

Comparative Analysis of PSK and PKI-Based IPsec VPNs



MCS

Author

Maj Athar Shahzad

00000398002

Supervisor

Asst Prof Dr Waleed bin Shahid

A thesis submitted to the faculty of Department of Computer Software Engineering, Military College of Signals, National University of Sciences and Technology (NUST), Rawalpindi in partial fulfillment of the requirements for the degree of MS in Software Engineering

(October, 2023)

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS Thesis written by **Mr. Athar Shahzad**, Registration No. **00000398002**, of **Military College of Signals** has been vetted by undersigned, found complete in all respects as per NUST Statutes/Regulations/MS Policy, is free of plagiarism, errors, and mistakes and is accepted as partial fulfillment for award of MS degree. It is further certified that necessary amendments as pointed out by GEC members and local evaluators of the scholar have also been incorporated in the said thesis.

Signature: Salad
Name of (Supervisor) _____
Date: _____

Signature (HOD): Asif Masood Brig
Head of Dept of CSE
Mil College of Signals (NUST)
Date: 14/11/23


Signature (Dean/Principal) Asif Masood Brig
Dean, MCS (NUST)
(Asif Masood, Phd)
Date: 15/11/23

Declaration

I Maj Athar Shahzad, declare that this thesis titled “Comparative Analysis of PSK and PKI based IPsec VPNs” and the work presented in it are my own and has been generated by me as a result of my own original research.

I confirm that: -

1. This work was done wholly or mainly while in candidature for a master of science degree at NUST.
2. Where any part of this thesis has previously been submitted for a degree or any other qualification at NUST or any other institution, this has been clearly stated.
3. Where I have consulted the published work of others, this is always clearly cited.
4. Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
5. I have acknowledged all main sources of help.
6. Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.



Maj Athar Shahzad

Dedication

This Thesis is dedicated to my beloved Parents, Children and my beloved Wife, who all have been my endless source of love, encouragement, and strength. Your unwavering beliefs in my abilities, countless sacrifices, and relentless support have been the foundation upon which I built my academic pursuits. Without their love and support this research work would not have been made possible.

Abstract

The rapid expansion of digital communication and the increasing need for secure data transmission have made Virtual Private Networks (VPNs) an essential tool in modern networking. IPsec (Internet Protocol Security) is a widely adopted framework for securing communications over the Internet. Within the IPsec framework, there are two primary authentication methods: Pre-Shared Key (PSK) and Public Key Infrastructure (PKI). This thesis presents a comprehensive comparative analysis of PSK and PKI based IPsec VPNs to evaluate their performance, security, scalability, and usability. The study involves the implementation of both PSK and PKI VPNs, followed by an extensive examination of their strengths and weaknesses in various real-world scenarios. The results of this analysis aim to provide valuable insights for network administrators, security experts, and decision-makers in selecting the most appropriate authentication method for their specific networking requirements.

Key Words: Pre-shared key, Public Key infrastructure, Virtual Private Network, Internet Protocol Security

Acknowledgments

In the name of Allah (S.W.A), the Creator and Sustainer of the Universe, to whom belongs all glory and power. He alone has the authority to elevate and humble individuals as He pleases. Truly, nothing can be accomplished without His will. From the moment I stepped foot into NUST until the day of my departure, it was by His divine blessings and guidance that I was able to navigate the path of success. His unwavering support and the opportunities He bestowed upon me were instrumental in completing my research journey.

I humbly acknowledge that no words or actions can fully express my gratitude for the countless blessings He has showered upon me throughout this research period. I am indebted to His boundless bounties and am forever grateful for His divine intervention in my academic pursuits. To Allah (S.W.A), I dedicate this thesis as a humble tribute, recognizing His infinite wisdom and benevolence. It is through His mercy that I have reached this milestone, and I pray that my work may be of benefit to others and serve as a means of pleasing Him.

I would also like to express my heartfelt appreciation to my thesis supervisor, **Assistant Professor Dr. Waleed bin Shahid**, for his unwavering support and guidance throughout my thesis. His knowledge, expertise, and dedication to his field have been a source of inspiration to me, and I am grateful for the time and effort he invested in my success. Whenever I encountered any difficulties, he was always available to offer his assistance and provide me with insightful feedback.

In addition, I extend my gratitude to my GEC member, **Col Imran Makhdoom, PhD** and **Assistant Professor Dr. Fawad Khan**, for their continuous availability for assistance and support throughout my thesis. Their expertise and knowledge have been invaluable to me, and I am grateful for their unwavering support and guidance.

Lastly, all praises and thanks be to Allah (S.W.A), the Most Merciful and the Most Gracious.

Contents

Chapter 1.....	1
Introduction	1
1.1 Overview	1
IPsec as a Security Framework.....	3
Role of PKI in IPsec.....	3
Utility of PKI and IPsec in VPNs	4
1.2 Motivation.....	6
1.3 Research Objectives.....	8
1.4 Relevance to National needs	8
1.5 Area of Application	12
1.6 Advantages.....	13
1.7 Thesis Organization.....	14
Literature Review	16
2.1 Introduction	16
2.2 Explanation of Literature Review	16
2.3 Importance of Comparative Analysis.....	17
2.4 Introduction to VPNs.....	18
2.4.1 Definition. VPN is a temporary physical path created over a public network having a mesh architecture. Data transmission through a VPN can be referred to as virtual private networking (VPN). This basic definition of VPNs does not deliberate the layer of OSI model in which the VPN is operating. VPNs operate mostly at layer 2 and layer 3 of the OSI model. But there are VPNs that operate at layer at layer 4,5 to 7 as well.....	18
2.5 Overview of IPsec.....	23
2.6 Previous Research's	28
Chapter 3.....	40
Overview of Proposed Frame Work	40
3.1 Introduction	40
3.2 Overview of Proposed Model	49
Implementation Of Proposed Model	50
Results And Analysis.....	55
Chapter 5.....	60
Conclusion And Future Work	60
References.....	62

List of Figures

Figure 1: Block Diagram of IPsec Based VPNs	5
Figure 2: Block Diagram of PKI Based IPsec VPNs.....	6
Figure 3: Targeted Organizations.....	9
Figure 4: PKI Survey Background.....	10
Figure 5: Taxonomy of thesis.....	15
Figure 6: Working of IPsec	24
Figure 7: Phases of IKE	27
Figure 8 Device Ethereum- Blockchain communication.....	30
Figure 9: Gavin-Lowe Protocol for PSK Key Exchange.....	32
Figure 10: PKI4IoT from a communication perspective	33
Figure 11: VPNalyzer Architecture.....	36
Figure 12: Architectural Diagram of Proposed Framework	54

List of Tables

Table 1 Pros and Cons of PSK and Certificates.....	2
Table 2 Comparison of Remote Access and site to site VPNs	18
Table 3 Protocols supporting VPN creation	22

Chapter 1

Introduction

1.1 Overview

In the rapidly evolving landscape of digital communication and data exchange, ensuring the security and confidentiality of sensitive information has become paramount. Organizations, individuals, and governments alike are faced with the daunting challenge of protecting their data as it traverses networks that are inherently susceptible to interception and unauthorized access [1]. In response to this pressing need, Virtual Private Networks (VPNs) have emerged as a fundamental technology for establishing secure and private communication channels over untrusted networks, such as the Internet. With the use of a Virtual Private Network (VPN), users can connect securely and securely over a public network, usually the internet, as if they were directly linked to a private network. A VPN essentially establishes a secure tunnel via which information can be sent, ensuring the privacy, confidentiality, and security of the data being transferred between the user's device and a distant server or network. VPNs are frequently used to safeguard sensitive data, preserve online anonymity, and provide secure access to resources housed on private networks or in other locations [2].

One of the most robust and widely adopted protocols for achieving secure communication within VPNs is the Internet Protocol Security (IPsec) protocol suite [3]. IPsec provides a comprehensive framework for implementing strong authentication, data encryption, and integrity verification, thereby creating a secure tunnel through which data can flow between remote endpoints. This technology has become an

essential component of modern network infrastructure, enabling remote workers to access corporate resources, facilitating secure communication between geographically separated branches of an organization, and ensuring the confidentiality of sensitive data for individuals seeking privacy online. IPsec has mainly two ways of authenticating a peer via a pre-shared key or by using certificates. Both the approaches have their pros and cons which are shown in table below

Table 1 Pros and Cons of PSK and Certificates

Pre-shared keys	
Advantages	
<ul style="list-style-type: none"> • Convenience--no need to go through the complicated process of obtaining a certificate 	
Dis-advantages	
<ul style="list-style-type: none"> • key compromise can result to unauthorized access to the network. • As the key is stored on all the IPsec peer systems it is more vulnerable to get detected. • If a pre-shared key is compromised there is no way to automatically notify the IPsec peers. • Replacing the pre-shared key requires updating it on all systems, which involves a lot of effort and time • Pre-shared keys are limited to a maximum size of 64 bytes (512 bits) 	
Certificates	
Pros	
<ul style="list-style-type: none"> • The key used to generate certificates is stored in a single location, separate from the systems using the certificates • All systems may be notified of a certificate's compromise via a certificate revocation list (CRL) 	

- | |
|---|
| <ul style="list-style-type: none">• A compromised certificate only needs to be replaced on the system to which the certificate belongs• The public key embedded in a certificate may be larger than a pre-shared key (1024, 2048, 4096, or more) |
|---|

Cons

- | |
|--|
| <ul style="list-style-type: none">• Creating/obtaining a certificate is more complicated, time consuming and potentially expensive than using a pre-shared key |
|--|

IPsec (Internet Protocol Security) and PKI (Public Key Infrastructure) are two distinct but closely related technologies often used together to provide secure communication and data protection in various networking scenarios, including Virtual Private Networks (VPNs). Here's how IPsec and PKI are related:

IPsec as a Security Framework

IPsec is a suite of protocols and standards designed to secure IP communication by offering features such as authentication, data encryption, and integrity verification. IPsec ensures that data exchanged between two devices over a network remains confidential, tamper-proof, and can be authenticated to prevent unauthorized access [4].

Role of PKI in IPsec

PKI is a framework that facilitates the management of digital certificates and keys used in encryption and authentication processes. It includes a hierarchy of entities, including Certificate Authorities (CAs), that issue digital certificates to validate the identity of users, devices, or servers. [5]

In the context of IPsec, PKI plays a critical role in several aspects.

Authentication: IPsec requires a strong mechanism to authenticate the identities of devices participating in a communication. PKI provides this by issuing digital certificates to devices, enabling them to prove their identity to each other. When two devices establish an IPsec connection, they present their certificates to verify their authenticity.

Key Exchange: IPsec needs a secure method for exchanging encryption keys to establish a secure tunnel. PKI helps in this process by using asymmetric encryption. Devices can use each other's public keys from their certificates to securely exchange a shared session key, which is then used for symmetric encryption during the IPsec communication.

Data Encryption and Integrity: IPsec uses encryption algorithms to guarantee the integrity and confidentiality of data. Digital certificates from the PKI are used to check the encrypted data's integrity and make sure it wasn't altered while being transmitted.

Revocation and Trust Management: PKI allows for the revocation of compromised or expired certificates. In IPsec, the CA can revoke the relevant certificate if a device's certificate or private key is compromised. Even if an attacker already has access to the compromised credentials, this prevents illegal access.

Utility of PKI and IPsec in VPNs

In VPNs, whether between two machines, a machine and a network, or two networks, IPsec is commonly used to create secure communication tunnels. PKI ensures the secure setup of these tunnels by providing strong authentication, secure key exchange, and encryption mechanisms.

In summary, IPsec and PKI are intertwined technologies in the realm of network security. While IPsec forms the foundation for secure communication, PKI provides

the necessary tools and infrastructure for secure authentication, key exchange, and data protection, contributing to the overall robustness of IPsec-based security solutions like VPNs.

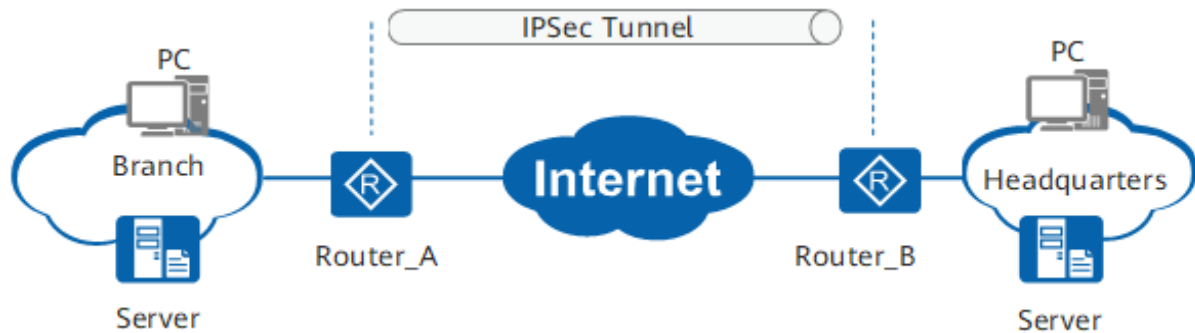


Figure 1: Block Diagram of IPsec Based VPNs

The main objective and inspiration behind this research are to carry out analysis of PSK and PKI based IPsec VPNs with a view to highlight the tradeoffs and benefits that can be drawn by implementing them in Air Gapped Systems. Figure 1 represents block diagram of PKI Based IPsec VPNs. During the course of our research, we carried out following work: -

- During the course of research an open-source implementation of CA was customized as per our specific needs.
- We created certificates and different networking devices were given certificates so that they can authenticate themselves while communicating and while establishing VPNs for secure communication.
- Firewalls which support certificates were given certificates through CA and PSK and PKI based IPsec VPNs were established for comparative analysis.
- A comparative Analysis of PSK and PKI based IPsec VPNs was carried out to analyze their strengths and weaknesses and the factors such as security

requirements, scalability, complexity, and management preferences were analyzed.

- RA application was developed for registration of users and equipment's and allocation of digital certificates.
- Code Signing application was developed for authentication of software applications.

Basing on the comparative analysis we suggested that PKI is secure mechanism but there are some issues in this approach and one of the significant issues is the latency issue. In order to address this issue, we have proposed a framework for reducing the latency issue in PKI based IPsec VPNs.

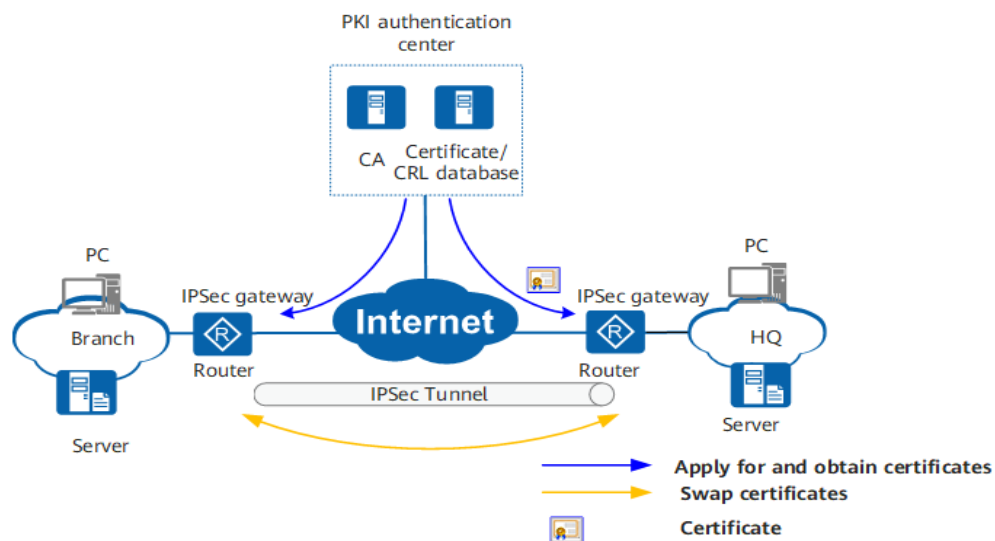


Figure 2: Block Diagram of PKI Based IPsec VPNs

1.2 Motivation

Security Enhancement and Risk Mitigation: The core motivation behind this comparative analysis is to assess the security landscape of PSK and PKI-based IPsec

VPNs. Security remains a top concern for organizations as cyber threats continue to evolve. By understanding the nuanced security features of these two authentication methods, we can provide valuable insights into their ability to thwart emerging cyber threats and safeguard sensitive information.

Operational Efficiency: The operational efficiency of any security solution directly impacts an organization's productivity. A thorough comparative analysis will provide insights into the ease of deployment, scalability, and management of PSK and PKI-based IPsec VPNs. Organizations can then make informed decisions about which approach aligns better with their operational requirements and resource constraints.

Performance and Latency: In the age of real-time applications and data-intensive tasks, network performance is critical. Comparing the performance of PSK and PKI-based IPsec VPNs can uncover potential bottlenecks and latency issues associated with each authentication method. This knowledge is essential for organizations seeking to maintain optimal network performance while ensuring data security.

Regulatory Compliance: Different industries and regions have varying compliance requirements pertaining to data security and privacy. By dissecting the regulatory implications of using PSK and PKI-based IPsec VPNs, this analysis can guide organizations in adhering to relevant regulations and standards while choosing the most suitable authentication method.

Future-Proofing: Technology is in a state of constant evolution. A thorough analysis of PSK and PKI-based IPsec VPNs can shed light on their adaptability and readiness for future security challenges. Understanding how these methods fare against emerging threats and technological advancements can help organizations invest wisely in long-term security solutions.

Decision-Making for Diverse Use Cases: Different organizations have varying needs and use cases for VPNs. By comparing the characteristics of PSK and PKI-based IPsec VPNs, this study will empower decision-makers to select the authentication method that aligns with their specific requirements, whether it's a small business looking for simplicity or a large enterprise demanding heightened security.

In an era where the digital realm is expanding exponentially, the importance of secure and reliable network communication cannot be overstated. The comparative analysis of PSK and PKI-based IPsec VPNs serves as a beacon, guiding organizations towards a better understanding of the trade-offs between security, performance, compliance, and operational efficiency. By shedding light on the unique strengths and limitations of each authentication method, this study empowers decision-makers to make well-informed choices that resonate with their organization's overarching goals and values.

1.3 Research Objectives

The main objectives of this research work are: -

To evaluate the security strength of IPsec implemented with PKI and PSK in context of Air Gapped System.

Analyze performance differences between PKI and PSK implementations of IPsec.

Analyze usability of various implementation of IPsec and provide recommendations for improving user experiences.

1.4 Relevance to National needs

More than 133 local organizations with both domestic and foreign operations were included in a 2009 study [5] that was conducted. IT and telecom-related businesses

were the main focus. Out of these 133, only the 55 organizations with some level of PKI installation were considered. According to the figure, the IT, financial/banking, government/public, and telecom sectors each have 43%, 26%, 17%, and 14% of the targeted organizations, respectively.

However, of these 55 firms, 20 (36%) had not yet deployed PKI but had planned to do so soon, and 35 organizations (64%) were at various stages of PKI deployment. 20 (57%) of the 35 organizations were implementing PKI, while 15 (43%) of them had already done so.

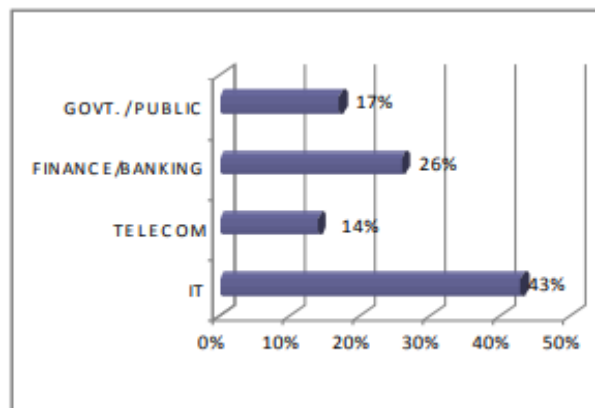


Figure 3: Targeted Organizations

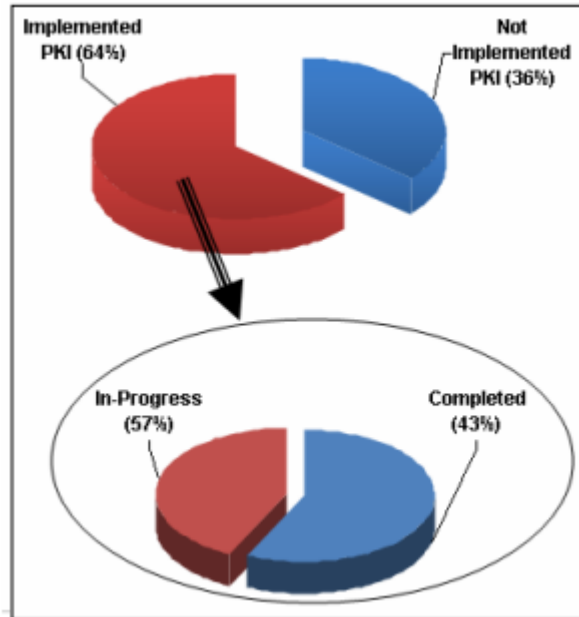


Figure 4: PKI Survey Background

When conducting a comparative analysis of PSK (Pre-Shared Key) and PKI (Public Key Infrastructure) based IPsec VPNs with relevance to the national needs of Pakistan, several key factors [6] should be considered:

Security and National Defense: Given Pakistan's strategic geopolitical position and security concerns, a PKI-based IPsec VPN might be more suitable. PKI offers stronger authentication and encryption, which is crucial for securing sensitive military and intelligence communications.

Government and Critical Infrastructure: PKI-based VPNs are well-suited for securing government communications and critical infrastructure, such as energy and transportation systems. They provide a robust mechanism for authentication, access control, and data protection.

Regulatory Compliance: Pakistan's regulatory landscape may require adherence to specific encryption and authentication standards. PKI-based VPNs, which align with international standards, can help ensure compliance with local regulations.

Cross-Border Communication: Pakistan engages in cross-border trade and diplomacy. PKI-based VPNs offer enhanced interoperability and secure communication with international partners and diplomatic missions.

Cybersecurity Capacity Building: PKI-based VPNs can promote cybersecurity capacity building within Pakistan. Developing expertise in managing a PKI infrastructure could contribute to the nation's cybersecurity workforce development.

Long-Term Viability: Pakistan's national needs likely include long-term viability and scalability. PKI-based VPNs offer flexibility for future expansion and technology advancements, making them suitable for accommodating evolving security challenges.

Counterterrorism and Law Enforcement: Effective communication between law enforcement agencies is essential for counterterrorism efforts. PKI-based VPNs can enhance secure communication channels among agencies involved in national security.

Academic and Research Collaboration: Pakistan's academic and research institutions collaborate globally. PKI-based VPNs can facilitate secure data exchange, collaborative research, and educational initiatives with international partners.

Public Services and Citizen Data Protection: For securing public services and citizen data, PKI-based VPNs provide a robust solution. This is especially important for e-government initiatives and protecting sensitive citizen information.

Threat Landscape and Adaptability: The evolving cyber threat landscape necessitates adaptable and resilient security solutions. PKI-based VPNs offer mechanisms for continuous monitoring, key rotation, and incident response, aligning with Pakistan's security needs.

Resource Allocation and Budgeting: Consideration of available resources, budget constraints, and expertise should factor into the decision. While PKI-based VPNs offer strong security, they may require higher initial investment and ongoing management compared to PSK-based VPNs.

Ease of Deployment: While PKI-based VPNs offer comprehensive security, PSK-based VPNs may be easier to deploy and manage, making them suitable for certain less-sensitive applications or scenarios.

1.5 Area of Application

Application of PKI based IPsec VPNs are as follows

Enterprise Connectivity

Remote Access

Vendor/Partner Access

Cloud Connectivity

IoT (Internet of Things) Security

Critical Infrastructure Protection

Healthcare

Financial Services

Government and Defense

E-commerce

Education

Manufacturing and Supply Chain

1.6 Advantages

Followings are the advantages of our research work: -

Security Levels and Key Management: Comparative analysis helps assess the security levels offered by each approach. PKI provides stronger security with asymmetric encryption and digital certificates, while PSK relies on a shared secret key. Analyzing key management mechanisms helps determine the robustness of each solution.

