iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** II **Month of publication:** February 2015

DOI:

www.ijraset.com

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

ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Network Security: A Study Using Cryptography Techniques

Tushar Gaikwad[1], Mayur Patil[2], Prof. Vijaya Sagvekar[3], Prof. Divya Racha[4]
[1,2]*Student member (Comp),* [3]*Assistant Prof. (Comp),* [4]*Lecturer (Comp), Atharva College of Engineering, Malad(W), Mumbai*

Abstract: ***We are study Network Security refers to all hardware and software functions, characteristics, features, operational procedures, accountability, measures, access control, and administrative and management policy required to provide an acceptable level of protection for Hardware and Software , and information in a network. Only one particular element underlies many of the security mechanisms in use: Cryptographic techniques; hence our focus is on this area Cryptography. Cryptography is an emerging technology, which is important for network security. Research on cryptography is still in its developing stages and a considerable research effort is still required for secured communication.***
Keywords- Network Security, accountability, access control, cryptography, cipher text, encryption, and decryption.

I. INTRODUCTION

Network Security & Cryptography is a concept to protect network and data transmission over wireless network. Data Security is the main aspect of secure data transmission over unreliable network. Data Security is a challenging issue of data communications today that touches many areas including secure communication channel, strong data encryption technique and trusted third party to maintain the database. The rapid development in information technology, the secure transmission of confidential data herewith gets a great deal of attention. The conventional methods of encryption can only maintain the data security. The information could be accessed by the unauthorized user for malicious purpose. Therefore, it is necessary to apply effective encryption/decryption methods to enhance data security. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network

Resource is by assigning it a unique name and a corresponding password. Network security starts with authenticating the user, commonly with a username and a password. Since this requires just one detail authenticating the user name —i.e. the password, which is something the user 'knows'— this is sometimes termed one factor authentication. With two-factor authentication, something the user 'has' is also used (e.g. a security token or 'dongle', an ATM card, or a mobile phone); and with three-factor authentication, something the user 'is' is also used (e.g. a fingerprint or retinal scan). Once authenticated, a firewall enforces access policies such as what services are allowed to be accessed by the network users. Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as computer worms or Trojans being transmitted over the network. Anti-virus software or an intrusion prevention system (IPS) helps detect and inhibit the action of such malware. An anomaly-based intrusion detection system may also monitor the network and traffic for unexpected (i.e. suspicious) content or behaviour and other anomalies to protect resources, e.g. from denial of service attacks or an employee accessing files at strange times. Individual events occurring on the network may be logged for audit purposes and for later high-level analysis .Communication between two hosts using a network may be encrypted to maintain privacy.

II. COMPUTER/NETWORK SECURITY HINGES ON TWO VERY SIMPLE GOALS

A. Keeping unauthorized persons from gaining access to resources
B. Ensuring that authorized persons can access the resources they need

1) Authentication and security: Authentication is an absolutely essential element of a typical security model. It is the process of confirming the identification of a user (or in some cases, a machine) that is trying to log on or access resources. There

are a number of different authentication mechanisms, but all serve this same purpose.

2) *Authentication vs. authorization:* It is easy to confuse authentication with another element of the security plan: authorization. While authentication verifies the user's identity, authorization verifies that the user in question has the correct permissions and rights to access the requested resource. As you can see, the two work together. Authentication occurs first, then authorization.
3) *Logon authentication:* Most network operating systems require that a user be authenticated in order to log onto the network. This can be done by entering a password, inserting a smart card and entering the associated PIN, providing a fingerprint, voice pattern sample, or retinal scan, or using some other means to prove to the system that you are who you claim to be.
4) *Network access authentication:* Network access authentication verifies the user's identity to each network service that the user attempts to access. It differs in that this authentication process is, in most cases, transparent to the user once he or she has logged on. Otherwise, the user would have to re-enter the password or provide other credentials every time he or she wanted to access another network service or resource.
5) *IPSec authentication:* IP Security (IPSec) provides a means for users to encrypt and/or sign messages that are sent across the network to guarantee confidentiality, integrity, and authenticity. IPSec transmissions can use a variety of authentication methods, including the Kerberos protocol, public key certificates issued by a trusted certificate authority (CA), or a simple pre-shared secret key (a string of characters known to both the sender and the recipient). An important consideration is that both the sending and receiving computers must be configured to use a common authentication method or they will not be able to engage in secured communications.
6) *IPSec configuration:* If IPSec policies have been configured to require that communications be secured, the sending and receiving computers will not be able to communicate at all if they do not support a common authentication method.
7) *Authentication types:* There are several physical means by which you can provide your authentication credentials to the system. The most common—but not the most secure—is password authentication. Today's competitive business environment demands options that offer more protection when network resources include highly sensitive data. Smart cards and biometric authentication types provide this extra protection.
8) *Password authentication:* Most of us are familiar with password authentication. To log onto a computer or network, you enter a user account name and the password assigned to that account. This password is checked against a database that contains all authorized users and their passwords. In a Windows 2000 network, for example, this information is contained in Active Directory.

IV. HOW DOES AUTHENTICATION WORK?

In theory, authentication is relatively simple: A user provides some sort of credentials—a password, smart card, fingerprint, digital certificate—which identifies that user as the person who is authorized to access the system. There are, however, multiplicities of methods and protocols that can be used to accomplish this. Regardless of the method, the basic authentication process remains the same.

A. The authentication process

In most instances, a user must have a valid user account configured by the network administrator that specifies the user's permissions and rights. User credentials must be associated with this account—a password is assigned, a smart card certificate is issued, or a biometric scan is entered into the database against which future readings will be compared.

When the user wants to log on, he or she provides the credentials and the system checks the database for the original entry and makes the comparison. If the credentials provided by the user match those in the database, access is granted.

V. CRYPTOGRAPHY

Cryptographic systems are generally classified along 3 independent dimensions:
Type of operations used for transforming plain text to cipher text. All the encryption algorithms are based on two general principles: substitution, in which each element in the plaintext is mapped into another element, and transposition, in which elements in the plaintext are rearranged.

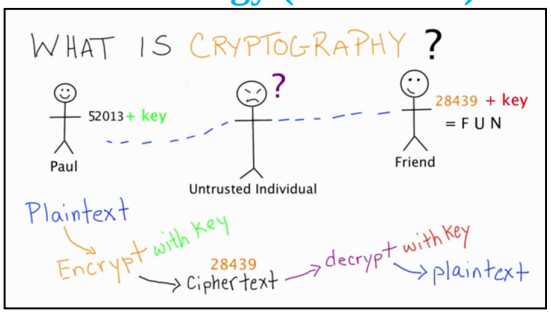


Fig.1 Cryptography

A. The number of keys used

If the sender and receiver uses same key then it is said to be symmetric key (or) single key (or) conventional encryption. If the sender and receiver use different keys then it is said to be public key encryption. The way in which the plain text is processed a block cipher processes the input and block of elements at a time, producing output block for each input block. A stream cipher processes the input elements continuously, producing output element one at a time, as it goes along.

VI. STEGANOGRAPHY

A plaintext message may be hidden in any one of the two ways. The methods of steganography conceal the existence of the message, whereas the methods of cryptography render the message unintelligible to outsiders by various transformations of the text. A simple form of steganography, but one that is time consuming to construct is one in which an arrangement of words or letters within an apparently innocuous text spells out the real message. e.g., (i) the sequence of first letters of each word of the overall message spell out the real (Hidden) message. (ii) Subset of the words of the overall message is used to convey the hidden message. Various other techniques have been used historically, some of them are Character marking – selected letters of printed or typewritten text are overwritten in pencil. The marks are ordinarily not visible unless the paper is held to an angle to bright light. Invisible ink – a number of substances can be used for writing but leave no visible trace until heat or some chemical is applied to the paper. Pin punctures – small pin punctures on selected letters are ordinarily not visible unless the paper is held in front of the light. Typewritten correction ribbon – used between the lines typed with a black ribbon, the results of typing with the correction tape are visible only under a strong light.

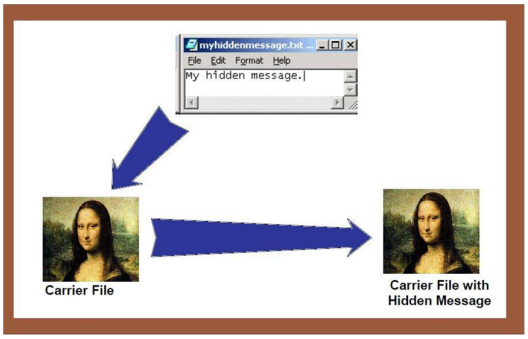


Fig.2 Steganography

A. Drawbacks of steganography

Requires a lot of overhead to hide a relatively few bits of information. Once the system is discovered, it becomes virtually worthless.

VII. DATA ENCRYPTION STANDARD (DES)

In May 1973, and again in Aug 1974 the NBS (now NIST) called for possible encryption algorithms for use in unclassified government applications response was mostly disappointing, however IBM submitted their Lucifer design following a period of redesign and comment it became the Data Encryption Standard (DES) it was adopted as a (US) federal standard in Nov 76, published by NBS as a hardware only scheme in Jan 77 and by ANSI for both hardware and software standards in ANSI X3.92-

1981 (also X3.106-1983 modes of use) subsequently it has been widely adopted and is now published in many standards around the world cf Australian Standard AS2805.5-1985 one of the largest users of the DES is the banking industry, particularly with EFT, and EFTPOS it is for this use that the DES has primarily been standardized, with ANSI having twice reconfirmed its recommended use for 5 year periods - a further extension is not expected however although the standard is public, the design criteria used are classified and have yet to be released there has been considerable controversy over the design, particularly in the choice of a 56-bit key.

VIII. THE ADVANCED ENCRYPTION STANDARD (AES)

On January 2, 1997, the United States' National Institute of Standards and Technology (NIST) announced the initiation of a new symmetric-key block cipher algorithm as the new encryption standard to replace the DES. The new algorithm would be named the Advanced Encryption Standard (AES). Unlike the closed design process for the DES, an open call for the AES algorithms was formally made on September 12, 1997. The call stipulated that the AES would specify an unclassified, publicly disclosed symmetric-key encryption algorithm(s); the algorithm(s) must support (at a minimum) block sizes of 128-bits, key sizes of 128-, 192-, and 256-bits, and should have a strength at the level of the triple DES, but should be more efficient then the triple DES. In addition, the algorithm(s), if selected, must be available royalty-free, worldwide.

IX. CATEGORIES OF ATTACK

This section will discuss how a hacker can perform an attack on a network.

A. Passive attack Passive attacks also know as reconnaissance attack is the first step the hacker takes in order to perform hacking. During this phase, the hacker tries to gather information with the aid of packet sniffing, scanning active ports or performing ping scans to see what IP addresses are active around the networks. This is the initial phase of hacking and usually it is very difficult to detect any such activity.

B. Active attacks after a passive attack, an intruder has enough information about active ports, IP addresses around the network and also have queried enough to launch an active (access) attack. In this phase, the attacker usually performs “Man in the Middle” attack. Man in the Middle attack is one of the most dangerous attacks and resides in the midway communication between the gateway and the client. It is transparent in nature, hence eliminating the possibility of it being detected while it sniffs sensitive data. Trust exploitation and password attacks also fall in this category.

X. WHAT ARE THE DIFFERENT WIRELESS NETWORK SECURITY METHODS?

Wi-Fi Protected Access encrypts information and makes sure that the network security key has not been modified. Wi-Fi Protected Access also authenticates users to help ensure that only authorized people can access the network.

1. There are two types of WPA authentication: WPA and WPA2. WPA is designed to work with all wireless network adapters, but it might not work with older routers or access points. WPA2 is more secure than WPA, but it will not work with some older network adapters. WPA is designed to be used with an 802.1X authentication server, which distributes different keys to each user. This is referred to as WPA-Enterprise or WPA2-Enterprise. It can also be used in a pre-shared key (PSK) mode, where every user is given the same passphrase. This is referred to as WPA-Personal or WPA2-Personal.

2. WEP is an older network security method that's still available to support older devices, but it's no longer recommended. When you enable WEP, you set up a network security key. This key encrypts the information that one computer sends to another computer across your network. However, WEP security is relatively easy to crack.

