ICCSE'21 International Conference on Contemporary approach on revolutionary Science and Engineering, April 9-10, 2021 ISBN: 978-81-910765-1-6

Network Security

Prof.UTHRADEVI, A.SURYA[1], M.RANJITH[2],V.AKASH[3]
Professor, Department of Information Technology, Indra Ganesan College of Engineering,uthra.ud@gmail.com
[1]Student, Department of Information Technology, Indra Ganesan College of Engineering,suryahope3@gmail.com
[2]Student, Department of Information Technology, Indra Ganesan College of Engineering,ranjithmani029@gmail.com
[3]Student, Department of Information Technology, Indra Ganesan College of Engineering,akashthiyagu22@gmail.com

ABSTRACT:

"SECURITY" in this contemporary scenarios has become a more sensible issue either it may be in the "REAL WORLD" or in the "CYBER WORLD". Network Security 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. 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. 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.

CONTENTS:

INTRODUCTION: Nowadays many people are interacting with the world of internet and the sense of security is enhancing day by day.
So, everyone needs to know about the basics of network security so that each and everyone can protect their network. The network security has the features like not allowing the unauthorized access, protecting your vital data and guarantees the interruption less service.
Network security is defined as an activity designed to secure the usability and integrity of the network and information.

It includes both the hardware and software applied sciences, its function is about targeting the various threats and blocking them from entering into the network and spreading in the network. The digital network has brought a revolution in everyone's life and the way of people's living, working, playing and learning

 ISBN: 978-81-910765-1-6

has changed and network security plays an important role in defending the personal dataof the people.

WHAT IS NETWORK SECURITY?

Network security is the security provided to a network from unauthorized access and risks. It is the duty of network administrators to adoptpreventive measures to protect their networks

from potential security threats.

Computer networks that are involved in regular transactions and communication within the government, individuals, or business require security. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

HISTORY OF NETWORK SECURITY :

Computers started being networked with one another in the late 80s. At that time, there became an increased concern for security, though it was minimal in comparison to today's concerns. That is why understanding the history of network security can help us grasp how important it is today. This is especially true given the number of potential cyber attacks that happen worldwide. Please note, that before the 90s, the concept of having a network of computers was fairly uncommon. And, there was a considerably small number of people in the populace who even had access to the internet. So, security at that time was really not a major concern or focus. But, as more and more sensitive information became accessible, the import of network security increased significantly. The internet was actually called the Arpanet back in the 70s and 80s. And, researchers fueled their downtime with practical jokes played online. While they amused one another with these antics, they also served an important purpose. The jokes played on the Arpanet revealed the flaws in the network security of that time. While the risk was minimal because these jokers all knew one another professionally, it was still very revelatory. During that period in this technological revolution, some serious violations occurred. War Games, the movie, popularized the concept of "hackers." And since the violations were high profile, this term has remained an important part of network security design. Hackers are dangerous individuals who seek to gain access to sensitive or personal information over the internet. Sometimes their plans are even more heinous. Network security exists to stop them.

Network security secures the network of the organization or firm that is furnishing the required services to the customers and their employees. Along with that, network security aids to secure the proprietary data from attack and finally it secures the reputation of the people. In the year of 1996, we had 13 million users of internet experienced programs who had the ability to exploit the network but coming to the present situation everyone can play the role of a hacker by downloading software from the internet.

NEED FOR NETWORK SECURITY:

In the past, hackers were highly skilled programmers who understood the details of computer communications and how to exploit vulnerabilities. Today almost anyone can become a hacker by downloading tools from the Internet. These complicated attack tools and generally open networks have generated anincreased need for network security and dynamic security policies.

The easiest way to protect a network from an outside attack is to close it off completely from the outside world. A closed network provides connectivity only to trusted known parties and sites; a closed network does not allow a connection to public networks.

Because they have no Internet connectivity, networks designed in this way can be considered safe from Internet attacks.

However, internal threats still exist. There is a estimates that 60 to 80 percent of network misuse comes from inside the enterprise wherethe misuse has taken place.With the

 ISBN: 978-81-910765-1-6

development of large open networks, security threats have increased significantly in the past 20 years. Hackers have discovered more network vulnerabilities, and because you can now download applications that require little or no hacking knowledge to implement, applications intended for troubleshooting and maintaining and optimizing networks can, in the wrong hands, be used maliciously and pose severe threats.