Scalability and Complexity: Comparative analysis evaluates the scalability and complexity of implementing each type of VPN. PKI-based VPNs can handle a larger number of users and devices without compromising security, making them suitable for large enterprises. PSK-based VPNs might be simpler to set up but can become less practical as the network grows.

Ease of Configuration and Maintenance: Analysis reveals differences in configuration and maintenance efforts. PSK-based VPNs might have simpler initial setup, while PKI-based VPNs often require more setup but can offer easier long-term management due to automated certificate renewal and revocation.

Risk Management and Flexibility: Comparative analysis helps in identifying potential risks and vulnerabilities associated with each approach. PKI-based VPNs offer greater

flexibility to revoke access in case of a security breach. PSK-based VPNs might pose risks if keys are compromised, as changing shared keys can be more cumbersome.

1.7 Thesis Organization

The research work has been organized and distributed in the following chapters: -

- **Chapter 1:** A brief introduction is given. Research objectives are listed. Relevance to National need is highlighted followed by area of application, its advantages and justification for selection of the topic is elaborated.
- **Chapter 2:** Describes related works carried out by various researchers. A comparison is drawn to observe existing work by various researchers.
- **Chapter 3:** Discuss the overall research methodology including, Overview of Proposed model followed by the application and implementation of proposed model.
- **Chapter 4:** This Chapters presents the results and objective achieved by our proposed model
- **Chapter 5:** This Chapter sums up the research with conclusion drawn and provides direction for future work
- **Chapter 6:** includes References



Figure 5: Taxonomy of thesis

Chapter 2

Literature Review

2.1 Introduction

In Chapter 1, an overall introduction was given about the topic. In this Chapter a detailed literature review of the topic has been carried out. The security and confidentiality of data transmission are now essential given how quickly modern communication networks are growing. Virtual Private Networks (VPNs), which provide a safe channel for transferring sensitive information between public and private networks, have emerged as a key technology in this attempt. IPsec (Internet Protocol Security) is one of the most well-known options for establishing secure communication channels among the different VPN protocols that are readily available. Pre-Shared Key (PSK) and Public Key Infrastructure (PKI) based implementations are two unique strategies that have become popular in the IPsec space. This examination of the literature compares and contrasts PSK and PKI-based IPsec VPNs in order to fully comprehend each one's advantages, disadvantages, and deployment issues.

2.2 Explanation of Literature Review

A literature review is an indispensable module of academic research, involving a critical examination of existing literature pertaining to a specific topic or research question. Its purpose is to comprehensively analyze, synthesize, and evaluate scholarly works to provide a bird eye view of the existing state of knowledge in the field. The primary purpose of conducting a literature review is to recognize significant

themes, trends, and findings from previous research that can inform the development of new research questions or hypotheses. It serves as a foundation for further investigation and helps researchers situate their work within the existing body of knowledge.

There are various approaches to conducting a literature review, including deductive, inductive, thematic, and theoretical approaches. A deductive approach involves testing existing theories or hypotheses, while an inductive approach aims to generate new theories or hypotheses based on the literature. A thematic approach involves identifying emerging themes or concepts, while a theoretical approach utilizes existing theories to frame the review. Conducting a literature review requires strong research skills and a critical mindset. Researchers must locate relevant sources, assess the quality of studies, synthesize the findings, and draw meaningful conclusions. It is important to ensure that the review is comprehensive, unbiased, and transparent. A well-executed literature review offers several benefits to academic research, such as identifying research questions, defining the research problem, selecting appropriate research methods, and highlighting the significance of the study. It also helps identify gaps in the existing literature, paving the way for new research questions or hypotheses.

2.3 Importance of Comparative Analysis

Conducting a comparative analysis of PKI (Public Key Infrastructure) and PSK (Pre-Shared Key) based IPsec VPN (Virtual Private Network) implementations is crucial for understanding their strengths, weaknesses, and suitability for different scenarios. Both PKI and PSK are authentication methods used in IPsec VPNs, and comparing them helps in making informed decisions when designing or choosing a VPN solution.

2.4 Introduction to VPNs

2.4.1 Definition. VPN is a temporary physical path created over a public network having a mesh architecture. Data transmission through a VPN can be referred to as virtual private networking (VPN). This basic definition of VPNs does not deliberate the layer of OSI model in which the VPN is operating. VPNs operate mostly at layer 2 and layer 3 of the OSI model. But there are VPNs that operate at layer at layer 4,5 to 7 as well.

2.4.2 Types of VPN. There are 2 basic types of VPNs. VPNs operating at layer 2 and 3 of the OSI model.

Layer 2 VPNs. The second tier (Data Link tier) of the OSI (Open Systems Interconnection) model is where Layer 2 VPNs, sometimes referred to as Data Link Layer VPNs, function. These VPNs extend the Layer 2 network over a shared or public network infrastructure to enable secure and private communication between two or more remote sites or networks. When connecting distant offices, branch sites, or data centers so that they seem to be part of the same local area network (LAN), Layer 2 VPNs are frequently utilized.

Layer 3 VPNs. Layer 3 VPNs operate at the network layer of the OSI model and they carryout routing and forwarding based on IP addresses. Because they operate on IP addressed therefore than can allow more complex network topologies as compared to layer 2 VPNs. L3 VPNs are suitable for a wide range of use cases, including site-to-site connectivity, remote access for individual users, secure access to cloud resources, and connecting diverse networks with different IP address spaces.

2.4.3 Categories of VPNs There are two basic categories of VPNs – remote access and site-to-site. A comparison between both has been given in the table below.

Table 2 Comparison of Remote Access and site to site VPNs

Aspects	Remote Access VPNs	Site-to-Site VPNs
Purpose	Allows individual users to securely access a corporate network from remote locations.	Connects entire networks or LANs at different physical locations, often branch offices, to a central corporate network.
User Type	Intended for remote employees, traveling users, or telecommuters.	Designed for connecting multiple remote offices, data centers, or branch locations.
Connectivity Method	Typically involves individual users installing VPN client software on their devices (e.g., laptops, smartphones).	Configured at the network level, with routers or firewalls establishing secure connections between entire networks.
Authentication	Users authenticate individually using credentials like usernames and passwords, two-factor authentication, or certificates.	Network devices authenticate using pre-shared keys, digital certificates, or other authentication methods.
Network Extension	Extends the corporate network to individual remote devices.	Extends the corporate network to other remote

		networks, creating a seamless LAN extension.
Traffic Flow	User-initiated; traffic flows from the user's device to the corporate network.	Network-initiated; traffic flows between remote office networks and the central network.
Scaling	Typically used for a relatively small number of remote users.	Suitable for connecting multiple remote locations, supporting a larger number of devices and users.
Encryption	Encrypts traffic between the user's device and the corporate network.	Encrypts traffic between remote office networks and the central network.
Use Cases	Ideal for remote work, secure access to corporate resources, and protection when using public Wi-Fi.	Used for interconnecting branch offices, data replication, and centralizing network management.
Network Complexity	Simpler in terms of network architecture and configuration.	Requires more complex network setup and management.

Common Protocols	Common protocols include SSL/TLS VPN, IPsec VPN, L2TP, and PPTP.	Common protocols include IPsec VPN, MPLS, and GRE (Generic Routing Encapsulation).
Centralized Management	Typically, less centralized management; focuses on individual user connections.	Centralized management is crucial for configuring and maintaining connections between remote sites.
Typical Hardware	May not require dedicated hardware for individual users; relies on VPN client software.	Requires VPN-capable routers, firewalls, or VPN concentrators at each site.
Security and Performance	Emphasizes security for individual user connections and may have variable performance based on the user's connection.	Prioritizes security between network locations and provides stable, predictable performance for site-to-site traffic.

2.4.3 Security Because VPN is created over a public network it is vulnerable to security related threats. The threats have a wide range. Due to these threats VPN is supposed to carryout encryption as well as authenticate the remote users. In addition to encryption and authentication VPNs also require mechanism to ensure integrity and a key management system for better scalability. The table below shows the pillars of

network security that are applicable to VPNs. Not all VPN protocols provide these services and even when supported organizations can choose as they require.

Functions	Duty
Accounting	Record activities to note potential threats or illegal attempted activities.
Authorization	Apply policy controls to network connectivity permissions
Encryption	Encode data to prevent unauthorized parties from viewing it
Integrity Check	Ensure data is not modified during transmission
Key Management	Select and distribute encryption keys

2.4.4 VPN Protocols There are different type of protocols that can be used to support the creation of VPNs.

Table 3 Protocols supporting VPN creation

Protocol	Layer	Authentication& Encryption	Use Case	Pros	Cons
PPTP	2	MS-CHAPv2, MPPE	Legacy remote access VPN, Windows-based	Widely supported - Easy setup - Low overhead	Weaker security (vulnerable to attacks) - Not recommended for sensitive data
L2TP/IPsec	2&3	L2TP: MS-CHAPv2, IPsec: Various	Legacy remote access and site-to-site VPN	Good compatibility - Stronger security (when used with IPsec)	Potential complexity - IPsec setup may be challenging
IPsec	3	Various (e.g., pre-shared keys, certificates) and Strong encryption (AES, DES, etc.)	Site-to-site VPN, remote access VPN, mobile device VPN	Strong security - Wide platform support - Flexible configuration	Complexity in setup and troubleshooting - Potential performance impact
SSL/TLS VPN	4	SSL/TLS (HTTPS)	Remote access VPN, web-based application	Ease of use (no client installation) - Strong encryption	Limited support for non-web applications - Can be slower for certain uses
IKEv2/IPsec	3	Various (e.g., EAP, certificates) and Strong encryption (AES, etc.)	Mobile device VPN, remote access VPN	-High security- Excellent for mobile devices	- May not be as widely supported as other protocols

				(seamless roaming)	
Wire Guard	3	Public key cryptography	Modern VPN, remote access, site-to-site	- Simplicity - High performance - Strong security	Limited adoption (emerging protocol) - May require manual configuration

2.5 Overview of IPsec

IPsec was developed by IETF (the Internet Engineering Task Force) for secure transfer of information at the OSI layer three across a public unprotected IP network, such as the Internet [7].

By authenticating and encrypting each IP packet in a data stream, the Internet Protocol Security (IPsec) protocol suite secures Internet Protocol (IP) connections. Protocols for initiating mutual authentication between agents and negotiating the cryptographic keys to be used throughout the session are also included in IPsec.

IPsec can be used to secure data transfers between hosts, security gateways (such as firewalls or routers), or between a security gateway and a host. Operating at the Internet Layer of the Internet Protocol Suite IPsec is a dual mode, end-to-end security protocol. Some other Internet security systems in widespread use, such as Secure Sockets Layer (SSL), Transport Layer Security (TLS) and Secure Shell (SSH), operate in the upper layers of these models. Hence, IPsec can be used for protecting any application traffic across the Internet. Applications need not be specifically designed to use IPsec. The use of TLS/SSL, on the other hand, must typically be incorporated into the design of applications [8]. Many different encryption methods and component technologies are used by IPsec [6]. However, the use of IPsec may be broken down into the following essential steps: The IPsec operational processes are explained below and shown in Figure 2.1.

