Date available online: 18-03-2024
Vol. 1, Issue 2 (July-December 2023)
This is an open-access article.

Evaluating the Effectiveness and Resilience of SSL/TLS, HTTPS, IPSec, SSH, and WPA/WPA2 in Safeguarding Data Transmission

Zain Tariq[1], Bint e Zainab[1], Muhammad Zunnurain Hussain[2*]

[1]Department of Computer Engineering Information Technology University of the Punjab Lahore, Pakistan
[2]Department of Computer Science Bahria University Lahore Campus Lahore, Pakistan

[*]Corresponding author: Muhammad Zunnurain Hussain (e-mail: zunnurain.bulc@bahria.edu.pk)

ABSTRACT This research paper focuses on evaluating the effectiveness and resilience of network security protocols, which are essential for protecting the confidentiality, integrity, and availability of data transmitted over the network. More and more communication protocols developed over the period to provide reliable and effective communication, and for most of them, security was their significant goal. The paper covers a comprehensive overview of different security protocols such as SSL/TLS (Secure Socket Layer/Transport Layer Security), HTTPS (Hypertext Transfer Protocol Secure), IPSec (Internet Protocol Security), SSH (Secure Shell Protocol), and WPA/WPA2 (Wi-Fi Protected Access), including their strengths and weakness. The study extends its contribution by analyzing how these protocols react to current emerging threats and attacks, revealing valuable insights into their real-world applicability. The finding of the paper helps network administrators to ensure the highest level of security for their networks.

INDEX TERMS *Network Security Protocols, Data Transmission, Emerging Threats, SSL/TLS, HTTPS, IPSec, SSH, WPA/WPA2*

I. INTRODUCTION

In today's contemporary world, the inclusion of security measures is required for any kind of communication that takes place via a network. Network security systems often provide encrypting and authenticating methods to their users as a means of ensuring the confidentiality of data flows. As a direct consequence of this, the idea of network security may be applied to every single aspect of information technology. Due to the increasing complexity of cyber threats and attacks, putting in place the best appropriate security protocol has become a challenging task for security specialists and network managers. When more individuals obtain access to the internet and when internet usage becomes more prevalent, the possibility that sensitive information may be compromised via network connection will rise. This is because more people will have access to the internet. The implementation of security measures is required to stop this from happening. There are further measures that may be taken to improve the security and effectiveness of computer communication [1]. Even while it is theoretically safe to utilize the network protocols, the method in which they were implemented was defective, and this enabled hostile opponents to take advantage of the situation. It is of the highest significance to validate that the network standards that we use for guaranteeing that communication is kept private are, in fact, as secret as we think them to be. This is because the privacy of our communications is of the utmost importance. To find a solution to this problem, one of our goals is to provide an overview of the possible security issues that are present in regularly used network protocols. These protocols will be the foundation for future communication systems. An examination of the security of network protocols, with a focus on data transmission and remote management, is going to be carried out by our team. While we are working on constructing the communication route between the devices, we will discuss the numerous security concerns that may appear at any moment [2]. The remaining sections of the article are organized as shown in the following paragraphs. In this section, the many different kinds of network protocols' varying degrees of security are broken down and studied. The security implementation of these protocols is analyzed in the third part. The Cyber Security Dataset and newly emerging threats are discussed in the fourth and fifth parts of the paper, along with possible solutions to those threats. The sixth portion is the concluding part of the paper.

II. NETWORK SECURITY PROTOCOLS

A network protocol is a preset set of standards and procedures that regulate the communication that takes place between two separate devices. This communication may take place through the Internet or another kind of network. A protocol for a network will specify both the structure of communication and the mechanism by which messages are sent between nodes on the network. There are many different protocols, each of which serves a distinct set of preferences and requirements; however, the fundamental implementation should be the same for all. Application developers create programs that, without the need for explicit programming, allow various electronic devices to communicate and collaborate with one another. We are going to study the security of those applications/devices, and more specifically, we are going to look at how vulnerable the communication is to being intercepted by dishonest third parties depending on which protocol is being used to deliver the data. This will be done using a range of different protocols. To get things started, we will present an overview of the main network protocols at a high level.

