopted. Cryptography is an emerging technology, which is imperative for today's digital world for protecting sensitive information. The widespread use of computerised data storage, processing and transmission makes sensitive, valuable and personal information vulnerable to unauthorised access while in storage or transmission. Due to continuing advancements in communications and eavesdropping technologies, business organisations and private individuals are beginning to protect their information in computer systems and networks using cryptographic techniques. Cryptography is vital for computer and communications networks for protecting everything: such as from business e-mail to bank transactions and internet shopping.
Cryptography consists of two basic processes: encryption and decryption. Encryption is the process of making information unintelligible to the unauthorized reader. Decryption is the process of reversing encryption to make the information intelligible. Cryptography has its origin in the ancient world. The Julius Caesar used simple cryptography to hide the meaning of his messages. Caesar cipher is a mono-alphabetic cryptosystem, since it replaces each given plain text letter, wherever in the original message it occurs, by the same letter of the cipher text alphabet. However the concepts of source and receiver, and channel codes are modern notions that have their ancestries in the information theory. Claude Shannon, in the 1948 provided the information theory basis for secrecy, which defines that the amount of uncertainty that can be introduced into an encoded message can't be greater than that of the cryptographic key used to encode it. Shannon was developed two important cryptographic concepts: confusion and diffusion. The term confusion means to any method that makes the statistical relationship between the cipher-text and the key as difficult as possible, and diffusion is a general term for any encryption technique that expands the statistical properties of the plaintext over a range of bits of the cipher-text.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue IX Sep 2021- Available at www.ijraset.com

II. OBJECTIVE OF THE STUDY

The article is done with the sole objective of briefly outline the basic concept of Network security and cryptography.

III. DATABASE AND METHODOLOGY

This article is exclusively based on secondary data. The secondary data required for the study is obtained from newspapers, periodicals, magazines, journals, websites, books etc.

IV. PRINCIPLES OF CRYTOGRAPHY

1) *Redundancy Cryptographic Principle:* All encrypted messages must contain some redundancy, that is, information not needed to understand the message. Messages must contain some redundancy.
2) *Freshness Cryptographic Principle:* Some method is needed to foil replay attacks. One such measure is including in every message a timestamp valid only for, say, 10 seconds. The receiver can then just keep messages around for 10 seconds, to compare newly arrived messages to previous ones to filter out duplicates. Messages older than 10 seconds can be thrown out.

V. PROCESS OF CRYPTOSYSTEM

Cryptographic systems are used to provide privacy and authentication in computer and communication systems. Encryption algorithms encipher the plaintext, or clear messages, into unintelligible cipher text or cryptograms using a key. A deciphering algorithm is used for decryption or decipherment in order to restore the original information. Cryptography is the science of secret communications. Generally cryptosystems are classified into two classes, depending only on whether the keys at the transmitter and receiver are easily computed from each other:

A. Asymmetric Cryptosystems

In an asymmetric cryptosystem (or public key cryptosystem), there are two different keys used for the encryption and decryption of data. The key used for encryption is kept public and so as called public key, and the decryption key is kept secret and called private key. The keys are generated in such a way that it is impossible to derive the private key from the public key. The transmitter and the receiver both have two keys in an asymmetric system. However, the private key is kept private and not sent over with the message to the receiver, although the public key is.

1) Advantages

a) In asymmetric or public key, cryptography there is no need for exchanging keys, thus eliminating the key distribution problem.
b) The primary advantage of public-key cryptography is increased security: the private keys do not ever need to be transmitted or revealed to anyone.
c) Can provide digital signatures that can be repudiated.

2) Disadvantages

a) A disadvantage of using public-key cryptography for encryption is speed: there are popular secret-key encryption methods which are significantly faster than any currently available public-key encryption method.