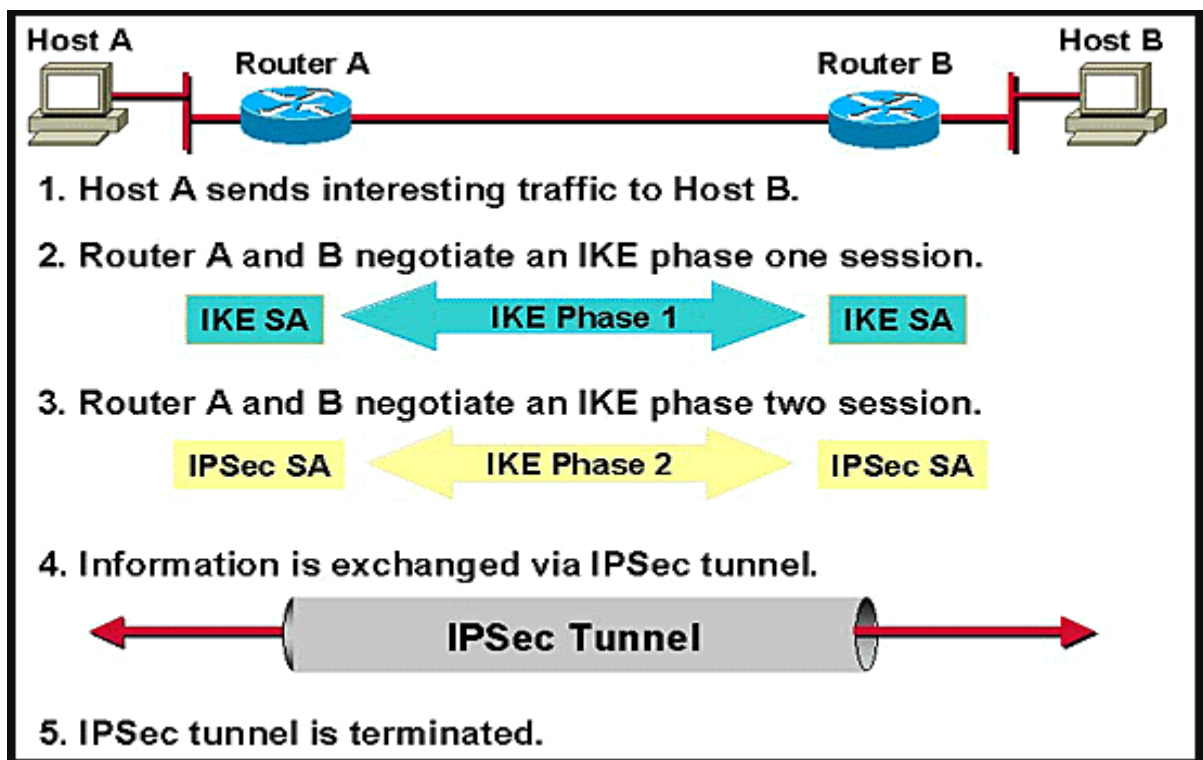


Figure 6: Working of IPsec

Security Association (SA) Establishment

Overview: The Security Association (SA) is a fundamental concept in IPsec. It defines the security parameters for communication between two network entities, such as hosts, routers, or gateways. Each SA is uniquely identified by its Security Parameters Index (SPI).

Negotiation: The SA establishment process begins with negotiation. Two devices that want to communicate securely must agree on various parameters, including encryption algorithms, authentication methods, and key lifetimes. This negotiation often occurs using protocols like Internet Key Exchange (IKE).

Key Exchange: Part of the SA establishment involves the exchange of encryption keys and other security-related information. This ensures that both parties have the necessary keys to encrypt and decrypt the data they exchange.

SA Database: SAs are stored in a database on each device. The database contains the details of each active SA, including SPI, encryption and authentication algorithms, and the shared keys.

Multiple SAs: A single device may have multiple SAs, each corresponding to different communication pairs and security requirements. SAs are uniquely identified by their SPIs.

Authentication

Overview: Authentication is a crucial aspect of IPsec to ensure that communicating parties are legitimate and not impostors. Authentication verifies the identity of devices or users involved in the communication.

Methods: IPsec supports various authentication methods, such as pre-shared keys, digital certificates, and Extensible Authentication Protocol (EAP). The choice of authentication method depends on the security requirements of the network.

Mutual Authentication: In most IPsec implementations, both communicating parties authenticate each other to establish mutual trust. This two-way authentication ensures that both parties are legitimate and authorized to communicate.

Key Management

Overview: Key management involves the generation, distribution, and management of cryptographic keys used for encryption and authentication. Proper key management is essential for maintaining the security of IPsec connections.

Key Exchange Protocols: Key management often relies on key exchange protocols like Internet Key Exchange (IKE) or manual keying. These protocols facilitate the secure exchange of keys between devices.

Key Lifetimes: IPsec keys have lifetimes, and they need to be refreshed or renewed periodically to maintain security. Key management protocols handle key rotation and rekeying processes.

Key Distribution: Keys must be distributed securely to all devices that need them. This can involve centralized key distribution servers or manual keying.

Data Encryption and Authentication

Overview: Once SAs are established, and keys are in place, data encryption and authentication can begin. This process ensures the confidentiality and integrity of data in transit.

Encryption: IPsec uses encryption algorithms, such as AES, DES, or 3DES, to encrypt data before it is transmitted. The choice of encryption algorithm is determined by the negotiated SA parameters.

Authentication: Authentication ensures data integrity and origin. Hash functions like HMAC (Hash-based Message Authentication Code) are used to create message digests that are attached to transmitted data. Receivers use these digests to verify the data's authenticity and integrity.

Packet Encapsulation: IPsec adds additional headers to the original IP packets, encapsulating them within secure IPsec packets. This encapsulation includes the SPI, source and destination addresses, and other security-related information.

Secure Data Transmission

Overview: With SAs established, authentication completed, and data encrypted, secure data transmission can occur. This process involves sending IP packets securely between the communicating parties.

Routing: Routers and gateways play a crucial role in forwarding secure IPsec packets between networks. They examine the packet's SA information to determine how to handle it.

Decryption and Authentication Verification: Upon receiving IPsec packets, the recipient device decrypts the data and verifies its authenticity using the SA parameters and shared keys.

Processing and Delivery: Once the data is decrypted and verified, it is processed and delivered to its intended destination. This secure process ensures that data remains confidential and unaltered during transit.

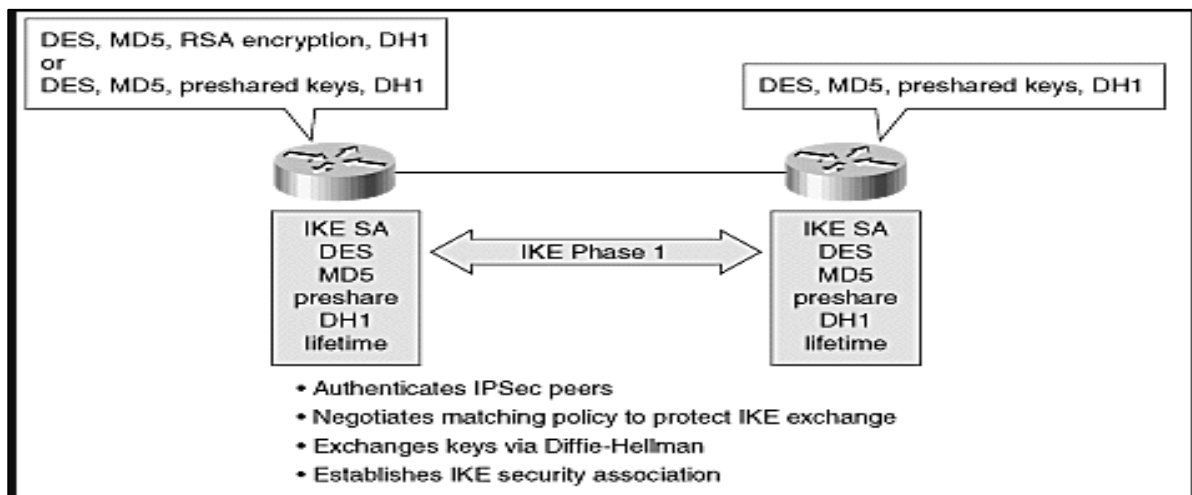


Figure 7: Phases of IKE

2.6 Previous Research's

In this research paper [9] the author has used the GPS information of the client to confirm the user for establishment of VPN connection. The global coordinates of the client will be stored in the form of Hash Values in the VPN authentication server to protect the geo privacy of the client. Also, when user will send his request, he will send the hash value of his geo location for the purpose of verification. In this way the establishment of VPN can be restricted to designated areas. The GPS locations will be retrieved from google Maps and to verify the accuracy of the readings gained from google Maps the author calculated the location of his laboratory for a period of one month from google Maps and compared it to the geo location of his laboratory calculated from some GPS device. The results showed 99.29 hit rate for latitude and 92.96 hit rate for longitude.

In this paper [10] the author concludes that the key negotiation process between the main mode and aggressive mode of IKEv1 protocol in IPsec VPN is vulnerable to DOS attacks. The proposed DOS attack method based on OSPF protocol adjacent route spoofing is effective in verifying the insecurity of IPsec VPN using IKEv1 protocol. The experiment shows that the attack method has the advantages of lower cost and easier operation compared with using botnet. The paper suggests that the vulnerability of the common routing protocol OSPF can be used to occupy the packet return path and realize the denial-of-service attack of the CPU resources of IPsec VPN server.

In this paper, [11] the authors has provided a secure enhanced structure of PKI named Cecoin which is distributively blockchain-based. The scheme processes the guarantee of consistency to prevent from false certificates. Besides, it provides practical services of multi-certificates and identity assignment. The scheme is achieved in prototype with

a desirable efficiency. However, there still exist improvement spaces in Cecoin. The storage cost of Cecoin is acceptable to the miners, while for other nodes, storing the decentralized Certificate Library will bring a lot of storage overhead. We will design a lightweight client with Simple Payment Verification (SPV) for users of Certificate owners to let them store the concerned nodes in modified Merkle Patricia tree. Besides, we will design a certificate browser for users of Certificate users to let them authenticate and search certificates quickly without having to join the network of Cecoin.

In this paper [12] the author analyzes and treats the vulnerability of key negotiation process in the main mode as well as aggressive mode of Internet Key Exchange (IKE) protocol in IP Security (IPsec) VPN. The author analyzes the vulnerability of the Open-Shortest Path First (OSPF) routing protocol in IPsec VPNs. First, a test environment was built using a GNS3 simulator, then a DoS attack was simulated in two modes, main mode and aggressive mode. These exploit the vulnerabilities in Internet Key Exchange (IKE) protocol through an OSPF network. The paper then provides a solution against DoS attacks. The solution exploits Suricata as a recent IDS/IPS to detect and protect the VPN server in the server side and contact the administrator to provide prevention in the network side. Experimental results show the robustness of the proposed approach in preventing the attack in the VPN communication.

The main challenge for distant corporate offices or educational institution branches, according to the author of this research [12], is keeping up with the always rising demand for services (voice, video, and data). Most multinational corporations choose to purchase dedicated leased lines from the service provider in order to meet these requirements, which is not only very expensive but also necessitates bandwidth planning in addition to Quality of Service (QoS) considerations. By establishing a

prototype Remote Access VPN network simulation on Cisco Packet Tracer, the author of this study has reported a solution. In terms of data integrity and authenticity, the solution shows promise. As VPN provides private communication over public infrastructure (Internet), many of these sites can be accessed remotely without experiencing any capacity issues. Additionally, it will lessen the jitter, dip, and delay.

The Ethereum blockchain technology is used in this study [13] to resolve security based on certificates, doing away with the requirement to trust a CA to distribute and manage certificates. Elimination of the PKI/CA, simplification of wallet management duties for end users, and implementation of a handshake protocol for PSK (Pre-shared Key) key distribution for PSK-based security protocols are the main contributions. One of the issues with adopting PKI for digital certificate-based client and server authentication was the sheer volume of certificates that needed to be disseminated and managed. By keeping client certificates on Blockchain platforms, the suggested method will do away with the necessity for CAs to hold them. The whole process is summarized in the following steps and clarified in figure 3.1.

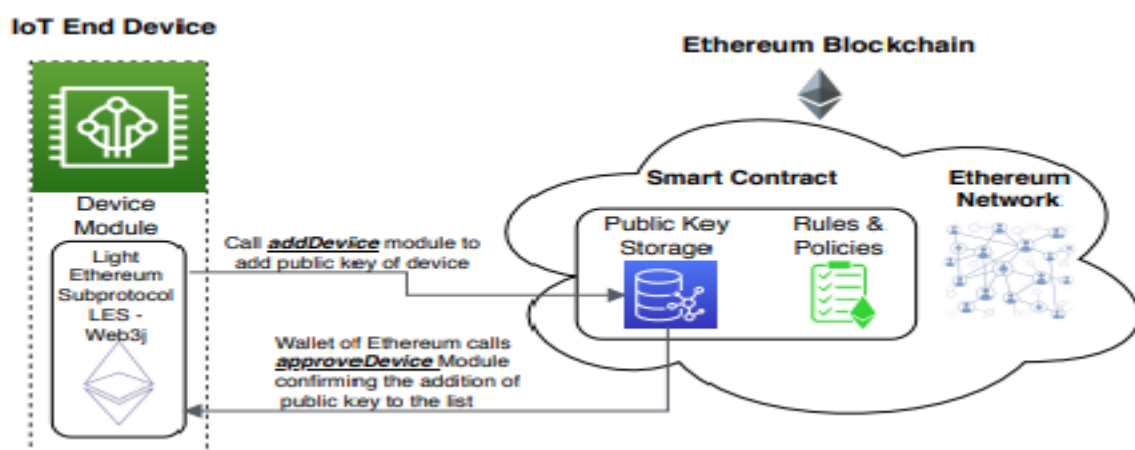


Figure 8 Device Ethereum- Blockchain communication

There are three primary parts to the architecture:

Digital Contract: on the Ethereum Blockchain network's apex. The policies, protocols, and regulations required to generate, store, and retrieve client (end device) public keys are contained in the high-level code. The subsequent steps serve as a summary of the entire procedure.

By signing a transaction, the IoT device invokes the smart contract's `addDevice` method. Any device can be added to the pending list using this function.

The wallet module that houses the token receives an approval request from the device module.

By utilizing the function `approveDevice`, the system manager can approve a device.

The specified device's public key can be obtained by calling the `getDevice` method on the device.

Device (IoT end device) Module: The essential component is to generate an Ethereum address for every external device so that it can access the Blockchain from the outside and communicate PSKs with other parties.

Wallet Module: The platform's network function, which is on the server side, authenticates the devices and approves requests for Blockchain storage. A public/private key pair and an Ethereum wallet will be included on each device. The Wallet module's main job is to authenticate the machine's device module and transfer the necessary ether to it so that it can store its public key on the Ethereum blockchain.

The elimination of the use of the certification authority (CA) for producing and confirming the digital certificates that contain the public key of the requested organization is one of the main contributions in the suggested solution. Pre-shared Key is utilized and deployed in place of conventional PKI to exchange PKs between

several parties seeking to interact. We implemented the module provided figure 3.2 below.

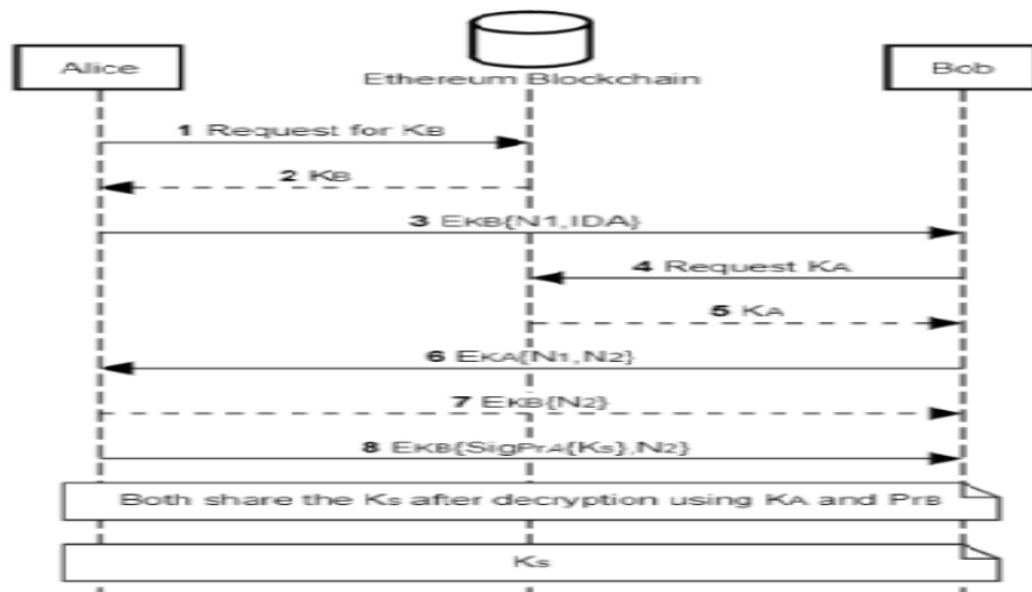


Figure 9: Gavin-Lowe Protocol for PSK Key Exchange

The authors of this study [14] have discussed two of the issues that need to be resolved in order to enable PKI for IoT: secure enrollment and certificate overhead reduction. It has been demonstrated that they are capable of carrying out their duties effectively, conducting initial enrollment and re-enrollment securely, and minimizing X.509 overhead for the intended IoT scenarios. These contributions are moving actual IoT deployments closer to having a fully operational PKI. In the IETF, where the enrolment protocol draft is almost ready to be accepted as an official RFC, enrollment and lightweight certificates are being pushed as standards for maximum impact and interoperability across different manufacturers. More thorough chain of trust scenarios for IoT devices in the automotive communication and health care sectors are being examined in an effort to further develop the PKI. New methods for certificate revocation and status checking have also been developed.

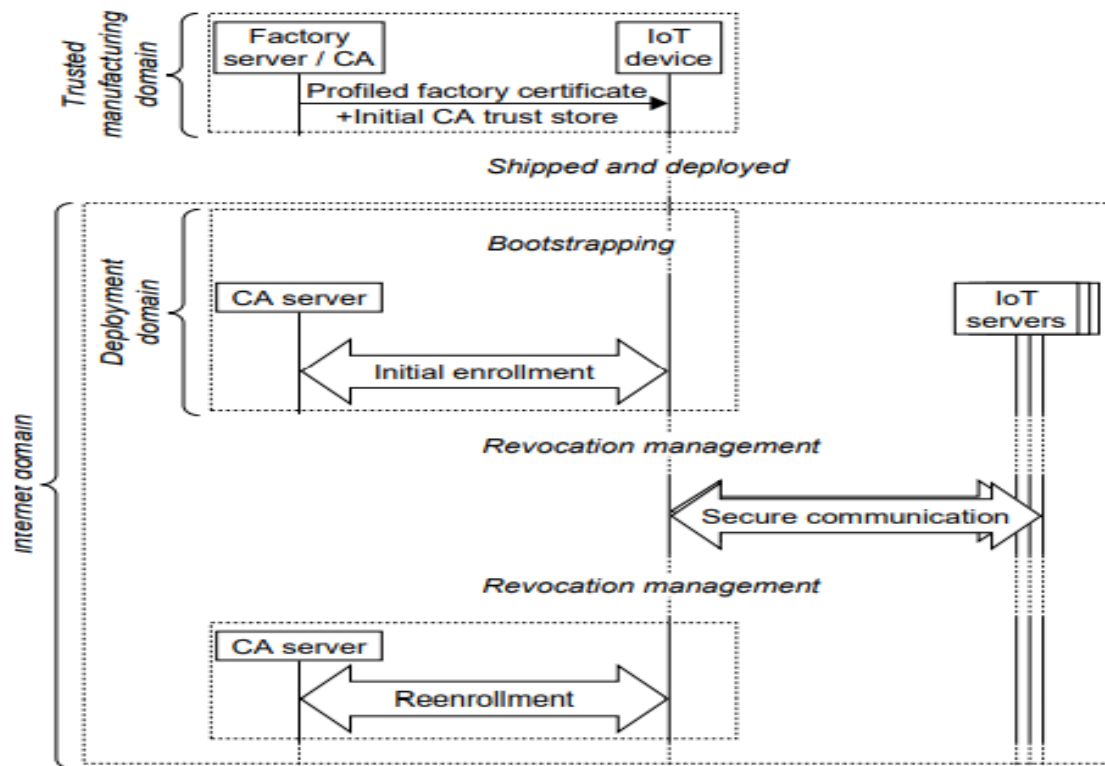


Figure 10: PKI4IoT from a communication perspective, showing the IoT device life cycle events in their respective domains: in factory environment, during deployment, and post-deployment, including communication, certificate re-enrollment and revocation

The authors of this article [15] have implemented PKI on a block chain. The distributed, fault-tolerant transaction log used by blockchain-based smart contract PKIs is used to store either all identity records or constant-sized data for off-chain identity record verification. However, because the majority of these technologies have never been put into use, there is little knowledge on how they will actually work. We implement, assess, and present a thorough security proof for the Ethereum-based smart contract-based PKI in this work. This design sacrifices computational complexity for constant-sized storage.

The authors developed a second architecture that eliminates the requirement for trusted setup, maintains its security features, and demonstrates that it is the only variant with constant-sized state that can be implemented on Ethereum's live chain in order to examine this trade-off. To highlight many flaws in Ethereum and its pricing scheme, they compared these structures with the straightforward strategy of storing all identity details on the state of the smart contract. It is suggested that the model be fine-tuned in a number of ways such that any smart contract platform, like Ethereum, can support any distributed application.

Due to its promised advantages for transportation efficiency and safety, C-ITS [16] is expected to be widely adopted. As C-ITS is being implemented in both the US and Europe, VPKI is advised to maintain its security and privacy. However, developing a secure VPKI is more difficult than designing any PKI since complicated corner circumstances make it necessary to address privacy. The background, evolution, fundamental ideas, general VPKI architecture, and the two preeminent VPKI standards approved in the US and Europe have all been covered in length in this work. The classification of VPKI proposals and suggestions that support the VPKI revocation procedure are the main topics of this article. Despite the existence of VPKI and revocation proposals, the article examines VPKI proposals in a systematic manner to investigate the research gap. The traditional CA model that VPKI used is no longer suitable for applications involving safety. Last but not least, VPKI schemes' performance and security flaws have been discussed. If they are fixed in the future, these issues could increase VPKI schemes' resilience to cyberattacks and help them satisfy the real-time performance needs of VC.

According to the PKI Survey of Pakistan [17], fewer companies and users have access to this technology. The main cause is the absence of a Certification Authority (CA) in

Pakistan that is commercially available. According to survey findings, the cost of PKI adoption is the primary deterrent for Pakistani organizations. In Pakistan, PKI is seen as crucial for cross-border trade because 53% of firms use it to communicate with overseas trading partners. Additionally, the majority of enterprises want to deploy PKI in the near future. Furthermore, as PKI programs do require some fundamental technological know-how to employ, a lack of technical expertise in this area has made it much more difficult for projects to be considered viable by the organizations. Banks and financial institutions make up the majority of PKI deployments in Pakistan's IT sector. While security implementation is not a top priority in other industries since they do not see it as being necessary. Last but not least, the most well-known possible uses of PKI in Pakistan, particularly for trade with foreign partners, are Cross Authentication-SSL and Secure Email. Additionally, rules pertaining to cyber security need to be revised frequently. However, countries like Pakistan do encounter many difficulties when putting these laws into practice all across the nation, particularly when it comes to e-Laws, e-Transactions, e-Crimes, digital signatures, digital certificates, and digital forensics, which are still in the very early stages of implementation. The acceptance of digital papers is not a standard in Pakistan, and the country's digital signature regulation is still not being enforced. However, things are getting better, and a few public and private sector institutions have started "paperless" efforts.

In order to give researchers and users the ability to evaluate the service offered to them by VPN providers, the authors [18] have created the VPNalyzer application with automated testing and capabilities. They have created a technology that makes it possible to do semi-automated, systematic research of VPN ecosystems. The program comprises 15 measurements that check for service features, privacy and security requirements, configuration errors, and leaks, as well as whether the VPN has

put in place a reliable system to safeguard users in the event of a tunnel failure. In addition to IPv6 leaks, kill switch leaks, DNS leaks during tunnel failure, and the absence of implementation of some security and privacy fundamentals, the authors have discovered a number of noteworthy problems and vulnerabilities. Researchers and consumers alike will gain from VPNalyzer, which also assists the general public in making more knowledgeable choices about which providers to choose for their individual requirements and, ultimately, promotes greater security and privacy policies in the VPN ecosystem.

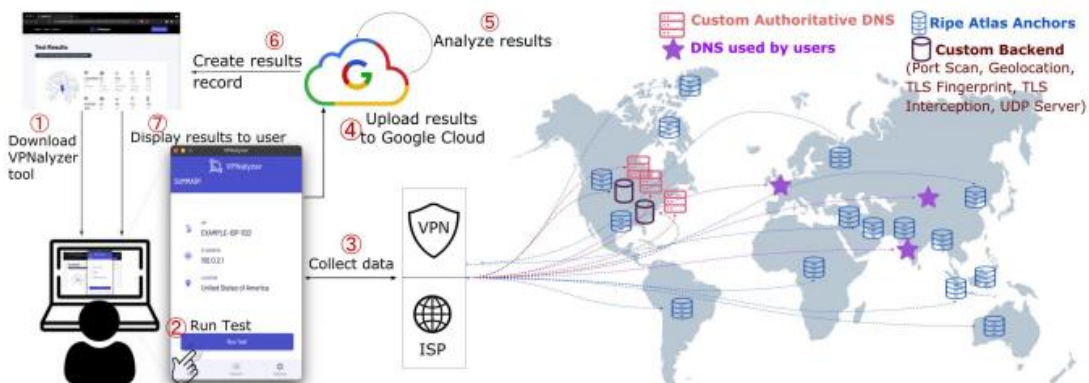


Figure 11: VPNalyzer Architecture— (1) User downloads application. (2) User installs the application, reviews our privacy policy, consents to be part of study. (3) User runs an “experiment” consisting of three stages: ensuring VPN is disabled and either granting or denying administrative privileges, enabling VPN and running VPN case, and disabling VPN and running ISP case (4) Once experiment is done, the application seeks explicit consent from user to upload experiment data to Google Cloud Storage. (5) Analysis pipeline works on the uploaded data. (6) Extracted results appear on website front-end. (7) User visits unique link pertaining to their “experiment” to view detailed results.

Ser	Name of Research Paper	Observations	Year of publication
1.	Enhancement of VPN authentication Using GPS	In this research paper the author has used the GPS information of the client in order to	2016

	Information with Geo-privacy Protection	carry out authentication of the user for establishment of VPN connection	
2.	DoS vulnerability verification of IPsec VPN	In this paper concludes that the key negotiation process between the main mode and aggressive mode of IKEv1 protocol in IPsec VPN is vulnerable to DOS attacks	2020
3.	VPN Remote Access OSPF-based VPN Security Vulnerabilities and Counter Measurements	In this paper the author analyzes and treats the vulnerability of key negotiation process in the main mode as well as aggressive mode of Internet Key Exchange (IKE) protocol in IP Security (IPsec) VPN.	2021
4.	Design of IPsec Virtual Private Network for Remote Access	The author presents a VPN design that allows many affiliated colleges to connect to the main university Head Office in order to ensure secure communication amongst entities.	2017
5.	Ethereum for Secure Authentication of IoT using Pre-Shared Keys (PSKs).	A new scheme has been developed to resolve security based on certificates by using Ethereum blockchain platform and eliminating the need to trust a CA for distributing and managing certificates.	2019

6.	PKI4IoT: Towards Public Key Infrastructure for the Internet of Things	the authors have presented challenges for enabling PKI for IoT, and new important PKI building blocks as answers to two of those challenges: secure enrollment and certificate overhead reduction	2019
7.	Implementing a Smart Contract PKI	Since the advent of Bitcoin, blockchains show promise for building systems that are completely distributed with no trusted parties. Blockchains solve the well-studied problem of distributed consensus in an open networking environment. They provide a distributed, fault-tolerant, auditable, append only ledger of transactions. As a result of this potential, there have been calls from the community to “recentralize” the Internet by leveraging blockchain technologies to build critical naming and PKI services and, thus, eliminate the Internet’s reliance on centralized entities.	2020
8.	Survey on Issues and Recent Advances in Vehicular Public-	This survey focuses on VPKI schemes designed to securely and privately manage and revoke public key certificates	2022

	Key Infrastructure (VPKI)		
9.	PKI Implementation Issues: A Comparative Study of Pakistan with some Asian Countries	paper includes technical issues hindering the implementation of PKI through comparison of PKI issues in Pakistan and some of Asian countries mainly Taiwan, Japan and Singapore.	2009
10.	VPNalyzer: Systematic Investigation of the VPN Ecosystem	The application benefits to have clear idea of which services are provided by which VPN providers and hence make well informed decisions in choosing the right provider as per their requirements.	2022

Chapter 3

Overview of Proposed Frame Work

3.1 Introduction

This chapter describes the overall architecture and functioning of our proposed model. When we conduct a comparison between PSK and PKI based IPsec VPNs we find out that PKI offers a lot of advantages over the Pre-Shared Keys (PSKs). Some of the advantages are given below: -

Enhanced Authentication

PSK Weakness: PSKs rely on a single, shared secret key for authentication, which can be vulnerable to unauthorized access if the key is compromised, or if an attacker can guess it [13].

PKI Solution: PKI employs asymmetric cryptography with public and private key pairs [14]. Each user or device is issued a unique private key and a corresponding public key. Authentication is based on the possession of the private key and the presentation of a digital certificate signed by a trusted Certificate Authority (CA). This approach significantly strengthens authentication, as each user's private key is secret and not shared. It is computationally infeasible to derive the private key from the public key [15], adding a strong layer of security.

Scalability:

PSK Weakness: As the number of users or devices in a network grows, managing and distributing PSKs becomes increasingly complex and error-prone.

PKI Solution: PKI is inherently more scalable [16]. The CA issues digital certificates to users and devices. Adding new users or devices merely involves the issuance and distribution of certificates, a process that can be automated and streamlined. There's no need to share secret keys individually, making PKI more suitable for larger deployments.

Key Management:

PSK Weakness: Changing a shared PSK for security reasons can be difficult and time-consuming, particularly in large networks where every device needs to be updated [17].

PKI Solution: In PKI, certificate revocation is a straightforward process. If a user or device's private key is compromised or if they need to be removed from the network, their certificate can be revoked by the CA. This prevents further access without having to update keys on all devices. Renewing certificates also facilitates the periodic rotation of keys for enhanced security.

Fine-Grained Access Control:

PSK Weakness: PSKs provide limited control over who can access the VPN. Once someone knows the PSK, they can potentially gain access.

PKI Solution: PKI allows for fine-grained access control through certificate policies. You can specify which users or devices are allowed access, what resources they can access, and under what conditions. This level of control enhances security by ensuring that only authorized entities can connect to the VPN.

Ease of Management:

PSK Weakness: Managing a large number of PSKs can become administratively burdensome, leading to potential errors and oversights [18].

PKI Solution: PKI streamlines management by centralizing certificate issuance and revocation through the CA [19]. It also enables automation of certificate distribution and renewal, reducing administrative overhead and the risk of configuration errors.

In conclusion, PKI successfully counters PSKs' drawbacks in IPsec VPNs' Internet Key Exchange. Through the use of distinct key pairs, it offers scalability and efficient key management, permits fine-grained access control, and streamlines administrative work. It also delivers stronger and more secure authentication. Because of these benefits, PKI is a preferred option for enterprises with higher security requirements and larger-scale deployments, improving the security and management of VPN connections.

Although PKI has a great advantage over the PSK but there are some difficulties and challenges in using PKI. Here are some of the common disadvantages associated with PKI.

Complexity: PKI implementations can be complex and require careful planning and management [20]. Setting up the necessary components, such as Certificate Authorities (CAs), Registration Authorities (RAs), and Certificate Revocation Lists (CRLs), can be challenging.

Cost: Establishing and maintaining a PKI can be expensive. Costs include acquiring and renewing digital certificates, hardware and software for CAs, personnel training, and ongoing maintenance [21].

Scalability Issues: While PKI is inherently scalable, managing a large number of certificates and users can become cumbersome [22]. It may require significant infrastructure upgrades and resource allocation [23].

Certificate Revocation: Revoking certificates can be a complex and time-consuming process. Ensuring that revoked certificates are promptly and effectively removed from use is essential for security [24].

Single Point of Failure: The CA is a critical component in PKI. If the CA is compromised or fails, it can lead to a significant security breach or a disruption in certificate issuance and management [25].

Key Management: Managing private keys securely is crucial in PKI [26]. If a private key is lost or compromised, it can result in unauthorized access. Proper key management practices are essential.

Interoperability: Ensuring that different PKI systems and certificate formats are compatible can be challenging, especially when organizations need to work together and exchange encrypted data [27].

Trust and Certificate Authorities: Trust in the CA system is fundamental to PKI [28]. If a CA's trustworthiness is compromised or if a CA makes errors in issuing certificates, it can undermine the entire PKI ecosystem. We can take the example of DigiNotar [29] which was a certificate authority—a well-established and reputable one. It was one of the root CAs for all of the major web browsers and issued many of the digital certificates used by the Dutch government for its online services. But DigiNotar also

made some serious mistakes during the summer of 2011. For one, it was running some unpatched software on its web servers, which allowed an intruder to begin burrowing into its maze of partitioned networks in June 2011. On July 10, the intruder successfully issued his first rogue certificate. It's still unclear how exactly the intruder managed to bypass all the physical security in place to protect the inner sanctum where certificates were generated, but the investigators' best guess was that the keycards for a few computers were left permanently in place.

User Experience: Some users may find the need to manage digital certificates cumbersome. For example, if a user loses their private key or forgets their passphrase, it can result in access issues.

Regulatory and Compliance Challenges: Compliance with data protection regulations (e.g., GDPR) and industry standards (e.g., PCI DSS) can be challenging when handling sensitive data and certificates [30].

Resource Intensive: PKI can be resource-intensive, both in terms of hardware and personnel. Organizations need to allocate resources for ongoing maintenance, monitoring, and responding to security incidents [31].

Security Risks: While PKI is designed to enhance security, if not properly implemented and managed, it can introduce security risks. For example, if a CA's private key is compromised, it can undermine the entire PKI system's security.

Lack of Education and Awareness: Many users and organizations may not fully understand PKI and how it works, which can lead to misconfigurations or misunderstandings about security measures.

The above-mentioned advantages and disadvantages clearly show that PKI has an upper edge over pre-shared keys. For organization where security is of paramount

importance the risks associated with using pre-shared key-based IPsec VPNs cannot be tolerated and the use of PKI based IPsec VPNs is the preferred option.

In the context of PKI-based IPsec VPNs (Virtual Private Networks), latency issues in the Certification Authority (CA) infrastructure can have significant implications for the performance and reliability of the VPN connections. The details of how latency issues can affect PKI-based IPsec VPNs are as under: -

Using regional Online Certificate Status Protocol (OCSP) and Certificate Revocation List (CRL) servers can effectively address latency problems in certificate validation processes. Here's how it can address latency problems.

Proximity to Clients: Regional servers are strategically placed geographically, closer to the clients or users who need to verify certificates. This reduces the round-trip time for certificate validation requests, significantly decreasing latency.

Reduced Network Congestion: By distributing OCSP and CRL servers regionally, the overall network traffic is distributed more evenly. This alleviates congestion on a single server or a centralized system, leading to faster response times.

Improved Scalability: Regional servers can be scaled independently based on the specific demands of their respective regions. This scalability ensures that each server can handle its share of certificate validation requests efficiently, even during traffic spikes.

Load Balancing: Load balancing techniques can be employed at the regional level to evenly distribute incoming certificate validation requests among multiple servers. This ensures that no single server is overwhelmed with requests, further reducing latency.

Fault Tolerance and Redundancy: Regional servers can be designed with redundancy and failover mechanisms. If one server becomes unavailable due to a failure or maintenance, clients can seamlessly switch to another nearby server, minimizing downtime and latency.

Localized Caching: Regional servers can cache frequently requested certificates and their status responses. This caching mechanism allows for faster responses for commonly accessed certificates, reducing the need for constant requests to the CA or centralized OCSP/CRL server.

Dynamic Routing: Implementing intelligent routing mechanisms can direct clients to the nearest regional server based on their IP address or geographical location. This ensures that clients automatically connect to the server with the lowest latency.

Content Delivery Networks (CDNs): Leveraging CDNs for distributing OCSP and CRL responses can further reduce latency. CDNs have a vast network of servers worldwide, enabling efficient content delivery, including certificate status information.

Quality of Service (QoS) Management: Regional servers can prioritize certificate validation requests based on factors such as the importance of the transaction or user, ensuring that critical certificate validations receive preferential treatment in terms of response time.

Monitoring and Optimization: Regular monitoring and analysis of regional servers' performance can identify bottlenecks and areas for optimization. Adjustments can be made to server configurations or regional placements to continually improve response times.

In summary, regional OCSP and CRL servers offer a practical solution to address latency problems in certificate validation. By strategically distributing servers,

optimizing their performance, and implementing failover and caching mechanisms, organizations can significantly reduce the time it takes to validate digital certificates, thereby enhancing the overall security and user experience.

Certificate Validation Latency

When two devices establish an IPsec VPN connection, they need to validate each other's digital certificates. This involves retrieving the certificates and validating their authenticity against the CA's digital signature. Latency in this process can lead to delays in the initiation of the VPN tunnel, affecting the overall connection setup time.

CRL and OCSP Latency

IPsec VPNs often require checking the validity of certificates through methods like Certificate Revocation Lists (CRLs) or Online Certificate Status Protocol (OCSP) queries. If the CA's CRL or OCSP server experiences latency, the VPN devices might experience delays in checking certificate revocation status, potentially leading to unnecessary retransmissions or even connection failures.

Certificate Distribution Latency

During VPN tunnel establishment, the devices exchange certificates for mutual authentication. If the CA's certificate distribution process is slow, it can lead to delays in retrieving the required certificates, again affecting connection setup time.

Handshake Latency

The IPsec VPN handshake involves a series of cryptographic operations, including key exchange and negotiation. The delay in any of these operations, including certificate verification, can extend the time required for the VPN tunnel to become operational.

Load Balancing Challenges

Many IPsec VPN deployments use load balancers to distribute VPN traffic across multiple VPN gateways. If the load balancers experience latency or if the CA infrastructure is not well-integrated with the load balancing setup, it can cause imbalances and delays in routing traffic to appropriate gateways.

Geographical Distribution Impact

In globally distributed IPsec VPN deployments, where VPN gateways are spread across various geographic locations, latency in accessing CA services (e.g., OCSP servers or CRL distribution points) can be exacerbated due to the geographical distances involved.

Certificate Renewal Latency:

Certificates used for IPsec VPNs have expiration dates, requiring periodic renewal. If there is latency in the certificate renewal process, VPN devices might continue using expired certificates, potentially leading to connection failures or security vulnerabilities.

Impact on Failover and Redundancy:

IPsec VPN deployments often have failover and redundancy mechanisms to ensure uninterrupted service. Latency issues affecting the synchronization of certificate and revocation status updates across redundant components can impact the effectiveness of these mechanisms.

User Experience and Productivity:

High latency in establishing or maintaining IPsec VPN connections can lead to slow data transfer rates, poor voice or video quality for real-time applications, and reduced

user productivity. It can also increase the likelihood of user frustration and support requests.

Security Implications:

Delays in certificate validation or revocation checking can potentially expose the VPN infrastructure to security risks. If a compromised or revoked certificate is not promptly detected due to latency, it could lead to unauthorized access or data breaches.

Addressing these latency issues in PKI-based IPsec VPNs involves careful planning, optimization of CA infrastructure, network design, and continuous monitoring. Performance tuning, geographical distribution of CA services, efficient OCSP implementation, and proper load balancing are some strategies that can help mitigate the impact of latency on IPsec VPNs' overall performance and security.

3.2 Overview of Proposed Model

In this study, we have proposed a decentralized deployment architecture of the CA in order to reduce the issue of latency in establishment of PKI based IPsec VPNs. As we know that these certificates, issued by Certification Authorities (CAs), ensure the authenticity and integrity of data exchanged over networks. But the traditional architecture of a centralized CA can sometimes lead to latency issues, especially when dealing with Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP) services. To address this challenge, a decentralized architecture is proposed, where CRL and OCSP services are located away from the CA, thereby reducing latency and enhancing the overall efficiency of certificate validation processes.

In the traditional centralized CA architecture, both the issuance of digital certificates and the management of certificate revocation are handled by a single entity. While this

approach simplifies management, it can result in latency issues, particularly during the validation process. When a relying party (RP) or client attempts to verify the validity of a certificate, it needs to interact with the CA's OCSP responder or check the CRL, which can introduce delays due to network latency and server load.

To mitigate the latency concerns associated with centralized CA architectures, a decentralized approach is suggested. In this model, the CA's core functions, such as certificate issuance and management, remain centralized, while the CRL and OCSP services are distributed across multiple geographically dispersed locations. This separation allows for more efficient certificate validation and reduces the impact of network latency on the overall system performance

Implementation Of Proposed Model

Implementing a regional OCSP and CRL server model with offline CA in a closed environment, such as an enterprise network or a private network within an organization or over the Internet requires careful planning and execution. Here are the steps to implement this model:

Infrastructure Design and Deployment:

Server Placement: Determine the geographical regions or segments within your closed environment where regional OCSP and CRL servers will be deployed. Consider factors like network topology, user distribution, network load and latency requirements.

Server Hardware: Procure or allocate the necessary hardware resources for each regional server, including compute, storage, and network resources. Ensure redundancy and scalability options are built into the design. Without allocation of enough resources, it is difficult to meet the criteria required for building of machines.

Network Configuration: Configure the network infrastructure to route certificate validation requests from clients to the nearest regional server. Here different strategies or protocols like DNS entries based on geography or group policies over AD to allocate OCSP and CRL servers on the basis of user group may be adopted. At times, /etc/hosts/ entries may be made if no other manual options are available in server / network devices. You may need to set up subnets, VLANs, or other network segmentation techniques to achieve this.

Server Setup and Configuration:

Install OCSP and CRL Software: Choose OCSP and CRL software solutions that are compatible with your closed environment of org. Popular choices include OpenSSL or other servers for OCSP and tools like Apache HTTP Server for CRL distribution.

Configuration Parameters: Configure each regional server with parameters like certificate revocation lists, OCSP signing certificates, cache settings, and routing rules based on regional criteria. Certificate revocation list periodically or on requirement basis issued by CA will be automatically distributed to OCSP and CRL Servers using crontab jobs from CA or any other feature of the sort in case of Microsoft CA.

Load Balancing: If needed, implement load balancing mechanisms to distribute incoming certificate validation requests among multiple servers within the same region. Ensure that the load balancer can handle failover and automatic routing. Different load balancing may be used including active-active and active-passive topologies. Hardware or software load balancers may be used as per the design and type of resources available with the organization.

Security Measures:

Access Control: Restrict access to the regional servers to authorized entities only. Implement firewalls, access control lists (ACLs), or other security measures to ensure the servers are not vulnerable to unauthorized access. Network security policies and hardening of servers using available methodologies and Secure Operational Centers (SOC) may also help regarding malicious attempts to compromise the OCSP and CRL Servers.

Encryption: Secure communication between clients and regional servers using encryption protocols like HTTPS or TLS to protect the confidentiality and integrity of certificate validation requests and responses. 802.1x authentication or any other certificate-based authentication between servers will be preferred option.

Authentication: Employ strong authentication mechanisms for clients connecting to the regional servers to ensure that only legitimate users and devices can access certificate validation services. Multi factor authentication for servers, devices and users will ensure CIA Triade. All this can be achieved using Access Control Lists and pre sharing of authorized hosts identities with CRL and OCSP Servers.

Monitoring and Management:

Logging and Monitoring: Set up logging and monitoring systems to track the performance and availability of regional OCSP and CRL servers. Monitor network traffic, server health, and the effectiveness of load balancing. All these can be achieved using simple network monitoring protocol for which different software like IBM Tivoli, NAGIOS etc are available.

Alerting: Configure alerts that notify administrators of any anomalies or issues, such as server downtime or performance degradation. Alerting can be achieved by

configuring different alerts over software used in NOC configuration to enable admin for viewing different type of logs about health status of servers.

Patch Management: Establish a process for keeping the regional servers up-to-date with security patches and updates. Anomalies and vulnerabilities keep up popping with the passage of time. In order to address them, patch management is of paramount importance to system health, performance and security.

Testing and Validation:

Testing Scenarios: Conduct thorough testing of the regional OCSP and CRL server infrastructure under various scenarios, including normal operations, failover, and scalability testing. Before putting in production, detailed testing and validations are absolutely necessary.

Performance Benchmarking: Measure the latency reduction achieved by the regional model compared to a centralized approach. Adjust configurations as needed to optimize performance. Baseline configurations will be used to configure OCSP and **CRL Servers**. In case of any deduction or before putting them in production, performance bench marking criteria will be met.

Documentation and Training:

Documentation: Create detailed documentation for server configurations, network settings, security policies, and maintenance procedures. This documentation will be invaluable for ongoing management. Human resources may be temporary, but for an organization to function properly, documentation of each and every step is required.

Training: Train IT staff responsible for managing and maintaining the regional servers on the implementation details and best practices. Training enables staff to keep care of the resources as per desired standards.

Deployment and Ongoing Maintenance:

Gradual Rollout: Implement the regional model gradually, starting with one or a few regions, and expand as needed based on feedback and performance metrics.

Regular Maintenance: Schedule regular maintenance and updates for the regional servers to ensure their continued reliability and security.

By following these steps, you can successfully implement a regional OCSP and CRL server model in a closed environment, reducing latency in certificate validation processes while maintaining security and reliability.

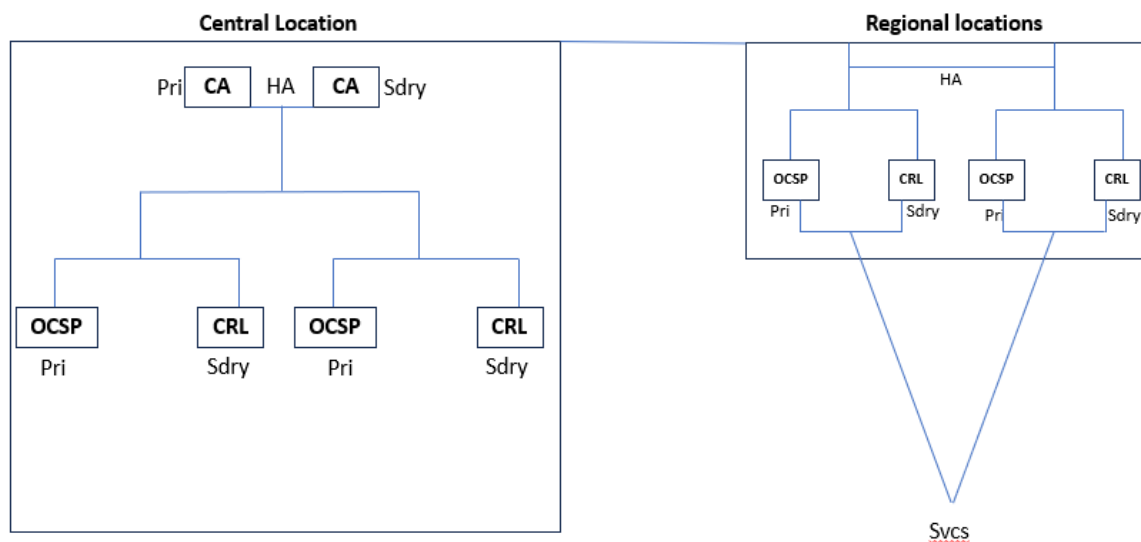


Figure 12: Architectural Diagram of Proposed Framework

Chapter 4

Results And Analysis

As discussed in the implementation of proposed model, we gradually started shifting VPNs of our organization from PSK to PKI based IPsec VPN and I noticed that there was no significant difference between both in terms of performance, but security of VPN increased manifolds. In this comparative study, we investigated the performance of PSK based VPN and PKI based VPN in terms of performance, which remained consistent and observed no significant difference. Surprisingly, we found that the performance metrics for both models remained nearly identical, with negligible variations. This result was consistent across multiple devices providing varying range of services and connectivity, indicating that there was no significant performance difference between the two configurations. While this outcome was unexpected, it suggests that factors such as PKI based certificate authentication had minimal impact on the performance. It implies that performance for the end users remained constant, but security of devices is multiplied manifolds owing to number of factors involved in the process of certificate creation, issuance, distribution and validation. The table below shows a qualitative analysis of PSK and PKI based IPsec VPNs.