SSL/TLS: Cryptographic technologies such as SSL and TLS (Secure Sockets Layer and Transport Layer Security) are created to guarantee that communication between two applications that use the internet is kept private and secure. The use of SSL/TLS, which is a system that enables secure communication for online transactions, may be beneficial for a variety of online activities, including electronic mail, online shopping, and even online banking. The data that is sent from one device to another is encrypted using SSL/TLS, which means that the data is unreadable to anybody who happens to intercept it while it is being transmitted and is thus more secure. To properly encrypt this information, a wide array of symmetric and asymmetric encryption algorithms was utilized in conjunction with one another. With the assistance of the SSL/TLS handshake protocol, it is possible to establish an encrypted connection between two distinct machines. During the process, the two devices will authenticate one another's identification, disclose information about their own encryption capabilities, and negotiate the encryption keys. After the handshake process, a secure connection is established between them, which enables the devices to send and receive data in an encrypted form. The SSL/TLS handshake process is illustrated in Figure 1.

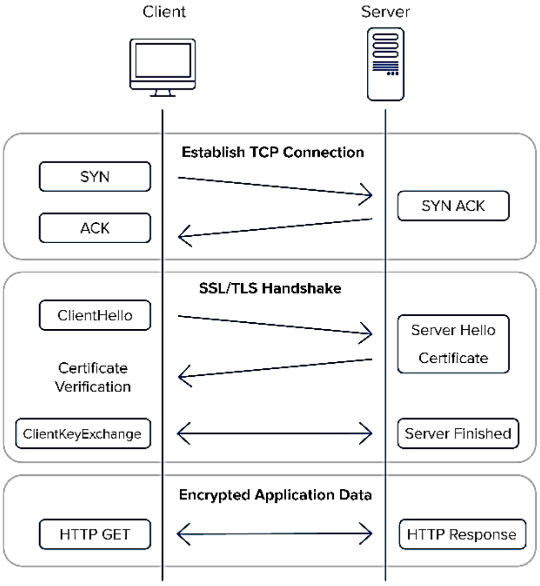

Fig. 1: SSL/TLS Handshake Process [3]

HTTPS: When communicating in a secure way over the internet, a web browser and a web server may make use of a network protocol known as HTTPS (HyperText Transfer Protocol Secure). It is an extension of the standard HTTP protocol, but it encrypts and authenticates data using SSL/TLS, giving users a higher security and reassurance about the identity of the person with whom they are communicating. HTTPS ensures that data cannot be intercepted, modified, or impersonated by unauthorized parties by establishing an encrypted connection between the client and the server. This makes secure communication possible and assures that data cannot be manipulated. Although it does not provide compression, caching, filtering, or any other kind of content optimization, it is what enables the protocol to keep its authenticity and anonymity while at the same time allowing it to function. This raises the question of whether it may have an impact on the quantity of data that will be consumed, the speed at which sites will load, or the upkeep of the infrastructure. To implement HTTPS for websites, SSL certificates are necessary, which enables consumers to check the legitimacy of the websites. SSL certificates are required to be registered by websites. Modern web browsers also display visual indicators, such as the “Secure” keyword or padlock icon on the address bar, to help consumers that the website they are using is secure. While HTTPS is secure and designed to provide encrypted communication over the web, it is not entirely immune to security threats. The transparency report issued by Google on April 2, 2023, discloses that the proportion of Google's total encrypted traffic has increased by 95% over the course of the previous year. This information is as of the date of the report's publication [4].

IPSec: Internet Protocol Security, often known as IPSec, is a collection of security protocols that provides secret communication at the IP layer. Creating a Virtual Private Network, often known as a VPN, between two network devices makes it possible to create a communication channel that is more resistant to intrusion. This is an example of a common use for the technology. Internet Protocol Security may be implemented in one of two ways: transport mode and tunnel mode.

- **Transport Mode:** In transport mode, only the IP packet's payload is encrypted, leaving the header unencrypted. This mode is used for communication between two hosts on a network.
- **Tunnel mode:** In tunnel mode, the IP packet is completely encapsulated and encrypted within a new IP packet, with a new header inserted into the encrypted packet.

SSH: The Secure Shell protocol, often known as SSH and shortened as SSH, is a cryptographic network protocol that offers authentication, secure encryption, and protection for the message's integrity. The Telnet and FTP protocols, both of which were regarded to have a lower level of security and were thus rendered obsolete with the introduction of the SSH protocol. It accomplishes this goal by using public-key cryptography, which is a kind of encryption, in order to verify the distant computer and, if necessary, to allow the remote computer to validate the user as well. SSH is able to maintain the secrecy of sent data by encrypting it using a number of different algorithms, some of which include AES, 3DES, and Blowfish, amongst others. In addition, digital signatures may be used with SSH in order to guarantee that the data has not been tampered with. When seeking to get secure remote access to servers and other network devices, it is standard custom to make use of the SSH protocol. It offers a safe channel for file transfer protocols such as SCP and SFTP, in addition to enabling secure remote shell access. SSH is also often used for secure tunneling, which enables users to encrypt communication that takes place between two network endpoints. This is another common usage for SSH. SSH is used for a lot of other things, including this as well. It is equipped with a number of different cyphers that may be used in order to maintain the confidentiality of the communication channel. In addition, a Message Authentication Code, or MAC, is appended to each packet before it is sent. This is done to ensure that the data is received in its original form.

WPA/WPA2: Wi-Fi Protected Access, abbreviated as WPA and WPA2, is the name of two different security protocols that were created to safeguard wireless networks. The initial version of the WEP (Wired Equivalent Privacy) protocol, which was shown to be susceptible to assaults, has been improved and is now known as WPA. WPA2, an even more secure version of WPA, is the protocol that is now recommended to use for securing Wi-Fi networks. It is presently advised that users protect their wireless networks using WPA2. The wireless communications that are protected by WPA2 are encrypted using the Advanced Encryption Standard (AES), which is an encryption method that is far more trustworthy than the RC4 encryption method that is used in WEP and WPA. The fact that the AES encryption technique uses a key of 128 bits makes it very hard to decrypt.

III. SECURITY ANALYSIS OF NETWORK PROTOCOLS

A. SECURITY IMPLEMENTATION OF SSL/TLS

TLS, which stands for Transport Layer Security, is the protocol that will eventually replace SSL. TLS is considered to be a more secure protocol than SSL in most circles. SSL is vulnerable to security issues, such as the Padding Oracle On Downgraded Legacy Encryption (POODLE) hole, which allows malicious actors to decode SSL communication. On the other hand, TLS comes with incremental fixes and does not have any of these problems in its design. However, SSL is still extensively used, even though Transport Layer Security (TLS) offers an upgrade in terms of its use of stronger cryptographic algorithms and more secure key exchange methods. This is due to the legacy system and compatibility with SSL. Most applications were initially designed to use SSL, and transitioning to TLS requires changes on both the client and server side and organizations are hesitant to make this transition due to its widespread implementation. After the latest release of TLS, modern improvements have been undergone to enhance its security and performance. With reduced handshake latency and improved security made TLS 1.3 the industry standard for secure communication. DHE (Diffie-Hellman Ephemeral) and ECDHE (Elliptic Curve Diffie-Hellman Ephemeral) key exchange methods are implemented on TLS to provide forward secrecy, ensuring the past communication remains encrypted, even if the server’s private key is compromised. In addition, ongoing research and improvements in cryptography focus on developing quantum cryptographic algorithms to ensure and further enhance TLS security in the Quantum Computer in the future.