B. Symmetric cryptosystems

A symmetric cryptosystem (or private key cryptosystem) uses only one key for both encryption and decryption of the data. The key used for encryption and decryption is called the private key and only people who are authorized for the encryption/decryption would know it. In a symmetric cryptosystem, the encrypted message is sent over without any public keys attached to it.

1) Advantages

a) A symmetric cryptosystem is faster.
b) In Symmetric Cryptosystems, encrypted data can be transferred on the link even if there is a possibility that the data will be intercepted. Since there is no key transmitted with the data, the chances of data being decrypted are null.
c) A symmetric cryptosystem uses password authentication to prove the receiver's identity.
d) A system only which possesses the secret key can decrypt a message.

2) Disadvantages

a) Symmetric cryptosystems have a problem of key transportation. The secret key is to be transmitted to the receiving system before the actual message is to be transmitted. Every means of electronic communication is insecure as it is impossible to guarantee that no one will be able to tap communication channels. So the only secure way of exchanging keys would be exchanging them personally.

b) Cannot provide digital signatures that cannot be repudiated

VI. CRYPTOSYSTEM METHODS

A. Secure Channel

Under this method gatherings provide security of the correspondence channel (provided the magic that is used to scramble those information remains same) Moreover shield those correspondence channel starting with at whatever invasions that might happen on the channel. The primary intention in this system may be with shield the correspondence channel as opposed the magic display for the encryption and unscrambling procedure. This system will be resolved to prevent the correspondence channel starting with At whatever outside strike which Might bargain the encrypted majority of the data continuously exchanged from sender should recipient. To actualize all these efforts to establish safety, might utilize Different systems or calculations. Those the vast majority prominently referred to system is with present exactly character code which will guarantee the sender that those individual who is on collector conclusion is a commissioned pernickety. This technique might be fruitful and might guarantee the authenticity for close discussion continuously conveyed looking into between the two conveying gatherings. This code is accessible on both those conveying gatherings What's more permit each from claiming them will produce a dependable method for verification.

B. Secure Key

Under this technique we give acceptable security to enter that is used to scramble those information (provided those channel that is used to exchange the magic remains same) What's more shield those correspondence channel from any invasions that might happen on the channel. This technique concentrates for safeguarding the way which is the A large portion paramount component in the cryptography methodology. We might attempt to utilize ‘Hybrid Encryption’ and ‘Double Encryption’ idea to guarantee that those facts that secure from persecutors who attempt will attack private data toward retrieving those enter. It may be a prestigious reality that a powerless magic bogs down Indeed those strongest of the calculations with the goal here we might attempt with secure the practically critical component in the transform for cryptography i.e. - the magic. With perform this technique there need aid a lot of people amount of prevailing calculations accessible. Each of these algorithm permits us will furnish extensive variety for security of the magic in play. Each calculation requires its own reductions and additionally drawbacks furthermore give a certain worth of the magic. Those principles keep tabs of these techniques lies on the observation that with the increment in the unpredictability of the key it gets An. Challenge to the invaders to split those ways. These techniques likewise give an exceptional stage for future meets expectations that might be completed around this observation.

