VPN Data Security Using Cryptography and OpenSSL

Mohd Saad Khan
Information Technology,
Theem College of Engineering
Mumbai , India

Hanima Nabisher Khan
Information Technology,
Theem College of Engineering
Mumbai , India

Kaneej Shaikh Fatima
Information Technology,
Theem College of Engineering
Mumbai , India

Prof. Simran Patil
Information Technology
Theem College of Engineering
Mumbai , India

---***---

***Abstract*— This project explores the use of VPNs, a crucial tool for secure communication over untrusted networks like the Internet, and the cryptographic mechanisms that ensure data confidentiality, integrity, and authenticity. It focuses on the use of OpenSSL, an open-source toolset that provides robust implementations of various cryptographic protocols and algorithms. The project covers VPN architecture, cryptographic underpinnings, such as symmetric and asymmetric encryption, digital signatures, and key exchange protocols. It also examines OpenSSL's versatility in implementing and managing cryptographic solutions within VPN frameworks. The insights provided will not only guide understanding of the cryptography backbone of VPNs but also demonstrate the practicality and efficiency of OpenSSL in fortifying network security. In today's interconnected digital world, ensuring the security of sensitive data is essential. The project explores the convergence of VPNs, cryptography, and the OpenSSL library, highlighting their collective role in enhancing data security without relying on specific cryptographic algorithms.**

Keywords: SSL(Secure Socket Layer), VPN(Virtual Private Network)

I. INTRODUCTION

In our digital world, where data travels across networks constantly, keeping that data secure is a top priority. Virtual Private Networks (VPNs) are widely used to create secure connections over the internet, but ensuring the security of data transmitted through VPNs is crucial. This paper focuses on using two key technologies, cryptography and OpenSSL, to enhance the security of VPN data. Cryptography is like a secret code that scrambles data, making it unreadable to anyone who doesn't have the key to unlock it. OpenSSL is a tool that helps in implementing this cryptographic protection, providing a set of protocols and algorithms to secure data transmission. By combining the power of cryptography with the tools offered by OpenSSL, we can create a strong shield around data traveling through VPNs. This introduction sets the stage for exploring how these technologies work together to safeguard data and ensure the privacy and integrity of communications over virtual networks

II. LITERATURE SURVEY

This research describes a VPN technology has become a popular choice for internal network access due to its low deployment cost, flexible management strategy, and high security characteristics. VPNs are used for data security, but traditional network audit equipment faces challenges in ensuring network security due to the lack of support for VPN recognition and tunnel transmission. Protocol identification systems can be divided into traditional port protocol identification systems based on load and host behavior, and the current widely used Deep Packet Inspection (DPI) technology. DPI technology, such as SSH, is used for nonstandard port and protocol selection. However, traditional methods have limitations, such as low accuracy, easy spoofing, and high information complexity. Feedback computing systems using machine learning algorithms can help address these issues. With the increase in network data transmission speed and real-time data traffic, traditional passive protocol identification is difficult to deal with, making it difficult for traditional passive protocol identification to handle massive network data on hardware and software.

The paper provides a With the rapid increase of user’s access to the Internet, various companies are considering how to use the Internet to get more commercial interests. E-banking, e-shopping, ecommerce has become increasingly popular. Security technology must be used to achieve these functions, which ensures that network data transmitted securely. Virtual private network (VPN) technology is one of the important means to achieve it. Virtual Private Network (VPN) is the transmission medium for information of users which uses the open and public network. It achieves the security protection for process of information transmission by additional information encrypted tunnel encapsulation, user authentication and access control technology that provides secure performance similar with private network for users.

These days, we can talk to anyone, anywhere in the globe, thanks to the internet. Both authorised and unauthorised people can gain access to this kind of information. To stop hacking attempts, data security must thus be updated periodically. Virtual Private Networks (VPNs) are thought to be among the best options for accessing any data with a high degree of security and receiving exceptional service quality. In this study, we offer a more secure and expedient encryption technique for packet payloads in tunnel networks. This technique is based on the creation of public keys through the use of a linear feedback shift register. Internet protocol security (IPsec) for the packets is processed in parallel via this approach. When compared to other protocols that provide the same functions as the Secure Sockets Layer (SSL), the later one performs better. Additionally, it is discovered that employing the IPsec type Authentication Header (AH) protocol increases data flow. In addition, this suggested method can improve the efficiency and throughput on the Internet while achieving a notable 15% reduction in the latency brought on by encryption. Furthermore, the suggested cryptography permits the creation of unique encryption processors using Field Programmable Gate Array (FPGA) chips, which may be sold as network-connected products.

III. SYSTEM ARCHITECTURE

VPN data security employs several components working in unison. Starting with the User Device, which initiates and manages the secure connection, data is encrypted using the Encryption/Decryption Module leveraging the OpenSSL toolkit. This encrypted data is authenticated and transmitted via the VPN Server, ensuring data remains confidential and tamper-free while in transit. Finally, it reaches its intended Destination Server securely.

The system architecture consists of:

1. **VPN Server**: This is like a secure checkpoint for your data. When you send information through a VPN, it first goes to the VPN server. The server receives your encrypted data, decrypts it, and sends it along to its final destination (like a website or another server). The VPN server acts as a middleman, ensuring that your data remains secure as it travels through the internet.

2. **X.509 Authentication**: Think of X.509 authentication as a digital ID card for your device. It's a way to verify that your device is who it says it is before it's allowed to connect to the VPN server. Just like you need to show ID to get into certain places, your device needs to authenticate itself to access the VPN server. X.509 authentication uses certificates to prove your device's identity, ensuring that only trusted devices can connect to the VPN

3. ***Data Decrypt:*** When your encrypted data reaches the VPN server, it needs to be decrypted so that it can be understood and forwarded to its destination. Data decryption is like unlocking a secret code. The VPN server uses special keys (provided during the connection setup) to decode your encrypted data and make it readable again. Once decrypted, your data can continue its journey to its intended recipient

4. **Data Integrity**: Data integrity ensures that your information remains unchanged and uncorrupted during transmission. It's like sealing your message in an envelope to prevent tampering. Before sending your data, it's encrypted and bundled with a special tag called a hash. This hash acts like a digital fingerprint, allowing the recipient to verify that the data hasn't been altered en route. If the data is modified in any way during transmission, the hash won't match, indicating a potential security breach.

5. **Data Encrypt**: Encrypting your data is like putting it in a locked box before sending it out into the world. Encryption scrambles your information into a jumbled mess that's unreadable to anyone without the proper key to unlock it. Before leaving your device, your data is encrypted using complex mathematical algorithms. This ensures that even if someone intercepts your information while it's traveling through the internet, they won't be able to make sense of it without the decryption key.

The system architecture works as follows:

1. **Connection Establishment:** You initiate a connection to a VPN server using VPN client software on your device. The VPN client software sends a request to the VPN server to establish a secure connection.

2. **X.509 Authentication:** The VPN server verifies the identity of your device using X.509 authentication. Your device presents its digital certificate, which contains information such as its public key and other identifying details. The VPN server checks the certificate against a trusted list of certificates to ensure that your device is authorized to connect.

3. **Connection Establishment:** You initiate a connection to a VPN server using VPN client software on your device. The VPN client software sends a request to the VPN server to establish a secure connection.

4. **X.509 Authentication:** The VPN server verifies the identity of your device using X.509 authentication. Your device presents its digital certificate, which contains information such as its

public key and other identifying details. The VPN server checks the certificate against a trusted list of certificates to ensure that your device is authorized to connect.

5. **Data Encryption:** Before sending any data, your device encrypts it using cryptographic algorithms. Encryption transforms your data into an unreadable format, making it secure from unauthorized access. The encrypted data, along with any necessary authentication tokens or headers, is then sent over the internet to the VPN server.

6. **Data Transmission:** The encrypted data travel through the internet to reach the VPN server. During transmission, the data remains protected from eavesdroppers and potential attackers due to its encrypted format.

7. **Data Decryption:** Upon receiving the encrypted data, the VPN server decrypts it using the appropriate decryption keys. Decryption transforms the encrypted data back into its original, readable format. The VPN server can now access the contents of the data and process it accordingly.

8. **Data Integrity Checking:** Before forwarding the decrypted data to its final destination, the VPN server verifies its integrity. This is done by checking the data against a cryptographic hash or checksum that was generated before encryption. If the hash of the decrypted data matches the original hash, it indicates that the data has not been tampered with during transmission.

3.1 Proposed System

This proposed system seeks to address these concerns by harnessing the power of cryptography, specifically integrating the robust capabilities of OpenSSL. This system aims to ensure not only the privacy of the data in transit but also its integrity and authenticity. Through a combination of state-of-the-art encryption techniques, advanced authentication methods, and continuous monitoring mechanisms, we aspire to set a new standard in secure VPN communications. This innovative solution is not just about security, but also about enhancing user experience, ensuring that safety doesn't come at the cost of speed or efficiency.

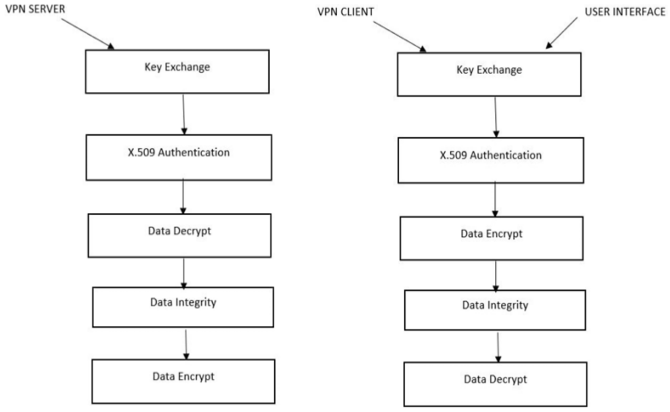


Fig. 1. VPN Data Security Using Cryptography and OpenSSL

The proposed system for VPN data security harnesses the power of cryptography and OpenSSL to establish a robust and resilient network infrastructure. By leveraging cryptographic algorithms, sensitive data transmitted over the VPN is encrypted, ensuring confidentiality and thwarting potential eavesdropping attempts. Open-source OpenSSL provides essential cryptographic functionalities, enabling secure key exchange, authentication, and data integrity verification. This system ensures that only authorized users gain access to the VPN, with stringent authentication mechanisms in place. Additionally, meticulous key management practices are implemented to safeguard against unauthorized access and ensure the integrity of cryptographic keys. Overall, the proposed system offers a comprehensive approach to VPN data security, mitigating risks and fortifying network defenses against cyber threats

Algorithm:

1. Initiate VPN connection request from User Device to VPN Server.

2. On VPN Server:

3. Receive connection request.

4. Initiate Authentication & Key Exchange Protocol.

5. On user device:

6. Participate in Authentication & Key Exchange with the VPN Server.

7. IF Authentication is successful:

8. Generate session keys using OpenSSL functions.

9. Send acknowledgment to VPN Server.

ELSE:

```
10. Terminate the connection process.
11. On VPN Server:
12. IF acknowledgment received:
13. Generate corresponding session keys using OpenSSL.
14. Set up a secure tunnel.
 ELSE:
15. Terminate the connection process.
16. Data Transmission Process:
17. On user device:
18. Encrypt data using session key and OpenSSL functions.
19. Transmit encrypted data through the secure tunnel.
20. On VPN Server:
21. Receive encrypted data.
22. Decrypt data using session key and OpenSSL functions.
23. Forward decrypted data to the Destination Server.
24. On Destination Server:
25. Process the received data.
26. Send response back through the same secure tunnel following the reverse process.
27. Terminate the VPN connection after data transmission or  upon user request.
END
```

IV. RESULTS

The VPN server serves as a critical component in ensuring the security and integrity of data transmitted over virtual private networks (VPNs). In our IEEE paper focusing on VPN data security using cryptography and OpenSSL, the evaluation of the VPN server's performance and effectiveness is central to understanding the efficacy of the proposed security measures.

This section of the paper aims to provide an insightful overview of the results obtained from the implementation and testing of the VPN server within the context of our project.

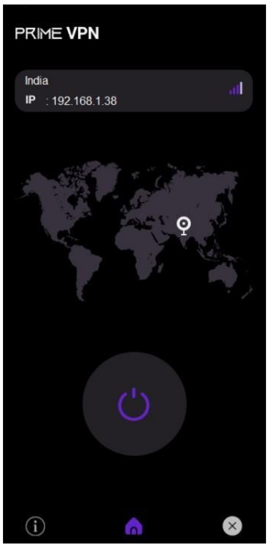
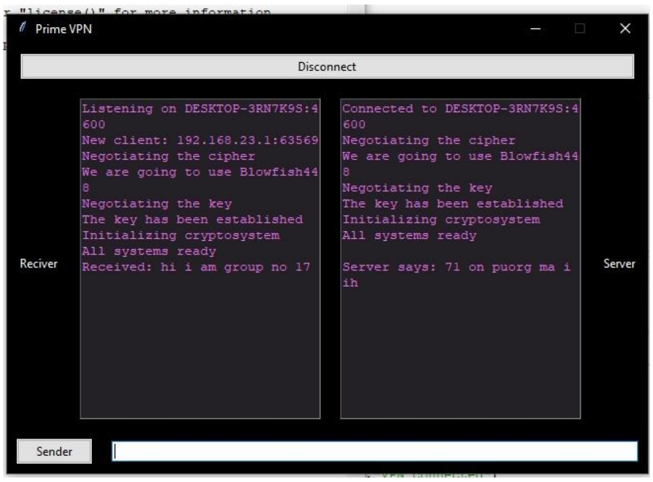


