Modern Network Security: Analysis, Vulnerability and Countermeasures

Mr. Balaji G.M
Department of MCA
Surana College, Kengeri
balajigm292@gmail.com

Mr. Pavana D
Department of MCA
Surana College, Kengeri
pavan07sagar@gmail.com

Mr. Veeresh K
Department of MCA
Surana College, Kengeri
veeresh1216v@gmail.com

Dr. Balaji K
Professor/HOD
Department of MCA
Surana College, Kengeri
balaji.mca@suranacollege.edu.in

***Abstract*—Network Security is a critical aspect of modern information technologies. The initial and the most important aspect of any network design, planning, construction, and operation is the significance of a solid security strategy. Network security has grown increasingly critical to individual computer users, businesses, and governments, as well as the military. With the introduction of the internet, security has become a big problem. The structure of the internet has made several security threats possible. Network security is becoming more crucial because of the ease with which intellectual property can be obtained online. When an attack is sent via a network, it can take several forms. Many organisations use firewalls and encryption methods to protect themselves from the internet. In this research, we attempt to investigate numerous types of assaults as well as various types of security mechanisms that might be applied based on the network's needs and architecture.**

***Index Terms*—Network Security, Attacks, Data Breaches, NGFW(Next generation Firewall), Unauthorised access, Cryptography, Zero-trust model ,Mitigation Strategies, Security Policies ,Secure Socker Layer(SSL)**

I. Introduction

Network security is a method that prevents messages and data from falling into the hands of malicious individuals. Public and private computer networks that are used in daily business activities, such as completing transactions and facilitating communications between businesses, governmental organisations, and individuals, are all included in the scope of network security. Private networks, such as those within a firm, can exist alongside public networks. Companies, corporations, and other forms of institutions are all concerned about network security. It performs exactly what its name implies: it secures the network while also protecting and monitoring operations. In this research paper different research papers are consulted in order to define the security model architecture. The paper discusses the different difficulties involved with network security, as well as the analysis of network threats and attacks. It also discusses the numerous implementation tactics used to maintain network security. The study also focuses on the architectural design to handle data flow and load, as well as offering access control measures to assure service quality.

II. Background and Significance of Network Security

The network model is critical in the world of computer networking and is very important. Here are some of the main reasons why the network model is important:

A. Conceptual Framework

The network model provides a conceptual framework for understanding and visualising how various devices, protocols, and technologies are interconnected to enable communication and data transfer inside a network. It enables network administrators and engineers to properly plan, design, and deploy networks.

B. Standardization

Network models, like the TCP/IP model and the OSI (Open Systems Interconnection) model, provide a common method for designing networks. It defines a collection of protocols and services that permit interaction between various network devices and systems. Standardisation enables diverse manufacturers to create networking devices that are compatible with one another, ensuring seamless communication and integration across heterogeneous networks.

C. Troubleshooting and Problem Solving

The network model offers a methodical way to troubleshooting network difficulties. It is easier to isolate and identify the core cause of problems when the network architecture is divided into various levels or components. To rapidly detect and address issues, network administrators might use an organised troubleshooting procedure based on the network model.

Different sorts of Architectures can be considered when creating a network model based on computational requirements. Some of them are as follows:

- Personal Area Network (PAN) - A network organised around an individual with any connecting device such as a mobile phone or any other handled device.
- Storage Area Network- The Storage Area Network (SAN) connects storage devices to the server. It provides storage that is accessible to the programme executing on the networked server.
- System Area Network - Also known as Clustered Area Network, this network connects computers and provides high-speed connections and settings.

III. Scope and Objectives of the Research

The scope of this research is to provide a complete analysis of internet via threats in network security and propose an effective countermeasures. The research has some following objectives:

- Network Infrastructure: The scope of network security includes securing the network infrastructure, including routers, switches, firewalls, and other network devices.
- Data Security: Protecting the confidentiality, integrity, and availability of data transmitted over the network through encryption, data loss prevention (DLP), and secure data storage mechanisms.
- Wireless Network Security: Extending security measures to wireless networks, including Wi-Fi networks, by implementing strong authentication, encryption, and intrusion detection mechanisms.
- Incident Response and Recovery: Establishing processes and procedures to respond to and recover from security incidents effectively, minimizing the impact on network operations and restoring normalcy.
- Confidentiality: Protecting sensitive information from unauthorized access or disclosure by implementing encryption, access controls, and secure transmission mechanisms.
- Integrity: Ensuring the integrity of data by preventing unauthorized modifications or alterations through data validation, integrity checks, and secure storage mechanisms.
- Availability: Ensuring network resources and services are accessible to authorized users when needed, protecting against denial of service (DoS) attacks, and implementing redundancy and fault tolerance measures.