NETWORK ATTACKS METHODS:

Whiteout implemented security measures and controls in place, your network and data might be subjected to an attack. Some attacks for instance could be passive, meaning that information is monitored; other could be active, meaning the information is varying within intent to destroy or corrupt the data or the network itself.

Likelihood your networks and data are vulnerable to any of the following types of attacks if you do not have a security plan inplace.

Eavesdropping – Interception of communications by an unauthorized party. **Data Modification** – Data altering, reading fromunauthorized party

Identity Spoofing (IP Address Spoofing) – IP address to be falsely assumed— identity spoofing and the attacker can modify, reroute, or delete your data

Password-Based Attacks – By gaining your access rights to a computer and network resources are determined by who you are, that is, your user name and your password.

Denial-of-Service Attack – Prevents normal use of your computer or network by valid users, and it could be used for sending invalid data to application, to flood the computer, block traffic,etc.

Man-in-the-Middle Attack – Is when someone between you and the person with whom you are communicating is actively monitoring, capturing, and controlling your communication transparently

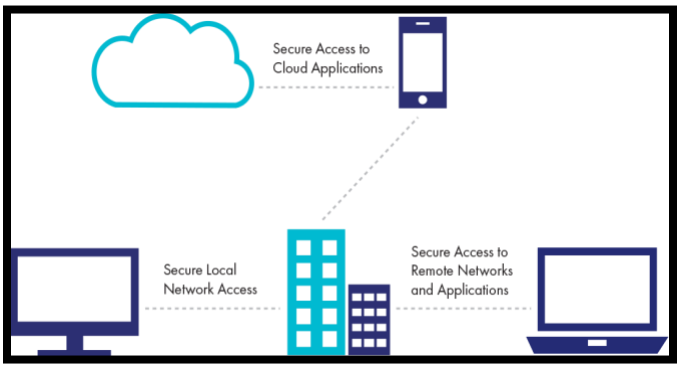
Application-Layer Attack – It targets applicationservers by deliberately causing a fault in a server's operating system or applications and the attacker gaining the ability to bypass normalaccess controls

TYPES OF NETWORK SECURITY:

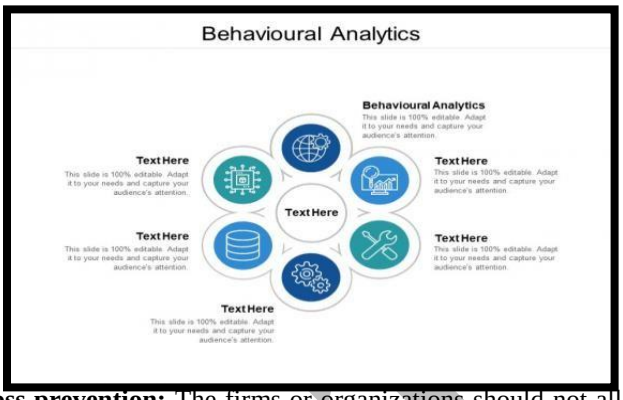
There are many types of network securities andsome of them are as follows:

★ Network access control
★ Antivirus and antimalware software
★ Application security
★ Behavioral security
★ Data loss prevention
★ Email security
★ Firewalls
★ Intrusion prevention system
★ Mobile device security
★ Network segmentation
★ Security information and event management
★ VPN
★ Web security
★ Wireless security

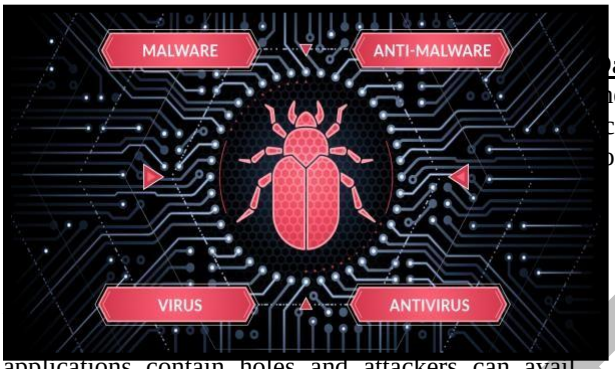
Network access control: To avoid the potential attackers, people need to recognize the users and the machines as those users and devices can regulate the security policies. The process of blocking the noncompliant endpoint machines and furnishing the limited access to them is called as network access control.



 ISBN: 978-81-910765-1-6

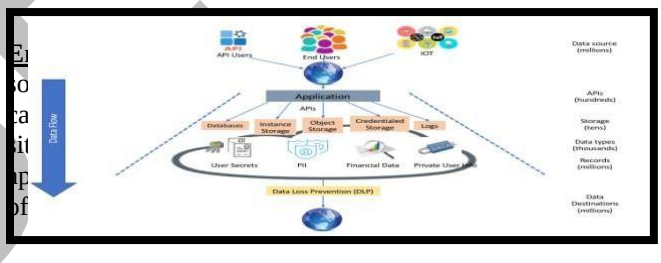


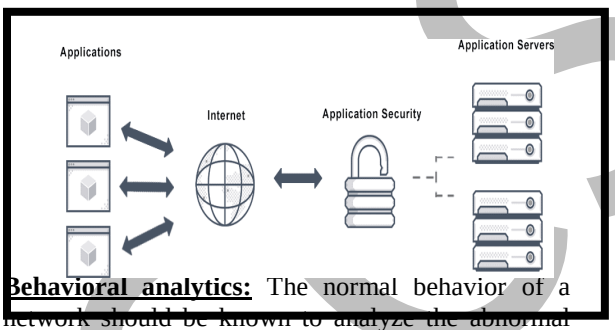
Antivirus and antimalware software: The viruses, worms, and Trojans come under malware, malware has the ability to infect the network. The available antimalware programs not only scan the malware but also take away itand at the same time fix the damage.



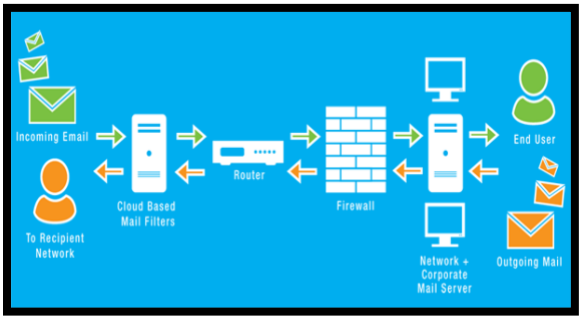
ata loss prevention: The firms or organizations should not allow eir staff to transmit the sensitive information and the applied cience of data loss prevention blocks the people from uploading, rwarding and printing the critical data in an unprotected way.

applications contain holes and attackers can avail these holes to infiltrate a network. The application security encircles the hardware; software and operations use to close the holes.



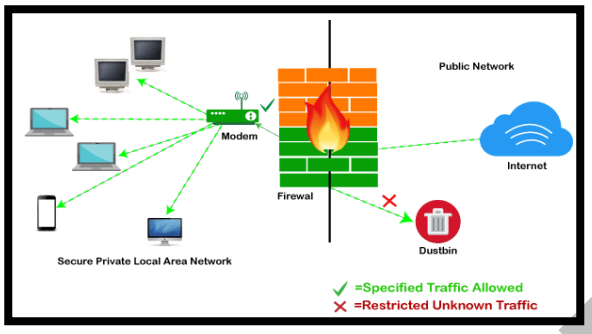


Behavioral analytics: The normal behavior of a network should be known to analyze the abnormal behavior of the network. The equipment of the behavioral analytics discriminate the abnormal activities which the security team takes it to process the further actions on it.



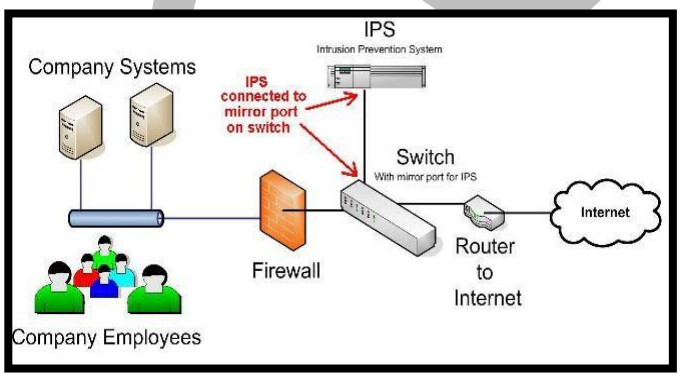
 ISBN: 978-81-910765-1-6

Firewall: A Firewall is a network security devicethat monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet. A firewall's main purpose is to allow non-threatening traffic in and to keep dangerous traffic out. The firewall creates a wall between a trusted internal network and the trustless internal network.