VII. CONCLUSION

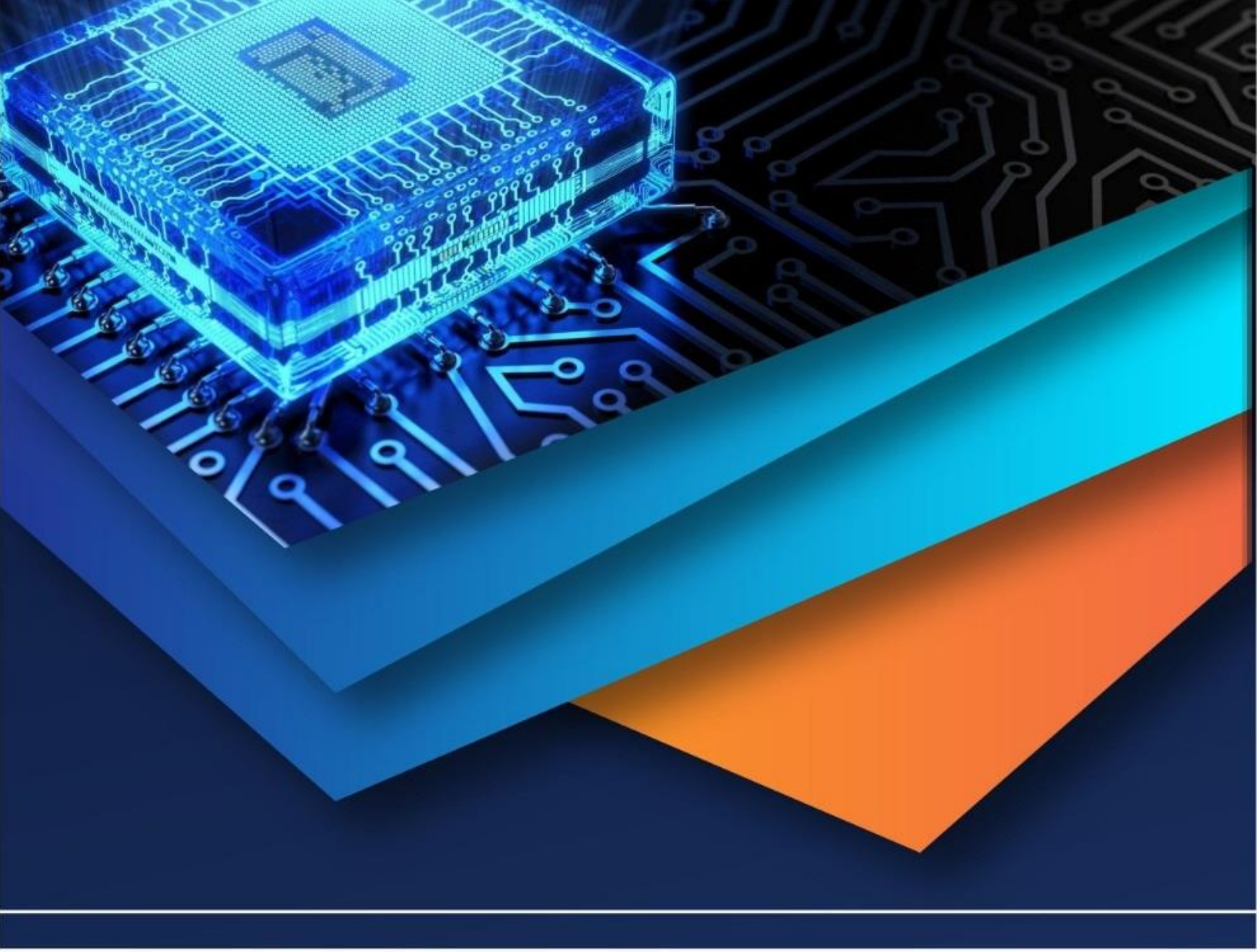
Network Security is the most significant component in information security because it is responsible for securing all information passed through networked computers. Network security comprises of the provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the accessible resources from unauthorized access, and consistent and continuous monitoring and measurement of its effectiveness or lack combined together. Cryptography, together with appropriate communication protocols, can provide a high degree of protection in digital communications against attacks as far as the communication between two different computers is concerned.

REFERENCES

[1] M.Kundalakesi, Devaprakash.A, & Azath.A. (2018). Network Security with Cryptography. IJSRD - International Journal for Scientific Research & Development|, 6(January), 4–6. https://www.researchgate.net/publication/327417301

[2] Mukund R. Joshi, & Karkade, R. A. (2015). Network Security with Cryptography. International Journal of Computer Science and Mobile Computing, 4(1), 201–204.

[3] http://www.uobabylon.edu.iq/eprints/paper_1_2264_649.pdf



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY