iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** VI **Month of publication:** June 2025

DOI: https://doi.org/10.22214/ijraset.2025.72764

www.ijraset.com

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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VI June 2025- Available at www.ijraset.com

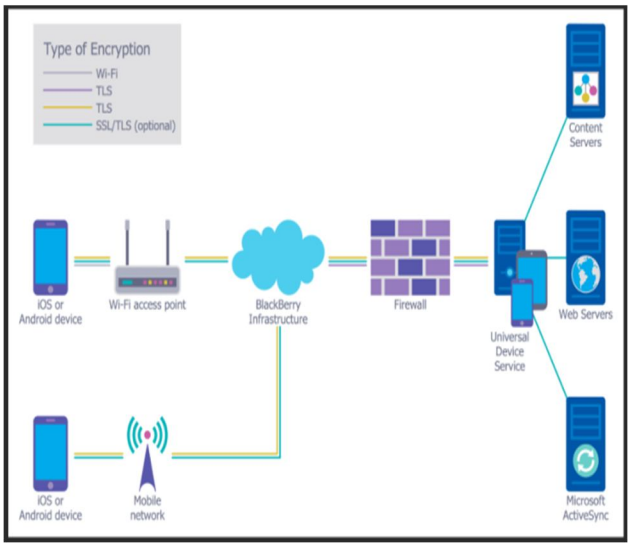
Security Protocols in Network Architecture

Sharada B.T.
Department of Computer Science, Field Marshal K.M Cariappa College, Madikeri, Karnataka, India

Abstract: ***Security protocols are essential for safeguarding data during transmission. In networking technologies, highly robust security protocols are required to ensure data integrity, confidentiality, and authority across different communication systems. The paper discusses the different types of security protocols, key components of security protocols, security protocol layers, treats and measurement of security and challenges and implementation of security protocols. These protocols encompass a suite of components that work together to achieve various security functions, such as encryption, access control, and message integrity.***
Keywords: TLS, SSL, IPsec, Kerberos, SNMP, SFTP, Encryption, ESP, AD, AH, IETF, SSH, LAN, WAN, FTP, HTTP, IP.

I. INTRODUCTION

Network design serves as the cornerstone of international communication in the current digital era, enabling seamless information sharing and connectivity among devices and systems. But this expansion also brings with it a rise in security. Threats, such as illegal access, cyber-attacks, and data breaches. Security protocols are used to protect data transfer by guaranteeing confidentiality, integrity, and authentication in order to address these issues. These protocols safeguard communication between different network layers by utilizing access control, key management, encryption, and authentication. Well-known protocols like SSL/TLS, IPsec, Kerberos, SNMPv3[5], and SFTP are crucial for protecting online activities like file transfers, email correspondence, and web browsing. The main security protocols utilized in network architecture are examined in this paper, along with their significance in safeguarding contemporary digital communications[4].



II. ELEMENTS OF SECURITY PROTOCOLS

1) Access Control: It authenticates a user's identity and enables access to certain resources depending on permission levels and access policies. It's an important part of keeping information secure and out of reach.
2) Encryption Algorithm: The encryption algorithm is the cryptographic cipher used to encrypt the plaintext under credentials. This way, even if data is intercepted, it will be impossible to read without the encryption key.
3) Key Management: Key management is the management of the generation, distribution, and storage of encryption keys. This process is key to securing and decrypting information to allow only the proper parties to access it.
4) Message Integrity: This includes checks to guarantee that the message received is the same as the one sent. This prohibits the data from being tampered with once it leaves your device[5].

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VI June 2025- Available at www.ijraset.com

III. EXAMPLE OF PROTOCOL SECURITY

1) SSL (Secure Sockets Layer): SSL is a protocol, originally developed by Netscape, that secures Internet communications and is the predecessor to TLS (Transport Layer Security). It provides privacy and data authenticity for all transactions between the application and transport layer across the internet. SSL is composed of sub-protocols, e.g. the Handshake Protocol, the Record Protocol and the Alert Protocol 47.
2) TLS (Transport Layer Security): Like SSL, TLS[3] is commonly used to secure the privacy and integrity of data over the internet. It generates a master secret (for encryption between) the client and server.
3) IPsec (Internet Protocol Security): This notifies the system how to secure the data exchange over the public network, including encrypting and authenticating each network packet. This includes formats such as ESP for encryption and AH for integrity traffic[6].
4) Kerberos: It is a protocol developed to authenticate requests for a service on untrusted networks like the Internet. It verifies requests/requests between trusted hosts and is a core part of services such as AD.
5) SNMP (Simple Network Management Protocol): At the application layer, SNMP takes care of network device management and monitoring. It prevents network-attached devices from being secured (for LAN or WAN) and it has back a couple of important security features: encryption, integrity check, and authentication, starting with the introduction of SNMPv3.
6) SFTP (Secure File Transfer Protocol): A network protocol called Secure File Transfer Protocol (SFTP) allows for safe files management, access, and transfer across any dependable data stream. In order to provide secure file transfer capabilities, the Internet Engineering Task Force (IETF) created it as an addition to the Secure Shell (SSH) protocol version 2.01. Because of its better security characteristics, SFTP is sometimes considered a substitute for the conventional File Transfer Protocol (FTP). Encryption, authentication, data integrity, advanced file operation, and platform independence are just a few of its benefits.

IV. LAYERS OF SECURITY PROTOCOLS

1) *Security at the application layer:* The top layer of the OSI model, where standard internet requests like HTTP GET and HTTP POST take place, is the target of application layer assaults, commonly referred to as Layer 7 (L7) attacks[1]. By taking advantage of application layer 2 software flaws, these attacks seek to interfere with the regular flow of traffic to a website or service. Application layer attacks are especially effective with less total bandwidth because, in contrast to network layer attacks, they use server resources in addition to network resources.

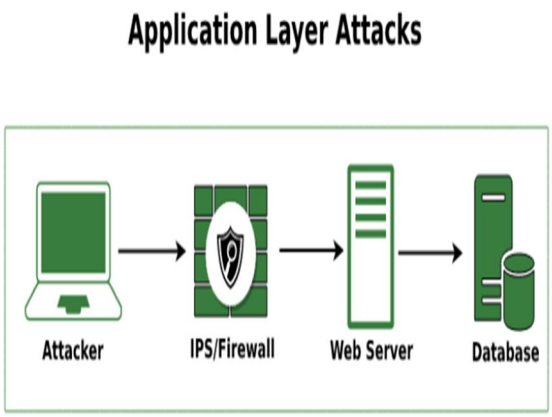


Fig:2 illustrate of attacks2

2) *Transport Layer Security:* TLS is a cryptographic protocol that facilitates safe communication across a network of computers. It guarantees data integrity, privacy, and authentication between two applications that are in communication. Although TLS is widely used in many other applications, including voice over IP (VoIP), email, and instant messaging, its most obvious use is in safeguarding HTTPS connections on the web12. Integrity, authentication, and encryption are essential elements of TLS.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

A. How do TLS and SSL vary from one Another?

Secure Sockets Layer (SSL), a prior encryption technology created by Netscape, was the ancestor of TLS. Although TLS version 1.0 was initially developed as SSL version 3.1, the protocol's name was altered before to release to reflect that it was no longer connected to Netscape. Because of this history, the terms TLS and SSL are sometimes used interchangeably.

- Network layer security: Since network layer security rules may cover several programs simultaneously without changing them, they have been widely utilized to secure communications, especially over shared networks like the Internet. To make up for the inherent lack of security in standard Internet Protocols, the majority of these protocols continued to concentrate on the higher layers of the OSI protocol stack. Despite their value, these techniques are difficult to generalize for use in any situation. For instance, SSL was created especially to protect programs like FTP and HTTP. However, secure communications are also required for a number of other applications. This requirement led to the creation of an IP-layer security solution that all higher-layer protocols could utilize. The Internet Engineering Task Force[3] (IETF) started working on an IPsec standard in 1992.

Summary Table: SSL vs TLS vs IPsec

Feature	SSL	TLS	IPsec
Layer	Transport/Application	Transport/Application	Network
Status	Deprecated	Current standard	Widely used for VPNs, secure IP
Main Purpose	Web security (historical)	Web, email, VoIP security	Secure IP packet transmission
Encryption	✅	✅	✅
Authentication	✅	✅	✅
Integrity	✅	✅	✅

V. WHY SECURITY PROTOCOLS ARE IMPORTANT

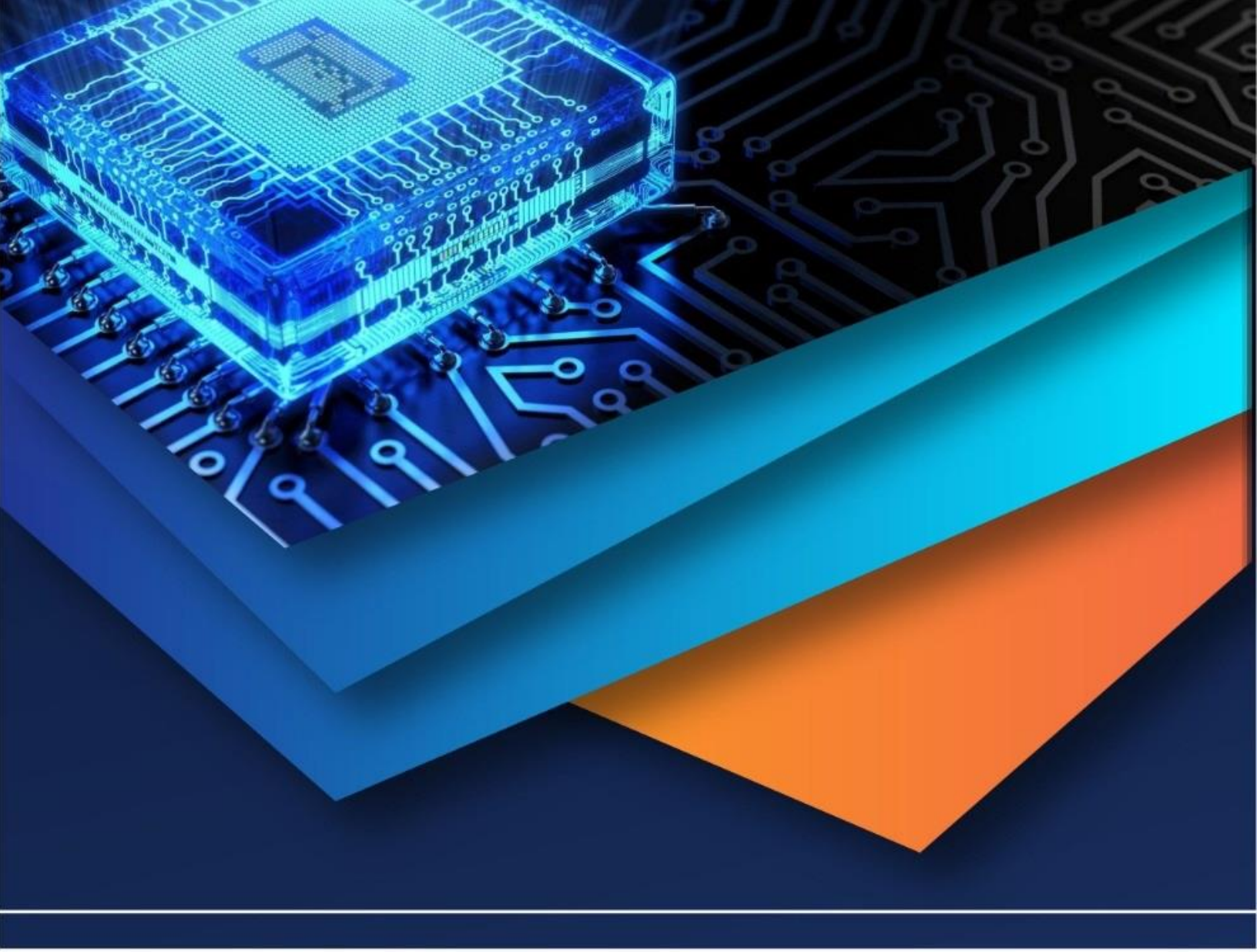
In the current digital environment, where data breaches and cyber threats are common, security practices are essential. They offer an organized method of data security, guaranteeing that private information is kept safe and undamaged from the place of origin to the final destination. Organizations can guard against many types of cyber-attacks, data leaks, and illegal access by putting strong security procedures in place.

VI. CONCLUSION

The foundation of data protection in network communications is security protocols. They create a secure environment for data transmission across many platforms and devices by using a variety of techniques to manage keys, encrypt data, authenticate users, and preserve message integrity. Give an overview of the significance of security protocols in network design, emphasizing the necessity of strong security measures to fend against changing threats.

REFERENCES

[1] http://www.cloudflare.com/learning/ddos/Application layer DDoS attack | Cloudflare
[2] http://www.geeksforgeeks.org/ethical-hacking/application-layer-attacks
[3] http://en.wikipedia.org/wiki/Transport_layer_security
[4] https://www.conceptdraw.com/How-To-Guide/picture/Computer-and-Networks-Network-Security-Diagrams-Recommended-Network-Architecture.png
[5] http://www.emgywomancollege.ac.in/templateEditor/kcfinder/upload/files/Network Security Essentials: Applications and Standards (Fourth edition) by William Stallings.
[6] James F Kurose and Keith W Ross, Computer Networking, A Top-Down Approach, Sixth edition,Pearson,2017 .



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)