IV. NGFW Most recently Network Attacks in 2021

Confidential information is frequently sent between networks in modern organisations that rely on the internet for communication. Additionally, remote accessibility gives unscrupulous parties access to susceptible targets for data eavesdropping. These might infringe on users' personal settings and jeopardise online-connected gadgets.

- N01:2022- DDoS (distributed denial of service) strike necessitate the use of massive networks of connected, malware-infected machines known as "botnets." These overburden organisations servers with erroneous traffic. Time-sensitive data, like that of healthcare facilities, may be the target of malicious attackers, disrupting access to crucial tolarent database records.
- N02:2022- Man-in-the-middle Attacks When malevolent actors eavesdrop on communication between networks and outside data sources or between networks themselves, network assaults happen. Man-in-the-middle attacks are typically carried out by hackers by taking advantage of holes in security protocols. As a result, hackers are able to pretend to be a relay or proxy account and change data during real-time transactions.
- N03:2022-Unauthorized access is a term used to describe network attacks in which malevolent actors access corporate assets without authorization. Such incidents may happen as a result of lax password security for accounts, unprotected networks, internal menaces that exploit role powers, and the abuse of lethargic roles with authority rights.
- N04:2022- SQL Injection sonsumate user data inputs could be place in management networks at risk of SQL injection raid. The network attempt method involves outside parties providing harmful codes in place of legitimate data values to alter forms. They break into the network and gain access to private information like user passwords. SQL injection techniques involve scanning databases to learn about their variant and design as well as subverting application-layer logic, causing problems with its operation and logic sequences.
- N05:2022- Persistent Advanced Threats in network offense, a group of expert cyberpunks may employ advanced persistent threats (APTs). Planning and carrying out a sophisticated cyberattack programme will be done by APT parties. This circumvents network security mechanisms like trap door and spyware software by exploiting a number of network flaws.
- N06:2022-Ransomware During ransomware threats, spiteful parties encrypt data access routes while withholding the decryption keys, enabling hackers to threaten the affected businesses. The most prevalent payment methods are anonymous cryptocurrency results. In the time cybersecurity experts warn against paying off adversaries, some businesses nonetheless do have temporary workaround for regaining access to data.
- N07:2022-Social Engineering In 15% of cases where parties have been compromised, social engineering has been used as a means of infiltration, based on to ISACA's State of Cybersecurity 2020 Report. Phishing is a clever treason and fraudulence technique used in social engineering to get access to users' personal information by playing on their emotions and trust.
- N08:2022: A buffer overflow attack happens when a hacker sends an application more data than is necessary. By using a command prompt or shell, an attacker can typically get administrative access to the system as a result of a buffer overflow attack.
- N09:2022- Attack with an exploit in this form of attack, An operating system or piece of software has a security hole that the attacker is aware of and employs to his or her advantage.
- N10:2022- Phishing Scheme In a phishing attack, The hacker makes a fake website that impersonates a well-known one, like PayPal or SBI Bank. The hacker then sends the victim an email message in an effort to trick them into clicking a link that takes them to the fake website. The hacker stores the username and password when a user tries to log in with their account details and then tries to log in on the real site using those credentials.

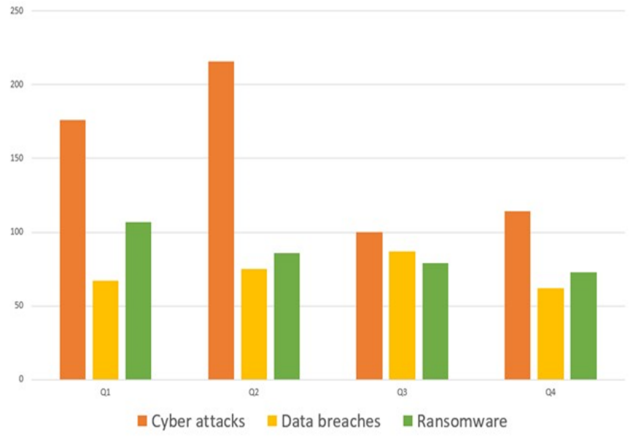

Fig. 1. Attack score of 3 main threats between (2019-2022)

V. Threats and Consequences in Network Security

The repercussions and impact of network security can be significant and far-reaching. Here are some important factors to consider:

- Secret Information Protection: Network security techniques such as encryption and access controls aid in the protection of sensitive and secret information against unauthorised access or exposure. A network security breach can expose proprietary data, personal information, financial details, or trade secrets. Financial loss, reputational damage, legal liability, and loss of customer trust are all possible outcomes.
- Individual Impact: Network security incidents can have a direct impact on individuals. Phishing attacks, identity theft, or unauthorised access to personal devices connected to the network, for example, can result in financial loss, invasion of privacy, and personal reputation damage.
- Malicious security software: Have you ever seen a pop-up window promoting a security update or alert? It appears authentic and requests that you click on a link to install the ”update” or ”remove” undesirable malicious software that it claims to have discovered. It’s possible that this is rogue security software designed to trick consumers into clicking and downloading harmful software.
- Intellectual Property Protection: Network security is essential for protecting intellectual property (IP). Organisations invest considerably in R&D, and a breach in network security can result in intellectual property theft, industrial espionage, or unauthorised access to private information. Financial losses, a loss of competitive edge, and probable legal fights are all possible outcomes.
- Trust and customer confidence: Network security is critical in establishing and sustaining trust with customers, partners, and stakeholders. When businesses show a commitment to preserving client data and maintaining a secure online environment, it boosts customer trust in their products or services. Security breaches, on the other hand, destroy trust, resulting in consumer loss, reputational damage, and potential legal ramifications.

VI. Countermeasures and Techniques of Network Security

Network security countermeasures and strategies are used to minimise risks and safeguard network infrastructure, data, and services against unauthorised access, breaches, and attacks. Here are some examples of frequent countermeasures and techniques

A. Firewalls

Firewalls operate as a barrier between an internal network and external networks, managing incoming and outgoing network traffic based on security policies that have been set. They aid in the prevention of unauthorised access and the filtering of harmful traffic.

B. Intrusion Detection and Prevention Systems (IDS/IPS)

IDS/IPS systems analyse network traffic for suspicious or malicious activity. IDS systems detect possible threats, whereas IPS systems respond quickly to stop or prevent those threats from affecting the network.

C. Virtual Private Networks (VPNs)

VPNs provide a secure and encrypted connection over a public network, such as the internet, allowing remote users to securely access a private network. VPNs ensure data secrecy and security while in transit.

D. Security Information and Event Management (SIEM)

SIEM is for Security Information and Event Management, and it is a system that collects and analyses logs and events from various network devices and systems in order to detect and respond to security incidents. For efficient security management, they provide real-time monitoring, threat intelligence, and centralised log management.

E. Security Policies and Procedures

Creating and implementing comprehensive security policies and procedures aids in the development of rule, standards and protocols for secure network use. It ensures organization-wide uniformity, accountability, and adherence to security standards.

VII. Some Advance Network Security Policies

A. Making Security in Clouds Environment

Making Cloud Security Analysts predict that IT spending will grow marginally from 2013. Cloud computing is largely responsible for this rise in investment [10]. More than half of IT organisations intend to boost their cloud computing investment in order to improve the flexibility and efficiency of their IT resources. Intel Trusted Execution Technology (Intel TXT) is specifically developed to protect platforms in virtual and cloud settings against hypervisor, firmware, BIOS, and system level threats.

B. Zero-Trust Segmentation Adoption

This approach was created by Forrester Research's John Kindervag and popularised as a required progression of old overlay security models. The zero-trust model (ZTM) is one promising solution for improving security. This aggressive approach to network security monitors every available piece of data, assuming that every file is a potential threat [11]. It necessitates that all resources be accessed securely, with access control based on need-to-know and strictly enforced. The systems must verify and never trust; every traffic must be scrutinised, logged, and evaluated; and systems must be created from the inside out rather than the outside in.