3. 802.1X authentication can help enhance security for 802.11 wireless networks and wired Ethernet networks. 802.1X uses an authentication server to validate users and provide network access. On wireless networks, 802.1X can work with WPA, WPA2, or WEP keys. This type of authentication is typically used when connecting to a workplace network.

XI. WHY IS NETWORK SECURITY IMPORTANT?

A. The good neighbour policy.

Your mistakes can be someone else’s headaches. If your network is insecure and someone takes control of one of your computers, they can use that machine to launch denial of service attacks on innocent third parties. They can also flood the Web

with spam.

B. Patron privacy. Obviously,

Patron records are of paramount importance. Trust between the library and its clients can be irreparably harmed if these records are compromised.

C. Money and time.

Tracking down a virus or a worm and eliminating it from your network is frustrating and time--consuming. You often have to rebuild your machines from the ground up, re-installing the operating system and software and restoring data from backup tapes. Lax security can lead to weeks of wasted time spent patching your network and fixing the wreckage.

XII. SERVICES FOR SECURITY

The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

A. Confidentiality

Ensure that the information in a computer system and transmitted information are accessible only for reading by authorized parties. This type of access includes printing displaying and other forms of disclosure, including simply revealing the existence of an object.

B. Authentication

Ensure that the origin of a message or electronic document is correctly with an assurance that the identity is not false;

C. Integrity

Ensures that only authorized parties are able to modify computer systems assets and transmitted information. Modification includes writing, changing, changing status, deleting, creating and delaying or replaying of transmitted messages.

D. Non-repudiation

Requires that neither the sender nor the receiver of a message is able to deny the transmission

E. Access control

Require that access to information resources may be controlled by or for the target system.

F. Availability

Require that computer systems assets be available to authorized parties when needed.

XIII. SECURITY TO KEEP INTRUDERS OUT

Network managers need to provide end users with freedom and mobility without offering intruder's access to the WLAN or the information sent and received on the wireless network. With a WLAN, transmitted data is broadcast over the air using radio waves that travel between client devices, or stations, and access points-the WLAN endpoints on the Ethernet network that link stations to the network. This means that any WLAN client device within an access point service area can receive data transmitted to or from the access point.

Because radio waves travel through ceilings, floors, and walls, transmitted data may reach unintended recipients on different floors or even outside the building that houses the access point. With a WLAN, the boundary for the network has moved. Without stringent security measures in place, installing a WLAN can be the equivalent of putting Ethernet ports everywhere, including in the parking lot.

Additionally, several research papers and articles have highlighted the vulnerabilities of Wired Equivalent Privacy (WEP) keys used to encrypt and decrypt transmitted data. Intruders have ready access to tools for cracking WEP keys, such as Air-Snort, which enables an attacker to passively monitor and analyze packets of data and then use this information to break the WEP key that encrypts the packets.

XIV. TRENDS IN THE FUTURE OF SECURITY: WHAT'S COMING?

A. *Economic Information Warfare (EIW),* consisting of sophisticated attacks against entire economies, commerce and enterprises will accelerate as a global threat.
B. *Smart Watchers,* a new generation of super-sensitive satellite and video networked electronic surveillance, will be everywhere. Real-time personal face scanning and suspicion profiling tied to massive supercomputers, sensory-aware networks and data warehouses will determine risks, provide prevention strategies and intelligence on neutralizing threats .
C. *National Identity Cards* with embedded smart chips, containing an individual's entire Genomic Profile will act as a secure personal identifier. They will wirelessly authenticate an individual's location, security clearance level and identity to a sea of intelligent networks tied to government, transportation, banking, telecom and enterprises.
D. *Pandora,* the next generation of computer virus attacks, will be self-mutating viruses created to destabilize, confuse and destroy critical electronic infrastructures essential to industry and government. These will be used as offensive and defensive weapons by all sides.
E. *Sniffers* designed to automatically sense, watch, and search and identify individual s with critical information; weapons or bombs will have the capability to navigate physical, wireless and electronic realities.
F. *Secure-* Wearable that are embedded, pinprick size hyper-sensing bio-reactive nano-chips, personal pin codes and GPS location monitoring will assist in security tracking, and recovery after kidnapping or theft.
G. *DEPS, Digitally Engineered Personalities,* personal sensors that live in the global telecom Internet network and provide 24/7 follow-you-anywhere security protection for individuals, enterprises and governments, will be necessary and in demand.
H. *Biometric Authentication:* facial, eye, fingerprint and genomic scanning will be necessary to validate an individual's physical or virtual entry into electronic networks o r physical areas. Security Tattoos with bar-scans will be popular and fashionable.
I. *Biowar and Agri*-Terrorism targeting the destruction of targeted ecosystems will emerge as common threats putting at risk public health, soil, food, water resources.
J. *Numerous* personal privacy violations will occur, requiring new laws to protect and preserve individual freedoms.