Intrusion prevention system: In short, an Intrusion

An Intrusion Prevention System's main functionis to identify any suspicious activity and either detect and allow (IDS) or prevent (IPS) the threat. The attempt is logged and reported to the network managers or Security Operations Center (SOC) staff. An intrusion prevention system scans the traffic of the network and
obstructs the coming attacks.

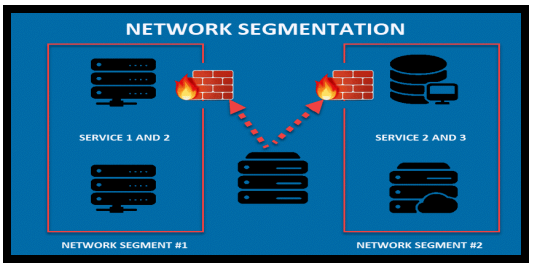


Prevention System (IPS), also known as intrusion detection prevention system (IDPS), is a technology that keeps an eye on a network for any malicious activities attempting to exploita known vulnerability

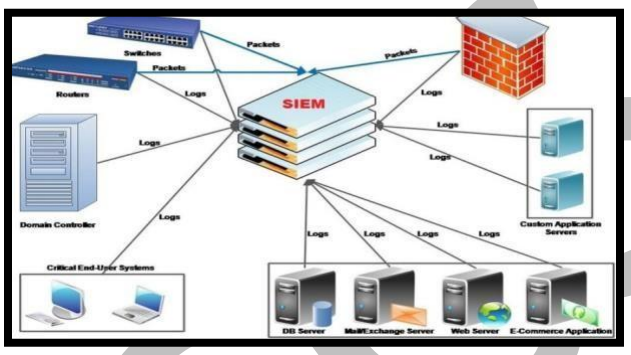
Mobile device security: In these days the cyber criminals are mostly targeting the mobile machines and apps, the mobile device security helps in controlling the device.Mobile Device Security refers to the measures designed to protect sensitive information stored on and transmitted by laptops, smartphones, tablets, wearables, and other portable devices. At the root of mobile device security is the goal of keeping unauthorized users from accessing the enterprise network. It is one aspect of a complete enterprise security plan.

multiple segments or subnets, each acting as its own small network. This allows network administrators to control the flow of traffic between subnets based on granular policies. Organizations use segmentation to improve monitoring, boost performance, localize technical issues and – most importantly – enhance security. The network segmentation helps in easily regulatingthe security policies in the network traffic.

 ISBN: 978-81-910765-1-6

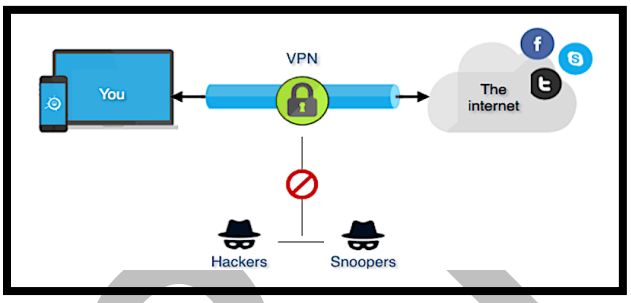


Security information and event management: Security information and event management (SIEM) technology supports threat detection, compliance and security incident management through the collection and analysis (both near real time and historical) of security events, as well as a wide variety of other event and contextual data sources. The core capabilities are a broad scope of log event collection and management, the ability to analyze log events and other data across disparate sources, and operational capabilities (such as incident management, dashboards and reporting). The security information and event management bring the data that the security staff needs to respond to the attacks or threats.



VPN: A virtual private network (VPN) is an Internet security service that allows users to access the Internet as though they were connected to a private network. VPNs use encryption to create a secure connection over unsecured Internet infrastructure.

VPNs are one way to protect corporate data and manage user access to that data. VPNs protect data as users interact with apps and web properties over the Internet, and they can keep certain resources hidden. They are commonly used for access control — however, other identity and access management (IAM) solutions can also help with managing user access. VPN avails safe socket layers between the device and network.