C. Advanced Threat Protection with Big Data

Big Data makes sense for security because it includes the use of specialised technology and procedures to collect, organise, store, and analyse genuinely vast amounts of linked and sometimes disparate data in order to reveal insights and patterns that would otherwise be obscured. Using Big Data for information security is not only logical, but also required [14]. Big Data analytics can help with information security and situational awareness. Big Data analytics, for example, can be used to analyse financial transactions, log files, and network traffic for anomalies and suspicious activity, as well as to connect many sources of information into a cohesive view.

VIII. Network Security Frameworks and Libraries

- The National Institute of Standards and Technology (NIST) developed the NIST Cybersecurity Framework, which provides a risk-based approach to monitoring and strengthening cybersecurity. It has five primary functions: identify, protect, detect, respond, and recover. The framework assists organisations in assessing their present security posture, identifying gaps, and putting suitable security measures in place.
- ISO/IEC 27001: This international standard establishes, implements, maintains, and constantly improves an information security management system (ISMS). It addresses a variety of network security issues, such as risk assessment, controls, monitoring, incident response, and compliance.
- SANS Critical Security Controls: This framework, developed by the SANS Institute, provides a prioritised set of security controls to assist organisations in defending against prevalent cyber attacks. It is primarily concerned with network security policies, vulnerability management, secure settings, and incident response.
- ITIL: The Information Technology Infrastructure Library (ITIL) is a widely used framework for managing IT services. It does not expressly address network security, but it does provide advise on incorporating security into service management processes, incident management, and change management.

IX. What An Organisation Must Do?

- The organisation should be prepared to deal with the organization's growth, which would necessitate new network enhancements in terms of both applications and scale.
- They must plan security in accordance with changing requirements, which may include issues such as remote and thirdparty access.
- Hackers' new playground is the application layer, rather than the network layer. Attack prevention systems must safeguard the network, services, and applications, as well as providing a secure office connection, secure remote employee access, resilient network availability, and regulated Internet access.
- The optimal solution for internal security difficulties is not only a traditional security product, but it must also contain threats (such as worms), split the network, and secure the desktop, server, and network infrastructure.

Conclusion

In these research paper we inspect that, network security is an important part of current technology design. The need of effective network security measures cannot be focused as organisations increasingly rely on networks to communicate and store sensitive information, secure valuable assets, and preserve operational continuity. Network security breaches can have serious implications, including financial losses, reputational damage, legal liability, and erosion of consumer trust. To prevent threats and protect their digital assets, organisations must invest proactively in network security countermeasures and approaches. By adopting network security frameworks such as NIST, ISO/IEC 27001, CIS Controls, or PCI DSS, organisations can build a structured approach to network security management. Continuous monitoring, regular updates, and ongoing education are critical for maintaining a solid network security posture in an ever-changing threat scenario. Organisations must keep up with developing threats, install appropriate security policies, conduct vulnerability assessments, and test their network defences on a regular basis.

References

[1] NGNF Cyber Research, "Next-Generation Firewall,"*Zscaler*, Available:https://www.zscaler.com/resources/securityterms-glossary/what-is-next-generation-firewall
[2] Bhavya Daya, "Network Security: History, Importance, and Future," *University of Florida Department of Electrical and Computer Engineering*
[3] Intel Corporation, "Securing the Intelligent Network," *White Paper*
[4] G.A. Marin, "Network security basics," *Security & Privacy*, IEEE, vol. 3, no. 6, pp. 68-72, Nov.-Dec. 2005.
[5] J. Daemen and V. Rijmen, "Rijndael: AES-The Advanced Encryption Standard," *Springer*, Heidelberg, March 2001.
[6] R. Anderson and M. Roe, "Network Security: The Complete Reference," A5, 1994.
[7] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 2nd edition, Prentice Hall, 1999.

[8] C.J. Kolodgy and C.A. Christiansen, "Network Security Overwatch Layer: Smarter Protection for the Enterprise," Sponsored by: Trend Micro, November 2009.
[9] "Network Security Types of attacks," [Online]. Available:standards-and-extended/types-of-attack.html
[10] "Network Security," [Online]. Available: https://en.wikipedia.org/wiki/Network$_security$
[11] O. Adeyinka, "Internet Attack Methods and Internet Security Technology," in *Modeling & Simulation*, 2008. AICMS 08. Second Asia International Conference on, vol., no., pp. 77-82, 13-15 May 2008.