POODLE is an acronym that means for Padding Oracle against Downgraded Legacy Encryption, and it is the name of one of the most well-known attacks that can be carried out against SSL/TLS. The vulnerability used in this attack is present in SSL 3.0 and TLS 1.0. As a direct consequence of this vulnerability, an adversary has the ability to decode data that is being sent between a client and a server. However, since contemporary web browsers no longer support SSL 3.0 and TLS 1.0, this attack can only be used against those specific versions of SSL and TLS. It is not possible to use it against any other versions. Another weakness that might be exploited is known as the Heartbleed bug, and it affects the OpenSSL library, which is used in SSL/TLS implementations. As a result of this vulnerability, attackers have the potential to get access to the memory of the server and steal sensitive data such as private keys and login information, amongst other pieces of personal information. Since this problem has been resolved in the most recent release of OpenSSL, it is strongly suggested that you make use of a version of OpenSSL that does not fall prey to the aforementioned vulnerability. Efforts have been made to address this issue. In addition, SSL/TLS is susceptible to attacks such as man-in-the-middle and denial-of-service attacks (MITM and DoS, respectively). DoS attacks may flood the server with traffic and make it unreachable, whereas MITM attacks enable the data that is passed between the client and the server to be intercepted and modified. MITM attacks are a subset of distributed denial of service attacks. Attacks known as man-in-the-middle (MITM) have the potential to steal and manipulate the data that is sent between the client and the server.

In order to reduce the likelihood of these vulnerabilities and attacks, SSL and TLS implementations should be configured to use the most recent versions of the protocol, such as TLS 1.2 or TLS 1.3. These newer versions of the protocol contain improved cryptographic algorithms and security features. There are a few instances of such versions, including TLS 1.2 and TLS 1.3. Only reputable certificate authorities should be authorized to issue SSL/TLS certificates, and those certificates should be renewed on a regular basis. Because of this, the usage of certificates that have either been invalid or have been compromised will be prevented. In conclusion, SSL/TLS is an established network security protocol that offers an additional degree of protection for the data transmission that takes place over the internet. This protection may be achieved via the use of a combination of both transport layer security and data link layer security.

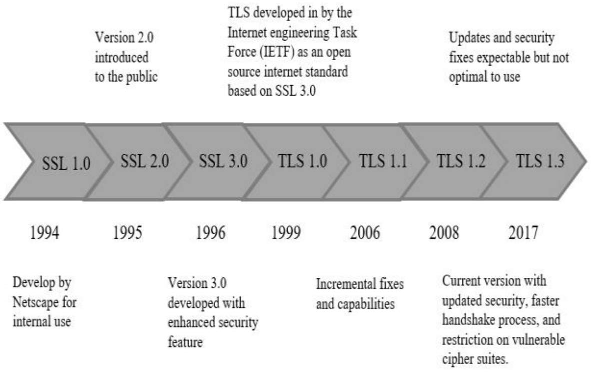
Version 2.0 introduced to the public
TLS developed in by the Internet engineering Task Force (IETF) as an open source internet standard based on SSL 3.0
Updates and security fixes expectable but not optimal to use
SSL 1.0
SSL 2.0
SSL 3.0
TLS 1.0
TLS 1.1
TLS 1.2
TLS 1.3
1994
1995
1996
1999
2006
2008
2017
Develop by Netscape for internal use
Version 3.0 developed with enhanced security feature
Incremental fixes and capabilities
Current version with updated security, faster handshake process, and restriction on vulnerable cipher suites.

Fig. 2: SSL/TLS Versions Development Timeline [5]

On the other hand, SSL/TLS implementations need to be kept up to date and suitably established in order to preserve the highest level of security that is achievable. This is required due to the fact that it is not resistant to weaknesses and assaults. The several iterations of SSL/TLS and the most recent security fixes are broken out graphically in Figure 2, which may be found here.

B. SECURITY IMPLEMENTATION OF IPSEC

IPSec provides various security features, including confidentiality, authenticity, data integrity, and anti-replay protection.

1. Data is encrypted using symmetric encryption techniques like AES or 3DES to provide **confidentiality**.
2. Digital signatures that use asymmetric encryption algorithms like RSA to confirm the sender and recipient's identities are used to provide **authenticity**.
3. **Data integrity** is ensured by hashing using a method like SHA-256 to produce a message digest, which is then decrypted and validated at the receiving end.
4. **Anti-replay protection** prevents attackers from intercepting and replaying old, encrypted packets by including a sequence number in the header of the encrypted packets.

When determining the degree of safety provided by a protocol, it is important to take into account both the implementation and configuration of the Internet Protocol Security (IPSec) security system. There is a possibility that the implementation of IPSec offered by a number of different vendors is distinct from one another and contains vulnerabilities such as buffer overflows or privilege escalation. It is often necessary to upgrade the patches and updates for the IPSec software in order to guarantee that all known vulnerabilities have been shut down. In addition, configuring IPSec is a very critical step that has to be taken. When you utilize encryption techniques or keys that are insufficiently robust, for instance, you leave your communication open to the possibility of being overheard. It is required to make use of stringent encryption algorithms and keys, such as those created by AES with a key length of 256 bits, in order to safeguard the privacy of the information that is being conveyed. This may be accomplished by using encryption software. IPSec should also be set to use mutual authentication, which is a procedure in which the client and the server authenticate each other by using digital certificates or other secure ways. This should be done in order to prevent unauthorized communication between the client and the server. This ought to be finished before the procedure is put into action.

C. SECURITY IMPLEMENTATION OF SSH

The acronym "SSH" stands for "Secure Shell," and it refers to a program that lets users securely access remote computers. When symmetric encryption is used, users are presented with a number of authentication and communication security choices from which to select. In addition, it offers an alternative to protocols such as telnet and FTP, both of which are comparable but do not have enough security. SSH is used to offer secure access in order to automate activities, report secure instructions across remote connections, and govern remote networks in a secure way. These goals may be accomplished through the use of SSH.

Despite the fact that SSH offers a large number of authentication methods, the most commonly used methods are password authentication and public key authentication. The use of a password as a mode of authentication is by far the most common practice for almost any sort of internet login system. In order to utilize the public key authentication technique, you will need to possess both a public key and a private key. This is a prerequisite for using the public key authentication method. Because the server is configured to utilize the public key, it is feasible for anybody who has a copy of the private key to access the server. The second primary objective that the SSH protocol works to accomplish is to ensure the confidentiality of the data exchanged between the two distinct computing systems. All of the parties involved have come to an agreement on a cypher suite that is quite similar to TLS in order to make symmetric encryption during conversations between the devices. This enhances the confidentiality and integrity of data transmitted between devices and ensures the establishment of a secure and standardized framework. The secure shell (SSH) connection that takes place between an edge client and a server is shown in Figure 3.

Modern implementations of SSH support multi-factor authentication (MFA), adding an extra layer of security beyond password and key-based authentication. Elliptic Curve Cryptography (ECC) based key exchange methods are currently under research and development that provide a more secure and efficient way to key exchange methods while reducing the computational effort. This advancement enhances the security of SSH even more and guarantees the key exchange is resource-efficient.

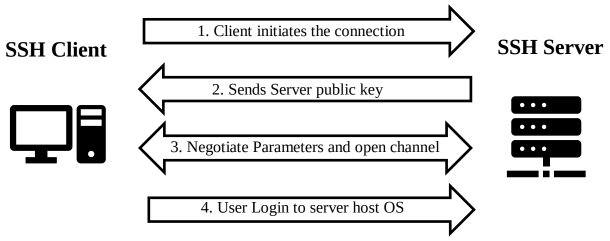
SSH Client
SSH Server
1. Client initiates the connection
2. Sends Server public key
3. Negotiate Parameters and open channel
4. User Login to server host OS

Fig. 3: SSH Implementation [6]

When trying to get into an SSH server, attackers will often resort to either the dictionary assault or the brute force assault as a method of attack. The method of trying to obtain entrance to the server's network by accurately guessing the needed password is referred to as "brute force". In order for researchers to carry out a brute-force attack, they must first construct a "honeypot" that serves to imitate the functioning of the real system for the benefit of the attacker. This is essential due to the fact that brute-force assaults are not dependent on the implementation that is being used. The "honeypot" categories that are most readily accessible are research and production jobs respectively. Honeypots in production are used by businesses in order to reduce the likelihood of a successful cyberattack on their information technology infrastructure. This is made possible by having a simulated system that appears real, with the idea that if unauthorized access is accomplished, it will be identified, and the strategies utilized by the hackers may be explored in order to make the actual system's security stronger. The existence of a simulated system that gives the impression of being genuine makes this conceivable. In the field of research, honeypots are used to collect as much information as possible, which a broad variety of researchers may subsequently use to achieve a number of different objectives [7].

D. SECURITY IMPLEMENTATION OF WPA/WPA2

WPA and WPA2 (Wi-Fi Protected Access) are susceptible to attacks, just like any other network security protocol; thus, it is essential to have an understanding of these threats in order to effectively apply security measures. The following are some frequent assaults against WPA and WPA2:

1. **Rogue Access Point attack:** In this attack, a fake access point is created that mimics a legitimate access point. Unaware users connect to the malicious access point, which gives the attacker access to their traffic and sensitive data.
2. **Evil twin attack:** The attack is similar to the rogue access point attack, but instead of creating a fake access point, the attacker sets up a malicious hotspot next to a real one.

In order to safeguard your network against WPA and WPA2 attacks, it is vital to make use of strong passwords, activate network encryption, and routinely upgrade the firmware of network devices in order to lessen the damage that these attacks have on a system. One of the crucial steps to enhance the security of Wi-Fi devices is to upgrade to WPA3. WPA3 is the latest Wi-Fi security standard, that offers more protection to various security threats than its predecessors. You can restrict devices by specifying which devices are allowed to connect to the network based on their MAC addresses by implementing MAC address filtering. In addition, managers of networks need to monitor network traffic and be on the lookout for any activity that seems out of the ordinary.

IV. CYBERSECURITY DATASETS

A. CICIDS2017

The CICIDS2017 dataset is a collection of data pertaining to cybersecurity that contains information on both benign and malicious traffic. Because this is a tagged dataset, each network traffic flow has been given a label indicating whether it should be used in a secure manner or if it should be avoided at all costs. This particular dataset was developed by the Canadian Institute for Cybersecurity (CIC), which operates out of the University of New Brunswick.

The dataset contains a diverse assortment of different types of network traffic, such as web traffic, traffic for file transfer, and email traffic, amongst others. It comes with more than eighty features, some of which include different types of protocols, port numbers, and the IP addresses of traffic origins and destinations. More than 2.5 million distinct traffic flows on the network are represented in the collection of data that was gathered. The dataset contains malicious traffic that was the result of a broad variety of attacks, including online assaults, brute force attacks, distributed denial of service attacks, brute force attacks, botnet attacks, port scan attacks, and denial of service attacks. In all, the collection includes more than 16 distinct attack categories in addition to 11 distinct kinds of benign categories. In addition to that, it comprises attacks that range in both complexity and seriousness in varying degrees. Research on cybersecurity, in particular the creation of intrusion detection and prevention systems, may benefit the modern development of security protocols from the use of this information and utilize it to their advantage. Furthermore, it may be used to assess the effectiveness of machine learning and deep learning algorithms in relation to the categorization of network traffic and the identification of irregularities.

Using the B-Profile approach, which was suggested by Sharafaldin et al. (2016) [10], the dataset simulated realistically benign background traffic and profiled the abstract behavior of human interactions. In addition to that, our system tracks the intangible behaviors of human interactions. We used the HTTP, HTTPS, FTP, and SSH protocols, in order to generate the abstract behavior of 25 individuals for this dataset. Anyone in the globe is able to access the dataset and download it; moreover, it may be used for the purpose of carrying out research. It is essential to bear in mind that the data collection in question contains information that might be considered sensitive and that this data gathering should only be utilized for research purposes that are appropriate.

The gathering of information took place over the course of five days, commencing on Monday, July 3, 2017, at 9 a.m. and coming to a close on Friday, July 7, 2017, at 5 p.m. On Monday, there are no noteworthy events to attend, and the level of traffic is often low. There are many various kinds of attacks that may be deployed, such as Brute Force SSH, Brute Force FTP, DDoS, DoS, web attacks, Heartbleed, infiltration, and botnet. On Tuesday, Wednesday, Thursday, and Friday of the next week, they were put to death twice a day, once in the morning and once in the afternoon on each of those days [10]. An instance of the attack statistics that are contained in the CICIDS2017 dataset may be seen in Figure 4, and the detailed timeline of the attacks and the protocols affected throughout the week is shown in Table 1.