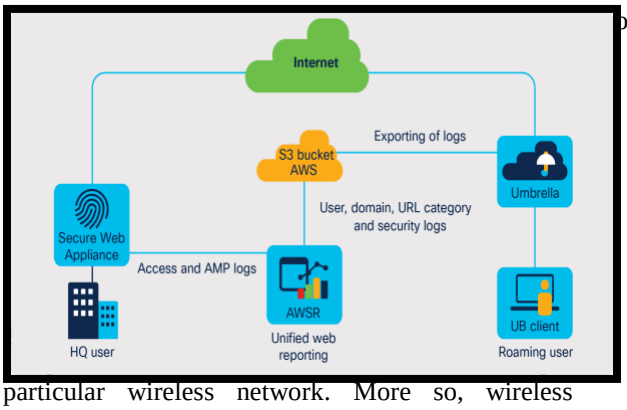
Web security: Web security is also known as "Cybersecurity". It basically means protecting a website or web application by detecting, preventing and responding to cyber threats.

Websites and web applications are just as prone to security breaches as physical homes, stores, and government locations. Unfortunately, cybercrime happens every day, and great web security measures are needed to protect websites and web applications from becoming compromised.

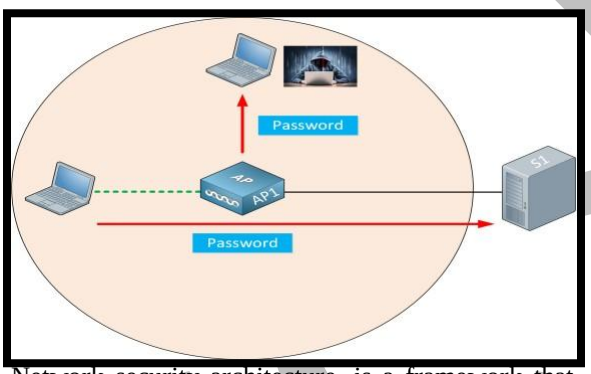
That's exactly what web security does – it is a system of protection measures and protocols that can protect your website or web application from being hacked or entered by unauthorized personnel. This integral division of Information Security is vital to the protection of websites, web applications, and web services.

Anything that is applied over the Internet should have some form of web security to protect it. Web security defends the web gateway on the sites.

 ISBN: 978-81-910765-1-6



particular wireless network. More so, wireless security, also known as Wi-Fi security, aims to ensure that your data remains only accessible to users you authorize. WirelessSecurity Protocols such as Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) are the authentication security protocols created by the Wireless Alliance used to ensure wireless security. The wireless networks are not as protected as the wired networks, the useof wireless security hinders the attacks.



Network security architecture, is a framework that specifies the organizational structure, standards, policies and functional behavior of a computer network, including both security and network features. Cybersecurity architecture is also the manner in which various components of your cyber or computer system are organized, synced and integrated.

A network security architecture framework is one component of a system's overall architecture. It's designed and built to

ovide guidance during the design of an entireproduct/system.

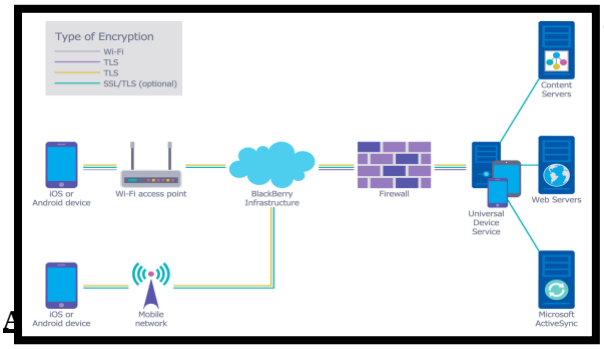
Security architecture helps to position security controls and breach countermeasures and how they relate to the overall systems framework of your company. The main purposeof these controls is to maintain your critical

system's quality attributes such as confidentiality, integrity and availability. It's also the synergy between hardware and software knowledge with programming proficiency, research skills and policy development. A security architect is an individual who anticipates potential cyber-threats and is quick to design structures and systems to preempt them. Most organizations are exposed to cybersecurity threats but a cybersecurity architecture plan helps you to implement and monitor your company's network security systems. A cybersecurity architecture framework positions all your security controls against any form of maliciousactors and how they relate to your overall systems architecture.