Aspects	PKI Based IPsec VPN	PSK Based IPsec VPN
Security	High	Medium
Authenticated	Public/Private Keys	Pre-shared Keys
Key Management	Complex	Relatively Simple
Scalability	More Complex	Easier to configure
Usability	Longer	Shorter

Initial Setup time	Typically, Slightly Slower	Generally sufficient
Performance (throughput)	Generally Lower	General Higher
Compatibility with many Devices	Yes	Yes
Suitable for large networks	Yes	Yes
Recommend Use Cases	Large Enterprises, Government Agencies, Critical Systems	Small to Medium Businesses, Remote Access

Explanation of above qualitative factors have been given below: -

Security

PKI-Based IPsec VPN: Offers a high level of security due to the use of digital certificates and asymmetric encryption.

PSK-Based IPsec VPN: Provides medium-level security, which can be strong if the pre-shared keys are robust, but it may be weaker if weak keys are used or compromised.

Authentication Method

PKI-Based IPsec VPN: Utilizes public and private keys for authentication, which is considered highly secure.

PSK-Based IPsec VPN: Uses pre-shared keys (shared secrets) for authentication.

Key Management:

PKI-Based IPsec VPN: Involves complex key management processes, including certificate issuance, revocation, and management of key pairs.

PSK-Based IPsec VPN: Has relatively simple key management as it only requires the distribution and updating of shared secrets.

Scalability:

PKI-Based IPsec VPN: Is scalable and suitable for large-scale deployments due to its centralized certificate authority infrastructure.

PSK-Based IPsec VPN: Has limited scalability and may be better suited for smaller network environments.

Usability:

PKI-Based IPsec VPN: Is generally more complex to set up and manage, particularly due to the complexities of certificate management.

PSK-Based IPsec VPN: Tends to be easier to configure and manage since it primarily involves shared secrets.

Initial Setup Time:

PKI-Based IPsec VPN: Typically takes longer to set up due to the complexities associated with certificate issuance and distribution.

PSK-Based IPsec VPN: Generally, has a shorter setup time since it primarily involves configuring pre-shared keys.

Performance (Throughput):

PKI-Based IPsec VPN: May have slightly slower throughput due to the computational overhead of asymmetric encryption.

PSK-Based IPsec VPN: Generally, provides sufficient throughput for most applications.

Performance (Latency):

PKI-Based IPsec VPN: Generally, has lower latency as asymmetric encryption is computationally efficient.

PSK-Based IPsec VPN: May have higher latency due to the use of symmetric encryption and shared keys.

Compatibility with Many Devices:

Both PKI and PSK-Based IPsec VPNs are compatible with a wide range of devices and platforms.

Suitable for Large Networks:

PKI-Based IPsec VPN: Suitable for large networks and enterprises with centralized certificate management.

PSK-Based IPsec VPN: Typically, more suitable for small to medium-sized networks due to limited scalability.

Recommended Use Cases:

PKI-Based IPsec VPN: Recommended for large enterprises, government agencies, and critical systems where strong security is essential.

PSK-Based IPsec VPN: Recommended for small to medium-sized businesses and remote access scenarios where simplicity and ease of configuration are valued.

In addition to the above qualitative analysis, I have also carried out a quantitative analysis of both authentication methods and used the PRTG software to monitor the results of both PSK and PKI based IPsec VPNs. In order to facilitate better understanding I have given scales of 1-10 to show the level achieved by the relative authentication method.

Metric	PSK (1-10)	PKI (1-10)
Security	6	9
Ease of Setup	9	6
Key Management	5	9
Scalability	5	9
Authentication	7	9
Certificate Management (PKI)	-	10
Revocation Management (PKI)	-	9
Complexity	3	7
Interoperability	8	9
Performance	8	7
Deployment Flexibility	8	6
Risk of Key Exposure	8	3
Cost	6	9

By taking into account this comparative analysis I came to the conclusion that PKI based IPsec VPNs are much better suited for bigger organization to meet their performance requirements as well as addressing their security concerns.

Chapter 5

Conclusion And Future Work

Owing to near-identical performance metrics across a range of devices, it is suggested that their ability to achieve our specified performance goals for end users is comparable. However, it is crucial to underline that security considerations have unveiled a clear distinction between the two in favour of latter. PKI based VPNs exhibit a significantly higher level of security robustness by providing enhanced protection against vulnerabilities, attacks, and unauthorized access.

Future Work:

While our study has shed light on the security advantages of PKI Based VPNs over PSK Based VPNs, several avenues for future research and exploration emerge:

Detailed Security Analysis: Conduct a more comprehensive and in-depth security analysis of both models to identify specific vulnerabilities and threats that could affect their real-world deployment.

Integration of Security Metrics: Develop and incorporate security-specific metrics into our performance evaluation framework to provide a more holistic assessment of models.

Dynamic Security Adaptation: Investigate approaches that allow models to dynamically adapt their security measures based on evolving threats and attack patterns.

User and Stakeholders Feedback: Gather feedback from end-users and stakeholders to understand the practical implications of security measures and their impact on usability and operational efficiency.

Incident Response Planning: Develop incident response plans and strategies for both models to ensure rapid and effective responses to security incidents.

In conclusion, our research has emphasized that performance alone cannot be the sole criterion for selecting a model or system. Security considerations must be at the forefront of decision-making processes. As technology continues to advance and new threats emerge, it is imperative to continuously evaluate, adapt, and enhance the security measures within our models to protect sensitive data and ensure the trust of our users and stakeholders

Chapter 6

References

- [1] W. Stallings, *Cryptography and Network Security Principles and practise*, Malaysia: Pearson Education Limited, 2017.
- [2] [Online]. Available: <https://cybernews.com/what-is-vpn/vpn-protocols/>.
- [3] G. Blokydyk, *IPsec VPN A Complete Guide - 2019 Edition*.
- [4] Q. D. F. Elaine Barker, "Guide to IPsec VPNs," June 2020.
- [5] "venafi," [Online]. Available: <https://venafi.com/machine-identity-basics/what-is-pki-and-how-does-it-work/#item-0>.
- [6] T. K. S. K. F. M. M. Nasir Mahmood Malik, "PKI Implementation Issues: A Comparative Study of Pakistan with some Asian Countries," *International Journal on Computer Science and Engineering Vol.1(2), 2009, 105-110*, vol. 1, p. 6, 2009.
- [7] "Wikipedia," [Online]. Available: <https://en.wikipedia.org/wiki/IPsec#History>.
- [8] M. D. D. S. B. P. R. Mr. Hitesh dhall, "IMPLEMENTATION OF IPSEC PROTOCOL," *2012 Second International Conference on Advanced Computing & Communication Technologies*, p. 6, 2012.
- [9] M. T. S. M. Yong Jin, "Enhancement of VPN authentication Using GPS Information with Geo-privacy Protection," p. 6, 2016.
- [10] K. Z. Yimin Zhou, "DoS vulnerability verification of IPsec VPN," 2020.
- [11] J. H. Q. W. X. L. B. L. W. S. Bo Qin, "Cecoin: A decentralized PKI mitigating MitM attacks," *Future Generation Computer Systems*, p. 36, 2017.
- [12] M. M. S. A. a. A. A. Hanan Sawalmeh, "VPN Remote Access OSPF-based VPN Security Vulnerabilities and Counter Measurements," in *2021 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, 2021.
- [13] [Online]. Available: <https://help.stonesoft.com/onlinehelp/StoneGate/SMC/6.5.0/GUID-2A1BC042-3AFE-4794-B738-BEAA94922B58.html>.
- [14] [Online]. Available: <https://doubleoctopus.com/security-wiki/digital-certificates/public-key-infrastructure/>.
- [15] [Online]. Available: <https://www.informit.com/articles/article.aspx?p=170808&seqNum=3>.
- [16] "Oracle (2002) The Public Key Infrastructure Approach to Security.," [Online]. Available: https://docs.oracle.com/cd/B10501_01/network.920/a96582/pki.htm.

- [17] [Online]. Available: https://en.wikipedia.org/wiki/Pre-shared_key.
- [18] [Online]. Available: <https://weberblog.net/considerations-about-ipsec-pre-shared-keys-psks/>.
- [19] [Online]. Available: <https://www.ssl.com/faqs/what-is-a-certificate-authority/>.
- [20] [Online]. Available: <https://ts2.space/en/the-challenges-of-public-key-infrastructure-implementation-and-management/>.
- [21] [Online]. Available: <https://www.securew2.com/blog/3-hidden-costs-of-an-inhouse-ca>.
- [22] [Online]. Available: <https://cpl.thalesgroup.com/faq/public-key-infrastructure-pki/what-insufficient-scalability-pki>.
- [23] [Online]. Available: <https://www.infosecurity-magazine.com/blogs/scaling-pki-lessons-enterprise/>.
- [24] [Online]. Available: <https://www.encryptionconsulting.com/what-is-certificate-revocation/>.
- [25] M. K. R. Rebecca Herold, *Encyclopedia of Information Assurance*, Harry B. DeMaio, 2010.
- [26] [Online]. Available: <https://cpl.thalesgroup.com/data-protection/pki-security-solutions>.
- [27] [Online]. Available: <https://pkic.org/pkimm/categories/interoperability/>.
- [28] [Online]. Available: <https://www.digicert.com/faq/trust-and-pki/why-is-pki-important-and-how-does-it-increase-trust>.
- [29] [Online]. Available: <https://slate.com/technology/2016/12/how-the-2011-hack-of-diginotar-changed-the-internets-infrastructure.html>.
- [30] [Online]. Available: <https://ts2.space/en/public-key-infrastructure-and-gdpr-ensuring-compliance-and-data-protection/>.
- [31] [Online]. Available: <https://www.axiad.com/blog/pki-based-authentication/>.
- [32] B. I. a. D. B. A. Dnyanesh Deshmukh, "Design of IPSec Virtual Private Network For Remote Access," in *International Conference on Computing, Communication and Automation (ICCCA2017)*, 2017.
- [33] A. F. C. S. Mohammad El-Hajj, "Ethereum for Secure Authentication of IoT using Pre-Shared Keys (PSKs)," in *WINCOM 2019 1570583880*, 2019.
- [34] A. F. C. a. A. S. Mohammad El-Hajj, "Ethereum for Secure Authentication of IoT using Pre-Shared Keys," in *WINCOM 2019 1570583880*, 2019.
- [35] S. L. M. F. R. Joel Hoglunda, "PKI4IoT: Towards Public Key Infrastructure for the Internet of Things," 2019.
- [36] K. S. A. K. a. M. R. Christos Patsonakis, "Implementing a Smart Contract PKI," 2020.

- [37] F. L. ,. Z. Z. ,. M. A. R. ,. M. A. ,. a. K. W. Salabat Khan, "Survey on Issues and Recent Advances in Vehicular Public-Key Infrastructure (VPKI)," 2022.
- [38] "<https://www.linkedin.com/pulse/exploring-world-cryptography-securing-information-digital-seddon/>," [Online].
- [39] T. K. S. K. F. M. M. Nasir Mahmood Malik, "PKI Implementation Issues: A Comparative Study of Pakistan with some Asian Countries," *International Journal on Computer Science and Engineering Vol.1(2), 2009, 105-110* , p. 6, 2009.
- [40] L. E. X. E. Reethika Ramesh, "VPNalyzer: Systematic Investigation of the VPN Ecosystem," *Network and Distributed Systems Security (NDSS)*, 2022.
- [41] [Online]. Available: <https://www.ciscopress.com/articles/article.asp?p=24833&seqNum=6>.
- [42] T. K. S. K. F. M. M. Nasir Mahmood Malik, "PKI Implementation Issues: A Comparative Study of Pakistan with some Asian Countries," *International Journal on Computer Science and Engineering Vol.1(2), 2009, 105-110*, vol. 1, p. 6, 2009.