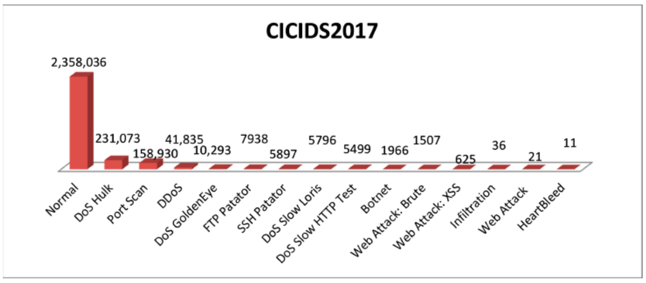

Fig. 4. Statistics of attacks and normal behavior in the CICIDS 2017 dataset [9].

TABLE 1:
Attacks Timeline in CICIDS2017 Dataset [10].

Days	**Attacks**	**Affected Protocol**
Monday, July 3	Benign	-
Tuesday, July 4	FTP-Patator	FTP - SSH
	SSH-Patator	SSH
Wednesday, July 5	DoS slowloris	SSL/TLS - HTTPS
	DoS Slowhttptest	SSL/TLS - HTTPS
	DoS Hulk	SSL/TLS - HTTPS
	DoS GoldenEye	SSL/TLS - HTTPS
Thursday, July 6	Web Attack – Brute Force	SSH
	Web Attack – XSS	HTTPS
	Web Attack – SQL Injection	HTTPS

The dataset helps us assess the different threats that could potentially be harmful to the network and evaluate the strengths and weaknesses of the respective security protocols in real-world events. The incorporation of both benign and malicious attacks allows for a comprehensive evaluation of the protocol's ability to behave in various security events. The detailed prevention measures of these threats are provided in the relevant section of the affected protocol and outlined in Table 2, with threat characteristics and potential impact.

TABLE 2:
Comparison of Security Threats.

Threat	**Characteristics**	**Potential Impact**	**Preventive Measures**
DoS Slowloris	Application layer attack	Service disruption	Rate limiting, Intrusion Prevention Systems (IPS)
SQL Injection	Exploits database vulnerabilities	Unauthorized access, data manipulation	Input validation, Parameterized queries
XSS	Injects malicious scripts into web pages	Data theft, session hijacking	Input validation, Content Security Policy (CSP)
Botnet ARES	Botnet-based attacks	Unauthorized control, DDoS attacks	Network monitoring, Anti-botnet measures

V. EMERGING THREATS AND POTENTIAL SECURITY ISSUES

Emerging risks and security challenges are threats that are new and continually changing. They may be the result of shifts in operational procedures, developments in technology capabilities, or other factors. As a direct consequence of the unceasing advancement of technology, businesses are confronted with an ever-increasing number of issues that are associated with the information security of their operations. In this environment, it is of the highest significance to recognize the potential dangers and develop preventative measures that may be put into action.

One of the main issues that network security must face is the proliferation of devices connected to the Internet of Things. The proliferation of the Internet of Things (IoT), whose gadgets often do not have enough protection and are open to attack, has led to an increase in the number of security issues that have been found throughout the globe. Attackers are able to use these tools to not only get access to sensitive data but also to carry out major attacks such as distributed denial of service (DDoS) operations [8].

In addition to the security issues that they encounter, users of IoT devices are also susceptible to a number of privacy attacks, including sniffing, de-anonymization, and inference attacks. These vulnerabilities are in addition to the security difficulties that they face. In addition, the data's privacy is put in jeopardy at all times, regardless of whether they are in the process of being moved or have already been stored. The use of blockchain technology has a significant impact on the success of efforts to solve issues that pertain to individuals' right to privacy. In terms of issues pertaining to one's privacy, it does this in the following ways [9]:

- Militarized intrusion techniques (MITs) are of two categories: active MIT attacks (AMAs) and passive MIT attacks (PMAs). The PMA observes the data transfer between two devices as a passive listener. The data are not changed even when the PMA violates privacy. When an attacker has access to a device, they can study it silently for months before attacking it. The influence of PMA is growing more substantial because of the rising number of cameras in IoT devices like toys, cellphones, and wristwatches.
- Passive data privacy attacks (PDPAs), on the other hand, are classified as active data privacy attacks (ADPAs). The main factor in identity theft and reidentification is data privacy. In this context, re-identification attacks take advantage of anonymization, location detection, and data aggregation. To identify their targets, they try to collect data from a variety of sources. Malware has the ability to pretend to be a user. Data tampering is covered under ADPA, whereas data leakage and re-identification are covered by PDPA.

The incorporation of artificial intelligence (AI) and machine learning (ML) into the realm of cybersecurity introduces an additional, previously unanticipated threat. AI and ML have the ability to boost security by recognizing and responding to threats in real-time; but, they also have the potential to be exploited by bad actors in order to develop more complicated forms of attack. While AI and ML have the potential to enhance security, they also have the potential to be used by evil actors. For example, thieves may utilize machine learning algorithms to create phishing strategies that are more successful or to circumvent security measures that are already in place.

In addition, the growth of cloud computing and the outsourcing of IT services has led to a rise in the number of security holes that may be exploited by hostile actors. These flaws may be exploited in a variety of different ways. It is essential for businesses to be certain that the cloud service providers they work with have stringent security protocols in place, not just to secure their internal systems, but also the private information they store there.

VI. CONCLUSION

This research article provides a comprehensive assessment of important network security protocols, such as SSL/TLS, IPSec, SSH, and WPA/WPA2, as well as how these protocols assist in preventing a number of security threats and attacks. These protocols include secure sockets layer (SSL), internet protocol security (IPSec), secure socket shell (SSH), and wireless protected access (WPA/WPA2). The number of different devices that may connect to a network, as well as the degree of complexity of such networks, will continue to rise, which will result in the emergence of new security threats and challenges. It is essential to keep a degree of acquaintance with the most current security best practices in order to protect oneself against new threats that are always appearing. Because of the weaknesses in the protocols that we have investigated in this study, there is a need for stronger security against malicious attackers. The broader problem is that a particular implementation of a single protocol that was built for one domain does not perform well in another domain, and the adoption of this implementation has a severe effect on overall security. The term for this kind of situation is the "domain mismatch" problem. In conclusion, the choice of security protocols depends on the specific use case. This research paper underlines the need to implement stringent security rules, as well as perform ongoing monitoring and updating of network security protocols, in order to lessen the possibility that there would be a security breach.

REFERENCES

[1] Xuemei Ding et al 2020 J. Phys.: Conf. Ser. 1648 032137

[2] D. Caballero, F. Gonzalez and S. A. Islam, "Analysis of Network Protocols for Secure Communication," 2021 9th International Symposium on Digital Forensics and Security (ISDFS), Elazig, Turkey, 2021, pp. 1-6, doi: 10.1109/ISDFS52919.2021.9486356.

[3] Establishing an SSL/TLS Session: https://developer.okta.com/books/api-security/tls/how/

[4] HTTPS Encryption on the Web: https://transparencyreport.google.com/https/overview

[5] SSL/TLS Vulnerabilities: https://www.hhs.gov/sites/default/files/securing-ssl-tls-in-healthcare-tlpwhite.pdf

[6] What is SSH (Secure Shell): https://www.ssh.com/academy/ssh

[7] G.Michael, R.Karthikeyan, "A RESEARCH ON SECURE SHELL (SSH) PROTOCOL," International Journal of Pure and Applied Mathematics Volume 116 No. 16 2017, 559-564

[8] W. Zhou, Y. Jia, A. Peng, Y. Zhang and P. Liu, "The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved," in IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1606-1616, April 2019, doi 10.1109/JIOT.2018.2847733.

[9] Alshaibi, A.; Al-Ani, M.; Al-Azzawi, A.; Konev, A.; Shelupanov, A. The Comparison of Cybersecurity Datasets. Data **2022**, 7, 22. https://doi.org/10.3390/data7020022

[10] Intrusion Detection Evaluation Dataset (CIC-IDC2017) https://www.unb.ca/cic/datasets/ids-2017.html