Various elements of cybersecurity strategies like firewalls, antivirus programs and intrusion detection systems play a huge role inprotecting your organization against external threats. To maintain and maximize these security tools as well as already existing and functional policies and procedures, your company should implement a detailed security architecture that integrates these different elements for your networks.

This framework unifies various methods, processes and tools in order to protect an organization's resources, data and other vital information. The success of a cybersecurity architecture relies heavily on the continuous flow of information throughout the entire organization. Everyone must work according tothe framework and procsses of your company'ssecurity architecture.

 ISBN: 978-81-910765-1-6



One-factor authentication – this is "something a user knows." The most recognized type of one-factor authentication method is the password.

Two-factor authentication – in addition to the first factor, the second factor is "something a user has." Examples of something a user has are a device that generates a pre-determined code, a signed digital certificate or even a bio-metric such as a fingerprint.

Three-factor authentication – in addition to the

previous two factors, the third factor is

"something a user is." Examples of a third factor are all bio-metric such as the user's voice, hand configuration, a fingerprint, a retina scan or similar .The advantage of using a 3 factor authentication is that it's made reassuringly sure that the person who is authenticating is the person who is authenticating through multiple layers of security.The disadvantage is that there is a possibility that the person trying to authenticate loses first or the second authentication, the process can also take time.

BENIFITS:

1) Protects system against viruses, worms,

spyware and other unwanted programs.

2) Protection against data from theft.

3) Protects the computer from being hacked.

4) Minimizes computer freezing and crashes.

5) Gives privacy to users

6) It hinders the cyber attacks. 7)It is centrally controlled.

8)The centralized network security system timely updates the antivirus system.

DRAWBACKS:

1) Firewalls can be difficult to configure correctly.

2) Incorrectly configured firewalls may block users from performing certain actions on the Internet, until the firewall configured correctly.

3) Makes the system slower than before.

4) Need to keep updating the new software inorder to keep security up to date.

5) Could be costly for average user.

6) It is very time-consuming.

7) It needs the skilled staff.

Thus, everyone must have the knowledge of protecting tools because the people can at leastprotect their own network from all suck attacks.

WHAT IS THE FUTURE OF NETWORK SECURITY?

"The Future of Network Security Is in the Cloud," describing the concept of the secure access service edge (SASE) for protecting digital business transformation with cloud-based, software-defined secure access.
If you want to secure the present threat environment, there is a need to provide more than just basic network security. It needs to equip with technologies like deep learning, AI, etc. for becoming effective and tackling the challenges. It will make sure the upcoming

 ISBN: 978-81-910765-1-6

threats get tackled adequately.

CONCLUSION:

Network security is a crucial factor that many organizations consider. An attack or threat maycause substantive loss of information or data to an organization. It may also destroy critical infrastructure. It is, therefore, the best decision to develop a reliable security policy for the firm's network. The above network security policies can play a significant role in mitigating the risks that the firm may experience in its operational environment. All the security policies should ensure that the information anddata are confidential without affecting its availability or integrity. That is why network security is an important field that is increasingly gaining attention as the Internet usage increases. The security threats and Internet protocols were analysed to determine the necessary security technology. However, the current development in network security is not very impressive and significant.

Therefore, researchers and scholars are rapidly evolving in developing and investigating the

threats further in a future. And with this information in mind, the process can be formalized and the path becomes clearer as youdelve deeper into the specifics of the security process, as well.

REFERENCES:

[1] https://studymafia.org/network-security-seminar-and-ppt-with-pdf-report/

[2] https://www.checkpoint.com/cyber-hub/network-security/what-is-ips/#:~:text=In%20short%2C%20an%20Intrusion%20Prevention,to%20exploit%20a%20known%20vulnerability.

[3] https://www.goodfirms.co/glossary/web-security/#:~:text=Web%20security%20is%20also%20known,%2C%20stores%2C%20and%20government%20locations.

[4] https://www.securew2.com/blog/complete-guide-wi-fi-security

[5] https://www.vmware.com/topics/glossary/content/mobile-device-security

[6] https://www.coursehero.com/file/p36t41r/Conclusion-Network-security-is-a-crucial-factor-that-many-organizations/