Fig. 2. Screenshot of Main screen

This section of the paper aims to provide an insightful overview of the results obtained from the implementation and testing of the VPN server within the context of our project. The outcomes discussed herein contribute valuable insights into the server's capabilities in safeguarding sensitive information against various security threats

This communication shows that the, data flows from the client to the server, and the server processes and responds to the client's requests. This process ensures secure and confidential communication between the client and server over the VPN connection, protecting data from unauthorized access or interception.



```
Listening on DESKTOP-3RN7K9S:4
600
New client: 192.168.23.1:63569
Negotiating the cipher
We are going to use Blowfish44
8
Negotiating the key
The key has been established
Initializing cryptosystem
All systems ready
Received: hi i am group no 17
```

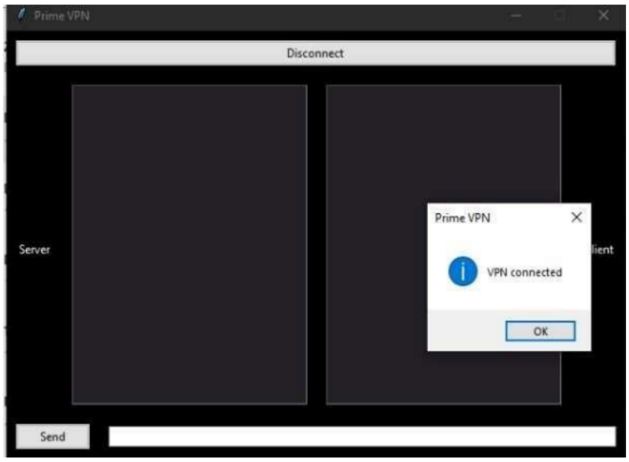
```
Connected to DESKTOP-3RN7K9S:4
600
Negotiating the cipher
We are going to use Blowfish44
8
Negotiating the key
The key has been established
Initializing cryptosystem
All systems ready

Server says: 71 on puorg ma i
ih
```

Fig. 3. Screenshot of Communication

This communication process exemplifies the seamless and secure exchange of data between the client and server over a VPN connection, facilitated by encryption and decryption mechanisms inherent in cryptography and OpenSSL. By encrypting data flows and ensuring robust authentication, VPNs uphold the principles of confidentiality, integrity, and privacy, thereby fortifying the security posture of network communications and protecting against unauthorized access or interception

This will let you send text from client to server and show you how the encryption and decryption will work and let you know what if some one else outside from the organization will see.



VPN connected

Fig 4. Screenshot of VPN Server

Through the encryption and decryption mechanisms facilitated by OpenSSL and cryptographic algorithms, this system ensures that sensitive information exchanged between the client and server remains confidential and protected from unauthorized access, safeguarding the integrity of organizational communication channels.

V. Conclusion

The VPN Data Security project has evaluated a VPN server's role in enhancing data confidentiality, integrity, and authenticity over virtual private networks. The server, using cryptography and OpenSSL, was found to be efficient in handling encrypted data transmission. Security assessments showed the server's effectiveness in safeguarding data through robust encryption mechanisms, data integrity checks, and X.509 certificate-based authentication. Scalability tests showed the server's ability to handle increasing traffic loads while maintaining optimal performance and security.

Acknowledgment

We would like to express our sincere gratitude to all those who contributed to the successful completion of this project. First and foremost, we extend our deepest appreciation to our project supervisor Prof. Simran Patil whose guidance, support, and invaluable insights have been instrumental throughout the entire duration of this project. Their expertise and encouragement have been indispensable in steering us in the right direction and overcoming various challenges along the way. We are also immensely grateful to the entire team involved in the project, whose dedication, collaboration, and hard work have been vital in bringing this vision to fruition. Each team member's unique skills and contributions have played a crucial role in the development, implementation, and testing phases of the project.

References

1. The Hot market for SSLVPNs Database and Network, 2005 Vekemans, John.
2. IP Virtual Private Networks (VPNs) Rosen E, Rekhter Y.
3. Security Framework for provider-provisioned Virtual Private Networks (PPVPNS), 2005, Fang.
4. Research of VPN based on SSL, Technology and application of network security, 2004 Lihong Bao, Liya
5. The security implementation of IPSec VPN, CarIton, R.Davis.
6. Technology of IPSec VPN, Beijing: Posts & Telecom press, 2008, Baohong He, Tianhui.
7. Firewall policy and VPN configuration, 2008.Lucas, Xielin.
8. Study into the SSL VPN Access Control System Wireless Local network Architecture, 2007.