XV. SECURITY AND PRIVACY

A. *Identity management* Every enterprise will have its own identity management system to control access to information and computing resources. Cloud providers either integrate the customer's identity management system into their own infrastructure, using federation or SSO technology, or provide an identity management solution of their own.
B. *Physical security* Cloud service providers physically secure the IT hardware (servers, routers, cables etc.) against unauthorized access, interference, theft, fires, floods etc. and ensure that essential supplies (such as electricity) are sufficiently robust to minimize the possibility of disruption. This is normally achieved by serving cloud applications from 'world-class' (i.e. professionally specified, designed, constructed, managed, monitored and maintained) data canters.
C. *Personnel security* Various information security concerns relating to the IT and other professionals associated with cloud services are typically handled through prepaid and post-employment activities such as security screening potential recruits, security awareness and training programs, proactive security monitoring and supervision, disciplinary procedures and contractual obligations embedded in employment contracts, service level agreements, codes of conduct, policies etc.
D. *Availability* Cloud providers help ensure that customers can rely on access to their data and applications; at least in part (failures at any point - not just within the cloud service providers' domains - may disrupt the communications chains between users and applications).
E. *Application security* Cloud providers ensure that applications available as a service via the cloud (SaaS) are secure by specifying, designing, implementing, testing and maintaining appropriate application security measures in the production environment. Note that - as with any commercial software - the controls they implement may not necessarily fully mitigate all the risks they have identified, and that they may not necessarily have identified all the risks that are of concern to customers. Consequently, customers may also need to assure themselves that cloud applications are adequately secured for their specific purposes, including their compliance obligations.
F. *Privacy* Providers ensure that all critical data (credit card numbers, for example) are masked or encrypted (even better) and that only authorized users have access to data in its entirety. Moreover, digital identities and credentials must be protected as should any data that the provider collects or produces about customer activity in the cloud.

XVI. CONCLUSIONS

Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. Discuss on various study papers and reference books to understand network security with Cryptography. Studied various concepts related to network security. We have studied various cryptographic techniques to increase the security of network.

REFERENCES

[1]Modern Cryptography: Theory and Practice By Wenbo Mao Hewlett-Packard Company Publisher: Prentice Hall PTR Pub Date: July 25, 2003 ISBN: 0-13-066943-1 Pages: 648

[2]Volume 2, Issue 12, December 2012 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering.

[3]Cryptography and Network Security Principles and Practices, Fourth Edition By William Stallings Publisher: Prentice Hall Pub Date: November 16, 2005

[4]Sanchez-Avila, C. Sanchez-Reillol, R, ―The Rijndael block cipher (AES proposal): A comparison with DES‖, 35th International Conference on Security Technology 2001, IEEE.

[5]Murat Fiskiran, Ruby B. Lee, ―Workload Characterization of Elliptic Curve Cryptography and other Network Security Algorithms for Constrained Environments‖, IEEE International Workshop on Workload Characterization, 2002. WWC-5. 2002.

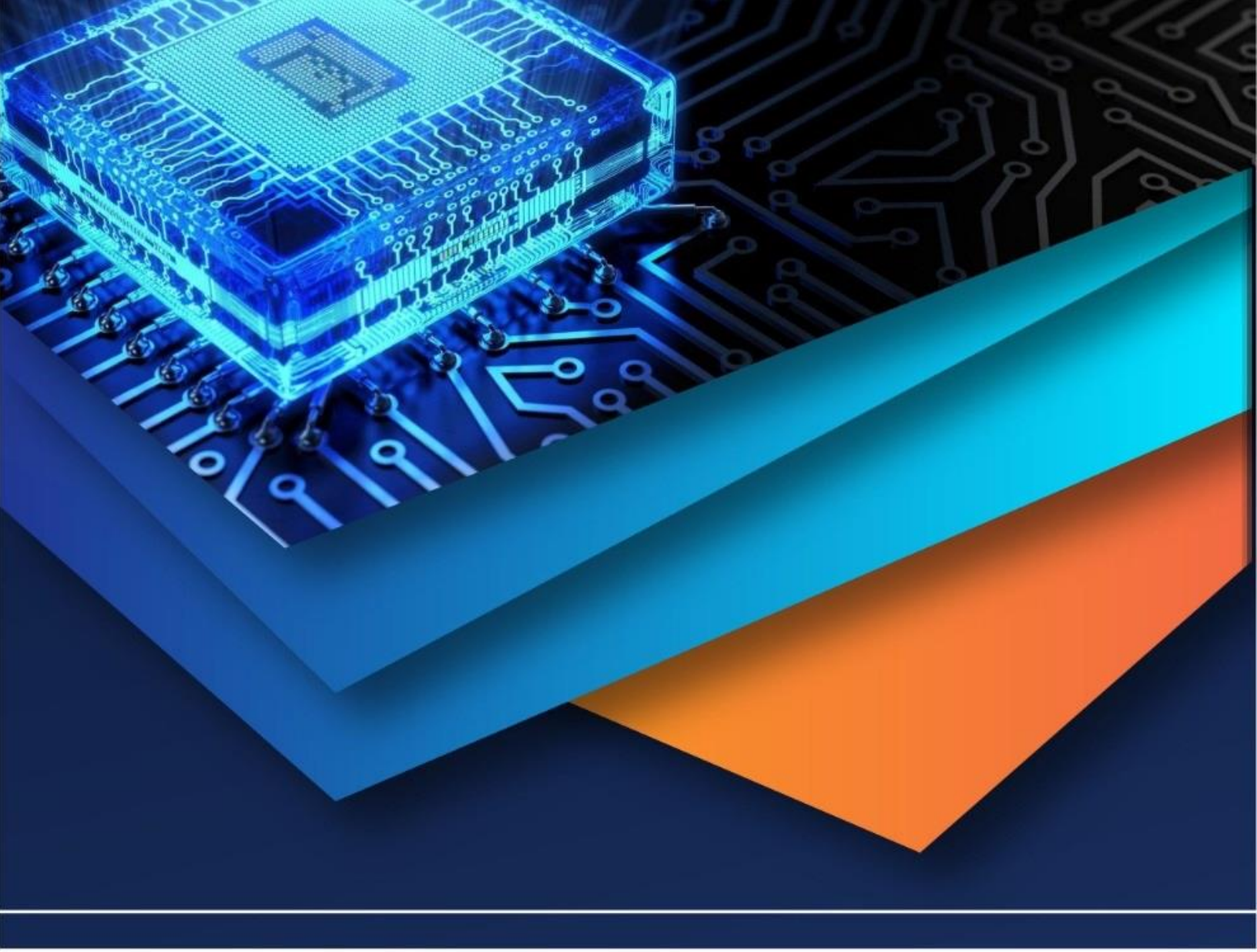
[6]Aameer Nadeem, Dr. M.Younus Javed, ―A performance comparison of data Encryption Algorithm‖, Global Telecommunication Workshops, 2004 Globe Com Workshops 2004, IEEE.

[7]Study of Network Security along with Network Security Tools and Network Simulators Amanpreet Kaur , Monika Saluja CSE Department.SBSCET,Fzr (Pb,India)

[8](IJIRSE) International Journal of Innovative Research in Science & Engineering ISSN (Online) 2347-3207 Network Security: it's time to take it seriously.

[9]Deepak Gahlot, Abhimanyu Thakur, Akshat Pokhriyal, Divyanshu Kukreti Students, Dronacharya College of Engineering Gurgaon, India

[10]ISSN: 2321-8134 international journals for engineering applications and technology. Title: Review Paper on Network Security and Related issues Mr. Mukesh K. Deshmukh1, Prof . Ajay B. Gadicha2



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY