ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug878

Design and Implementation of a Secure IPSec-GRE Virtual Private Network Framework for Remote Banking Communications

Ewunonu T. C.[1]; Etus C.[2]; Chuks-Ugochukwu C. M.[3]; Esomonu N. F.[4]; Benson-Emenike M. E.[5]

[1](PhD.); Department of Cybersecurity Federal University of Technology, Owerri
[2](PhD.); Department of Information Technology Federal University of Technology, Owerri
[3](PhD.); ICT Directorate; Alvan Ikoku Federal University of Education, Owerri
[4](PhD.); Department of Information Technology Federal University of Technology, Owerri
[5](PhD); Department of Computer Science Federal University of Technology, Owerri

[1][https://orcid.org/0000-0003-3152-6788]
[2][https://orcid.org/0000-0001-9095-7196]
[3][https://orcid.org/0000-0002-1979-6446]
[4][https://orcid.org/0000-0003-3736-8143]
[5][https://orcid.org/0000-0003-1771-5806]

Publication Date: 2026/09/02

Abstract: The increasing adoption of digital banking services and remote connectivity has heightened the demand for secure, reliable, and resilient communication infrastructures within the financial sector. Financial institutions require network solutions that safeguard sensitive information exchanged among headquarters, branch offices, and remote users against unauthorised access, interception, and other cyber threats. Conventional networking approaches often face limitations in security, scalability, and fault tolerance, creating the need for more robust Virtual Private Network (VPN) architectures. This study presents the design and implementation of a secure VPN framework that integrates Internet Protocol Security (IPSec), Generic Routing Encapsulation (GRE), and the Open Shortest Path First (OSPF) routing protocol to facilitate secure and efficient communication across geographically distributed banking networks. The framework was modelled using Unified Modelling Language (UML) and implemented in Cisco Packet Tracer to simulate connectivity between a bank's headquarters, two branch offices, and remote users. To ensure the confidentiality, integrity, and authenticity of transmitted information, the system employed Advanced Encryption Standard (AES-256) encryption, Secure Hash Algorithm (SHA-256) hashing, and Authentication, Authorisation, and Accounting (AAA) services. Dynamic routing was achieved through OSPF, enabling rapid route optimisation and automatic recovery during network failures. Performance evaluation demonstrated the effectiveness of the proposed framework. The implementation achieved a 100% VPN tunnel establishment success rate, an average network latency of 3.4ms, throughput stability of approximately 98%, and zero packet loss during the transmission of 1,000 data packets. In addition, OSPF restored network connectivity in less than two seconds following simulated link failures, ensuring uninterrupted communication among all network nodes. The findings indicate that the integration of IPSec, GRE, and OSPF provides a secure, scalable, and resilient VPN solution capable of supporting inter-branch and remote banking communications. The proposed framework strengthens data confidentiality, improves network availability, and enhances communication reliability while providing a practical and cost-effective approach for secure remote access and business continuity in modern banking environments.

Keywords: *Virtual Private Network (VPN), IPSec, GRE, OSPF, AAA, Remote Access.*

How to Cite: Ewunonu T. C.; Etus C.; Chuks-Ugochukwu C. M.; Esomonu N. F.; Benson-Emenike M. E. (2026) Design and Implementation of a Secure IPSec -GRE Virtual Private Network Framework for Remote Banking Communications. *International Journal of Innovative Science and Research Technology*, 11(8), 2479-2490. https://doi.org/10.38124/ijisrt/26aug878

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug878

I. INTRODUCTION

The banking industry has experienced significant transformation over the past decade due to rapid advances in Information and Communication Technology (ICT). These developments have fundamentally changed how financial institutions deliver services, process transactions, and exchange information across geographically distributed branches and digital platforms (Stallings, 2017). The widespread adoption of internet banking, cloud computing, and mobile financial services has further increased dependence on secure communication networks. This shift became even more pronounced during the COVID-19 pandemic, when many banks adopted remote working arrangements to ensure business continuity. Consequently, protecting communications between headquarters, branch offices, and remote employees has become a critical cybersecurity priority.

As financial institutions continue to expand their digital infrastructure, they face growing exposure to cyber threats such as unauthorised access, credential theft, packet interception, and man-in-the-middle (MitM) attacks. These threats compromise the confidentiality and integrity of sensitive financial information, disrupt business operations, and may result in substantial financial and reputational losses. Recent industry reports indicate that attacks targeting Virtual Private Networks (VPNs) and remote-access services remain among the most common attack vectors against financial organisations (Cisco Systems, 2023). These developments highlight the need for communication frameworks that provide robust security while maintaining reliable network performance.

Historically, banks relied on Wide Area Network (WAN) technologies such as leased lines, Frame Relay, and Multiprotocol Label Switching (MPLS) to interconnect geographically dispersed branches. Although these technologies provide dependable connectivity, they are associated with high deployment and maintenance costs and offer limited flexibility for rapidly expanding networks (Guzman, 2023). In many developing countries, these cost constraints have encouraged institutions to utilise public internet infrastructure for branch connectivity and remote access, thereby increasing exposure to cybersecurity risks.

Virtual Private Network (VPN) technology has emerged as a practical solution for securing communications over public networks. By creating encrypted tunnels between communicating endpoints, VPNs provide confidentiality, integrity, and authentication while reducing infrastructure costs (Kumar & Patel, 2021). Among the available VPN technologies, Internet Protocol Security (IPSec) remains one of the most widely adopted because it offers comprehensive protection through strong encryption algorithms, including the Advanced Encryption Standard (AES), and secure hashing mechanisms such as SHA-256 (Zhou, 2022). Authentication, Authorisation, and Accounting (AAA) services further strengthen network security by ensuring that only authenticated and authorised users can access protected resources while maintaining detailed records of user activities (Rose, Borchert, Mitchell, & Connelly, 2020). In addition, the integration of Generic Routing Encapsulation (GRE) with IPSec enables dynamic routing protocols, including the Open Shortest Path First (OSPF) protocol, to operate efficiently across encrypted tunnels, thereby improving scalability, redundancy, and fault tolerance (Whitman & Mattord, 2023).

Several researchers have proposed approaches to improving secure remote communication. Cheswick, Bellovin, and Rubin (2013) introduced an enhanced IPSec-based enterprise VPN architecture incorporating dynamic routing capabilities. Kurose and Ross (2021) examined the integration of Multi-Factor Authentication (MFA) with VPN gateways to mitigate credential theft, while Thottoli (2023) investigated hybrid cryptographic techniques combining AES-256 with Elliptic Curve Diffie-Hellman (ECDH) to improve both security and computational efficiency. Similarly, Singh and Brown (2022) demonstrated that IPSec VPNs provide stronger confidentiality and integrity than SSL VPNs for financial environments. More recently, Porfirio (2024) emphasised the importance of Zero Trust Architecture (ZTA), which continuously verifies users and devices to complement conventional VPN security.

Despite these advances, several limitations remain evident in existing VPN implementations. Many solutions rely on static routing, provide limited redundancy during network failures, or fail to integrate encryption, authentication, and dynamic routing into a unified architecture. In addition, centralised authentication mechanisms are often absent, increasing the risk of unauthorised access and identity spoofing (Cisco Networking Academy, 2023). These shortcomings underscore the need for a more comprehensive VPN framework capable of delivering secure communication, dynamic routing, automated failover, and centralised access control within a single integrated solution.

To address these challenges, this study presents the design and implementation of a secure VPN framework that combines IPSec, GRE tunnelling, OSPF dynamic routing, and AAA services. The proposed architecture provides end-to-end encryption, efficient routing, rapid fault recovery, and secure authentication for communication between a bank's headquarters, branch offices, and remote users. By integrating these technologies into a unified framework, the study aims to enhance data confidentiality, network resilience, service availability, and operational efficiency in modern banking environments.

- *Problem Statement*

Secure and reliable communication is fundamental to modern banking operations, enabling financial institutions to support inter-branch transactions, customer services, digital banking platforms, and remote access to organisational resources. As banks increasingly depend on internet-based communication and cloud-enabled services, sensitive financial information is routinely transmitted across public networks. This growing dependence has heightened exposure to cybersecurity threats, including unauthorised access, data

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug878

interception, packet manipulation, man-in-the-middle (MitM) attacks, and service disruptions.

Although Virtual Private Networks (VPNs) are widely employed to secure communications over public infrastructure, many existing implementations primarily emphasise data encryption while giving limited attention to routing resilience, scalability, and centralised access control. Consequently, organisations may experience inefficient traffic management, extended recovery periods following network failures, and difficulties supporting secure communication among multiple branch offices and geographically distributed users. These limitations can adversely affect service availability, operational continuity, and customer confidence.

Furthermore, several enterprise network deployments implement IPSec, GRE tunnelling, dynamic routing protocols, or authentication mechanisms as separate technologies rather than as components of an integrated security architecture. The absence of a unified framework reduces operational efficiency and limits the ability of financial institutions to achieve secure communication, automated failover, dynamic route optimisation, and centralised user authentication simultaneously.

In view of these challenges, there is a need for a secure, resilient, and scalable VPN architecture that combines encrypted communication, intelligent routing, rapid fault recovery, and robust access control within a single framework. This study addresses this need by designing and implementing an integrated IPSec–GRE Virtual Private Network that incorporates Open Shortest Path First (OSPF) for dynamic routing and Authentication, Authorisation, and Accounting (AAA) services for centralised user management. The proposed framework is intended to provide secure, reliable, and efficient communication among a bank's headquarters, branch offices, and remote users while improving network availability, operational resilience, and overall security.

➢ *Objectives of the Study*

The primary objective of this study is to design, implement, and evaluate a secure, resilient, and scalable Virtual Private Network (VPN) framework for banking communications by integrating Internet Protocol Security (IPSec), Generic Routing Encapsulation (GRE), Open Shortest Path First (OSPF), and Authentication, Authorisation, and Accounting (AAA). The proposed framework is intended to provide secure communication between a bank's headquarters, branch offices, and remote users while ensuring efficient routing, rapid fault recovery, robust access control, and high network performance.

To achieve this objective, the study seeks to:

- Design a secure VPN architecture that integrates IPSec, GRE, and OSPF to support secure communication among geographically distributed banking networks.
- Implement the proposed VPN framework using Cisco Packet Tracer as the simulation environment.
- Integrate Authentication, Authorisation, and Accounting (AAA) services to provide centralised user authentication, authorisation, and accounting for secure remote access.
- Evaluate the performance of the implemented framework using key network performance indicators, including VPN tunnel establishment success rate, latency, throughput, packet loss, and OSPF routing reconvergence time.
- Assess the suitability of the proposed framework for supporting secure, reliable, and resilient communication in modern banking environments.

II. SUMMARY OF LITERATURE REVIEW

This work reviewed the conceptual, theoretical and empirical frameworks for achieving the system design and analysis. Table 1 presents the summary of the reviewed existing work and their inherent difference from the proposed system.

Table 1 Summary of the Related Existing Work Reviewed

Author(s) & Year	Study Focus	Method/Technology Used	Key Findings	Limitations/Research Gap
Stallings (2017)	ICT transformation in banking communication	Enterprise networking and ICT infrastructure	ICT has significantly improved banking operations and communication across distributed branches.	Did not address secure VPN implementation for remote workers or cybersecurity challenges.
Kent & Seo (2015)	Internet Protocol Security (IPSec) architecture	IPSec security framework	IPSec provides authentication, confidentiality, and integrity for IP communications.	Focused on IPSec standards without integrating dynamic routing or enterprise VPN resilience.
Cisco Systems (2023)	Remote-access cyber threats in financial institutions	Security threat analysis	Financial institutions face increasing attacks on VPNs and remote desktop services.	Identified threats but did not propose an integrated secure VPN solution.
Guzman (2023)	Traditional WAN technologies	Leased lines, Frame Relay, MPLS	Traditional WANs provide reliable connectivity but	Lacks scalability and cost efficiency for geographically

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug878

			incur high deployment and maintenance costs.	distributed banking environments.
Kumar & Patel (2021)	VPN technologies for secure communication	VPN over public Internet	VPNs provide secure and cost-effective communication through encrypted tunnels.	Limited discussion on redundancy, dynamic routing, and fault tolerance.
Zhou (2022)	IPSec encryption techniques	AES encryption and SHA-256 hashing	Demonstrated strong encryption and secure authentication for VPN communication.	Focused primarily on cryptographic security without addressing routing resilience.
Rose, Borchert, Mitchell & Cornell (2020)	Authentication, Authorisation and Accounting (AAA)	AAA framework	AAA improves user authentication, authorisation, and accounting for secure network access.	Did not integrate AAA with a complete VPN architecture for banking applications.
Whitman & Mattord (2023)	GRE and dynamic routing integration	GRE tunnels with OSPF routing	GRE enables transport of routing protocols while OSPF improves scalability and network resilience.	Did not evaluate the framework specifically within banking environments.
Cheswick, Bellovin & Rubin (2013)	Secure enterprise VPN architecture	IPSec with dynamic routing	Proposed an improved IPSec framework for enterprise communication.	Limited evaluation of failover performance and centralised authentication.
Kurose & Ross (2021)	VPN gateway authentication	Multi-Factor Authentication (MFA)	MFA significantly reduces credential theft and unauthorised remote access.	Did not address routing optimisation or VPN redundancy.
Thottoli (2023)	Hybrid encryption for remote access	AES-256 with Elliptic Curve Diffie-Hellman (ECDH)	Improved security and computational efficiency during secure communication.	Concentrated on cryptographic enhancement without dynamic routing integration.
Singh & Brown (2022)	Comparison of SSL VPN and IPSec VPN	Comparative performance analysis	IPSec VPN provides stronger confidentiality and integrity than SSL VPN for financial institutions.	Did not incorporate redundancy mechanisms or centralised authentication.
Porfirio (2024)	Zero Trust Architecture (ZTA)	Continuous identity verification	Zero Trust complements VPN security by continuously validating users and devices.	Does not replace the need for resilient VPN routing and encrypted tunnelling.
Cisco Academy (2023)	Enterprise VPN deployment challenges	VPN implementation best practices	Highlighted problems such as poor scalability, static configurations, and lack of automated failover in many VPN deployments.	Recommended stronger integration of authentication, redundancy, and dynamic routing but did not present an implementation.

➢ *Research Gap*

The empirical review of literature in this work showed the following research needs to explore, which the proposed network system model seems to fix:

Table 2 Research Gap

Identified Gap	**How This Research Addresses It**
Poor scalability in existing VPN implementations	Integrates OSPF dynamic routing to support scalable multi-branch banking networks.
Static routing configurations	Employs OSPF to enable automatic route discovery and rapid network convergence.
Lack of redundancy and automatic failover	Combines GRE tunnels with OSPF to ensure resilient communication during link failures.
Limited integration of security mechanisms	Integrates IPSec, GRE, OSPF, and AAA into a unified secure communication framework.
Weak centralized authentication	Implements Authentication, Authorisation, and Accounting (AAA) for centralised access control.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug878

Limited evaluation using performance metrics	Evaluates the framework using tunnel establishment success, latency, throughput, packet loss, and routing reconvergence time.
Few banking-specific VPN implementations	Designs and validates a secure VPN architecture specifically for banking headquarters, branch offices, and remote workers.

III. METHOD

This study adopted a simulation-based research design to develop and evaluate a secure Virtual Private Network (VPN) framework for banking communications. The approach combined Unified Modelling Language (UML) for system analysis and design with Cisco Packet Tracer for network implementation and performance evaluation. A simulation-based methodology was selected because it provides a practical and cost-effective means of designing, configuring, and validating complex network architectures without the financial and operational constraints associated with physical deployment.

The research was conducted in two sequential phases. The first phase focused on conceptual system modelling using UML diagrams to define the architecture, functional requirements, and interactions among the major components of the proposed VPN framework. The second phase involved implementing the modelled architecture in Cisco Packet Tracer, followed by configuration, testing, and performance evaluation under simulated banking network conditions.

➢ *UML System Modelling*

UML modelling was employed to define the structural and behavioural aspects of the proposed VPN framework.

- Use Case Diagram: This diagram identifies the primary system actors—namely the network administrator, remote user, and router—and illustrates their interactions with the VPN framework. The major use cases include user authentication, VPN tunnel establishment, encrypted data transmission, and network administration. Figure 1 identifies the main actors (administrator, remote user, and router) and the core interactions, such as authentication, connection establishment, and data transfer.

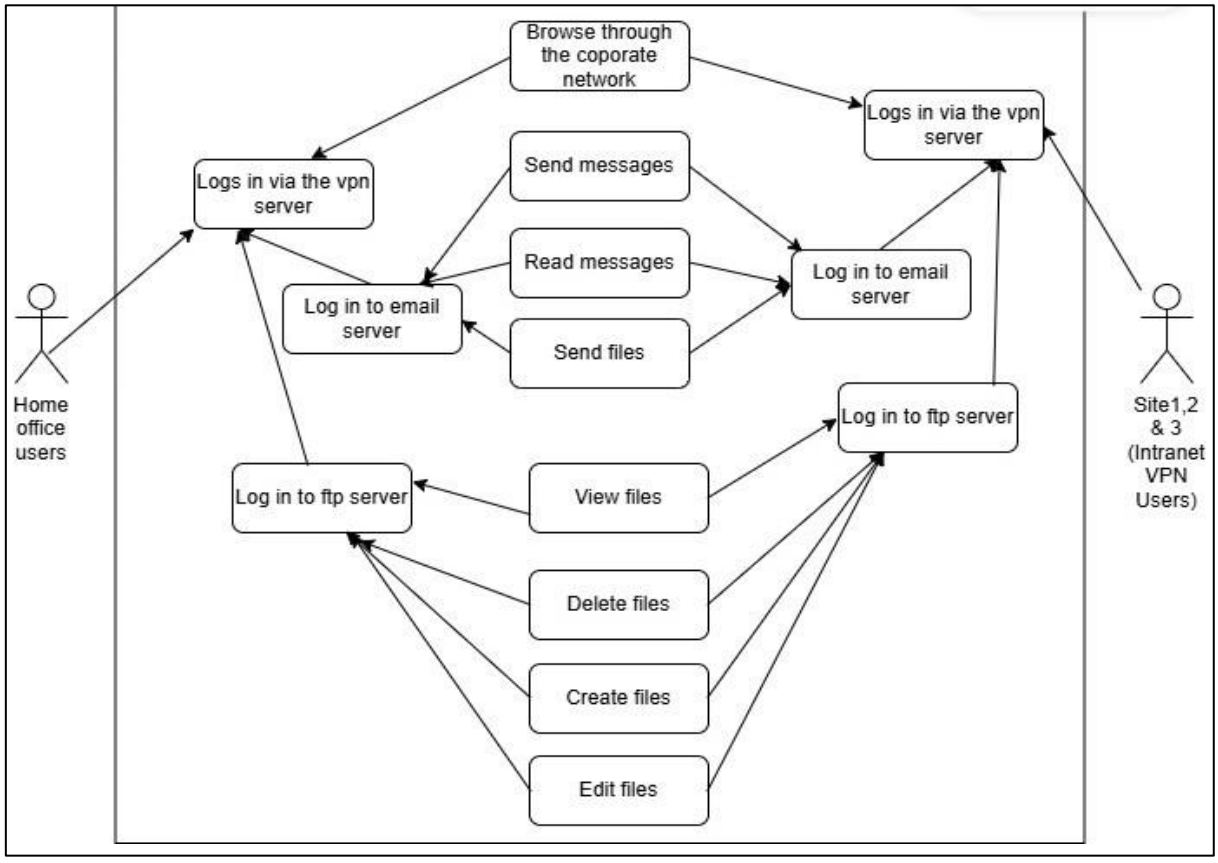

Fig 1 Use Case Diagram

- Component Diagram: The component diagram illustrates the relationships among the major functional elements of the proposed architecture, including IPSec encryption modules, GRE tunnels, AAA authentication services, OSPF routing processes, and network devices. Figure 2 depicts the key components of the VPN system and their relationships, including encryption modules, authentication entities, and routing functions.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug878

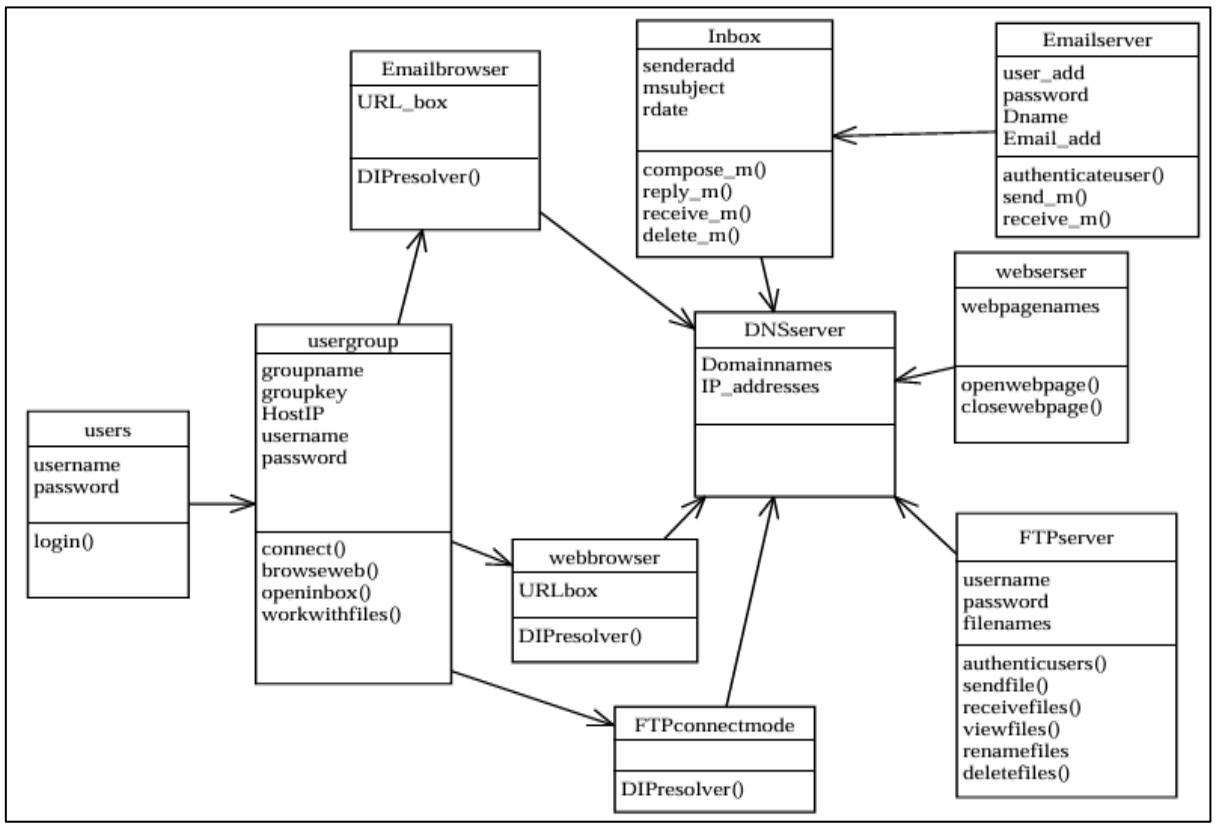

Fig 2 Components of the VPN System

- Sequence Diagram: The sequence diagram describes the operational workflow of the system, beginning with user authentication through the AAA service, followed by tunnel establishment using IPSec, secure data transmission, and session termination. Figure 3 shows the operational sequence, starting from user login through AAA verification to the establishment of an encrypted tunnel and transmission of secured data.

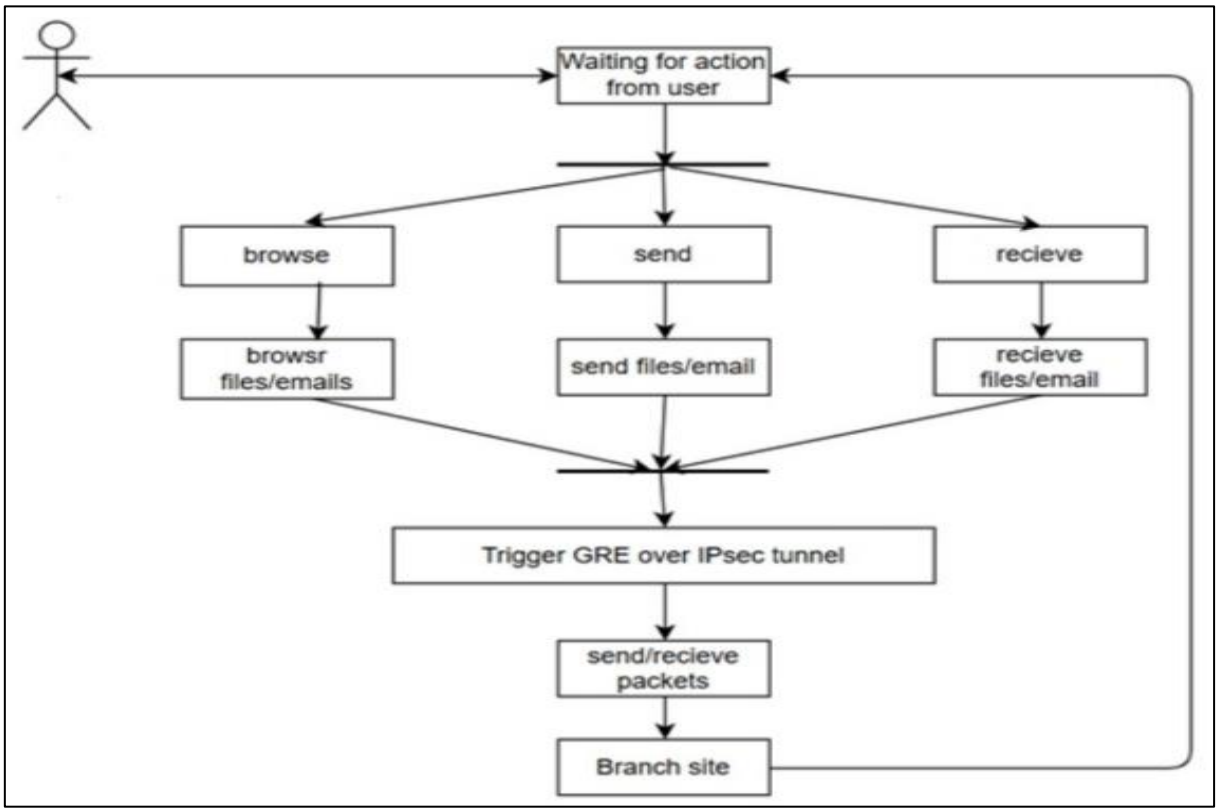

Fig 3 Operational Sequence

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug878

The UML models ensured that the implementation accurately reflected the intended system architecture and operational processes.

➢ *Simulation Environment Setup*

The proposed framework was implemented and evaluated using Cisco Packet Tracer version 8.2 on a Windows 11 workstation. Cisco 2911 routers served as VPN gateways connecting the headquarters, two branch offices, and remote users through a simulated public Internet infrastructure.

The simulated banking network was divided into four logical subnets:

- Headquarters LAN: 172.21.0.0/24
- Branch A LAN: 172.21.1.0/24
- Branch B LAN: 172.21.2.0/24
- Remote Users: 172.21.100.0/24

Static IP addressing was assigned to routers and core network devices to ensure consistent peer identification, while Dynamic Host Configuration Protocol (DHCP) was configured for remote users to simplify address allocation and network management.

➢ *IPSec Remote-Access VPN Configuration*

A remote-access VPN architecture was developed to enable authorised employees to securely access internal banking resources from remote locations. The headquarters router functioned as the VPN server, while remote users established encrypted IPSec tunnels through authenticated connections.

The VPN configuration incorporated the following security mechanisms:

- Encryption Algorithm: AES-256
- Integrity Algorithm: SHA-256
- Key Management: Internet Key Exchange Version 2 (IKEv2)
- Authentication: Pre-shared keys integrated with Authentication, Authorisation, and Accounting (AAA)

Remote users were required to authenticate through the AAA service before VPN tunnel establishment. Upon successful authentication, all traffic exchanged between remote users and the banking network was encapsulated within IPSec tunnels to ensure confidentiality, integrity, and authenticity. The logical flow of this architecture is illustrated in *Fig. 4.*

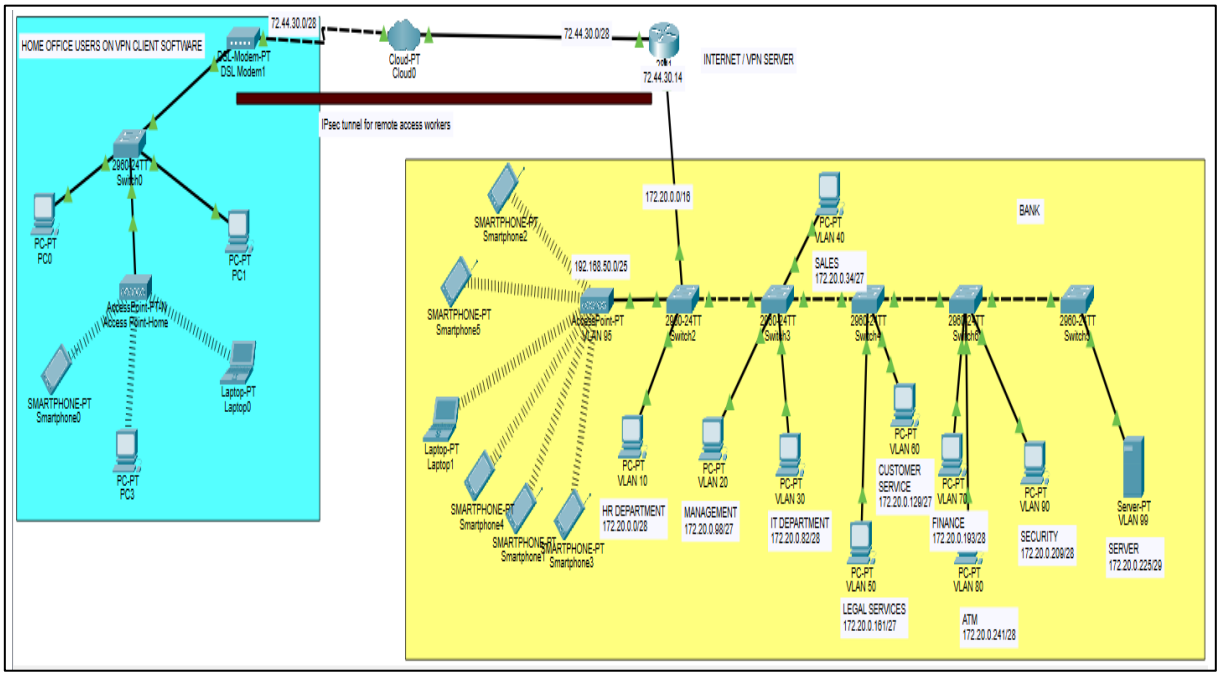

Fig 4 Logical Model of the Proposed IPSec Remote Access VPN

➢ *Site-to-Site VPN Architecture*

A site-to-site VPN was implemented to establish secure communication between the bank's headquarters and two branch offices. Cisco 2911 routers located at each site functioned as VPN endpoints.

To support dynamic routing across encrypted tunnels, Generic Routing Encapsulation (GRE) was deployed over IPSec. GRE enabled the transportation of routing information, while Open Shortest Path First (OSPF) dynamically managed route discovery, route updates, and automatic failover whenever communication links became unavailable.

This integrated GRE-over-IPSec architecture combined strong encryption with routing flexibility, resulting in improved scalability and enhanced network resilience. The physical model of the GRE-over-IPSec setup is shown in *Figure 5*, while *Figure 6* illustrates the logical topology.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug878

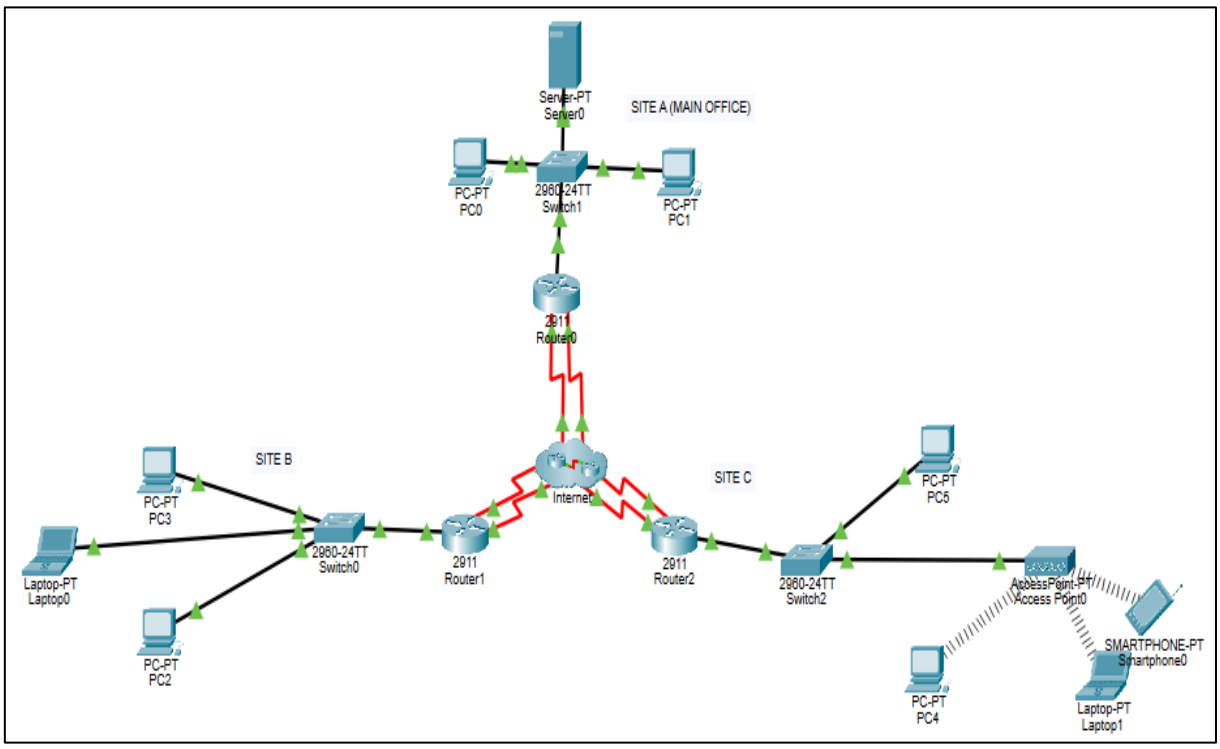

Fig 5 Physical Model of the Proposed Site-to-Site GRE over IPSec VPN

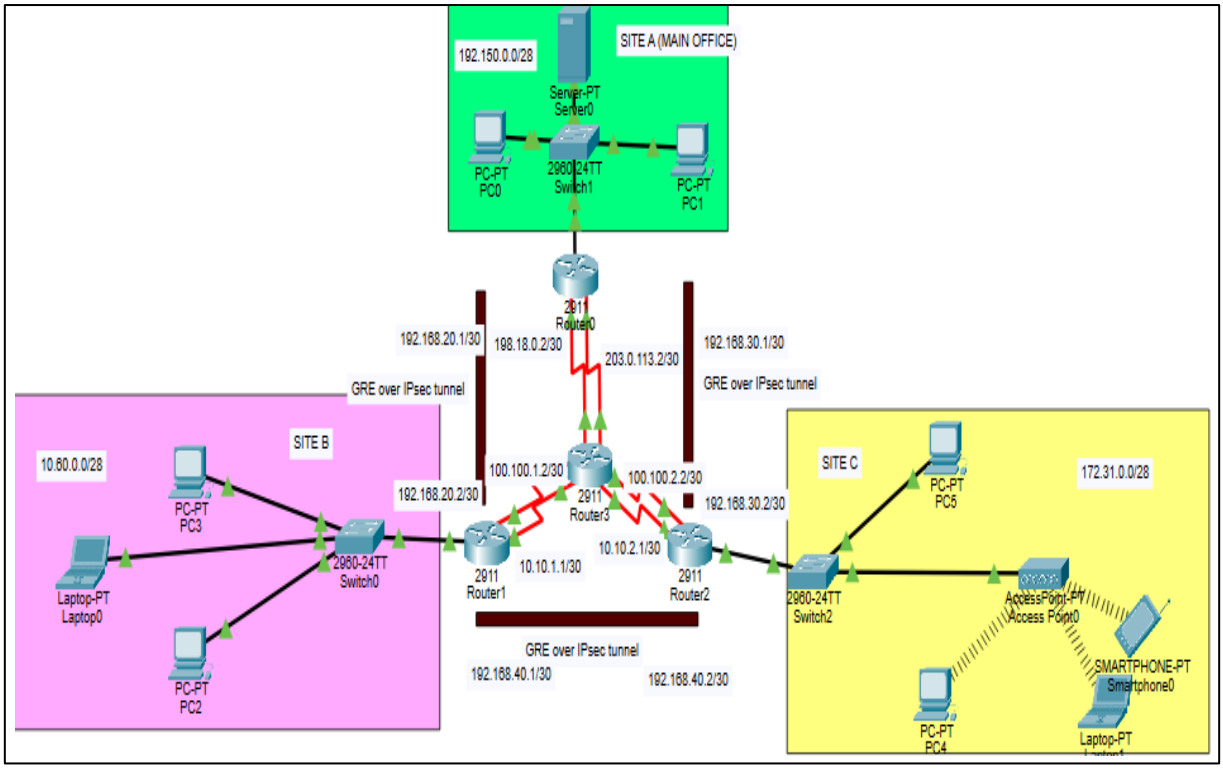

Fig 6 Logical Model of the Proposed Site-to-Site GRE over IPSec VPN

➢ *Security Mechanisms*

Several complementary security mechanisms were incorporated into the proposed framework to strengthen network protection:

- AES-256 Encryption: Protected the confidentiality of transmitted data.
- SHA-256 Hashing: Ensured message integrity and detected unauthorised modifications.
- AAA Services: Provided centralised authentication, authorisation, and accounting for all VPN users.
- Access Control Lists (ACLs): Restricted unauthorised access to sensitive network resources.
- IKEv2: Performed secure negotiation and management of cryptographic keys.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug878

- OSPF Dynamic Routing: Enabled automatic route optimisation and rapid recovery following network failures.

The integration of these mechanisms provided multiple layers of security while maintaining efficient and reliable communication across the distributed banking network.

➢ *Performance Evaluation*

The effectiveness of the proposed VPN framework was assessed using quantitative performance metrics obtained from the simulation environment. The evaluation focused on both network performance and security effectiveness.

The following metrics were used:

- VPN tunnel establishment success rate
- End-to-end network latency
- Throughput stability
- Packet loss
- OSPF routing reconvergence time
- Authentication success
- VPN connectivity verification

Verification commands, including show crypto isakmp sa, show crypto ipsec sa, show aaa session, show ip ospf neighbour, and show ip route ospf, were executed to confirm successful tunnel establishment, encryption, authentication, and dynamic routing performance.

The collected results were analysed to determine whether the proposed framework satisfied the security, reliability, scalability, and performance requirements expected in modern banking communication networks.

IV. RESULTS AND DISCUSSION

➢ *System Verification and Connectivity Evaluation*

Following the implementation of the proposed VPN framework, several verification procedures were conducted to confirm the successful establishment of secure communication channels and the correct operation of routing services. Cisco IOS verification commands, including show crypto isakmp sa and show crypto ipsec sa, were executed on the headquarters and branch routers to validate the status of the IPSec tunnels.

The verification results confirmed that both Internet Key Exchange (IKE) Phase 1 and Phase 2 negotiations completed successfully for all VPN peers. Correspondingly, active IPSec Security Associations (SAs) were established between the headquarters, branch offices, and remote users, demonstrating that the encrypted communication channels were operating as intended (Figure 7).

Network connectivity was further evaluated using ICMP echo requests between remote users and internal banking resources. Successful responses were received across all configured VPN tunnels, confirming that encrypted traffic was transmitted correctly and that routing information was consistently synchronised through the OSPF protocol (Figure 8).

The tunnel verification results presented in Table 1 indicate that all configured VPN connections achieved successful establishment, corresponding to a 100% tunnel establishment success rate. The simulation output confirmed that the IKE Phase 1 and Phase 2 negotiations completed successfully, and IPSec Security Associations (SAs) were active between VPN peers, as shown in Figure7.

```
Router#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
72.44.30.2      72.44.30.14     QM_IDLE           1055    0 ACTIVE


IPv6 Crypto ISAKMP SA
```

Fig 7 ISAKMP (Internet Security Association and Key Management Protocol) Status for Remote Access VPN.

Table 1 summarises the verification results of all configured tunnels. The simulation confirmed 100% tunnel establishment success across all connections.

Table 3 VPN Tunnel Verification

Tunnel Pair	IKE Phase 1	IKE Phase 2	Status
HQ↔ Branch A	Completed	Completed	Active
HQ↔ Branch B	Completed	Completed	Active
HQ↔ Remote Users	Completed	Completed	Active

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug878

```
C:\>ping 172.20.0.34

Pinging 172.20.0.34 with 32 bytes of data:

Reply from 72.44.30.14: Destination host unreachable.
Reply from 72.44.30.14: Destination host unreachable.
Reply from 72.44.30.14: Destination host unreachable.
Reply from 72.44.30.14: Destination host unreachable.

Ping statistics for 172.20.0.34:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 172.20.0.34

Pinging 172.20.0.34 with 32 bytes of data:

Request timed out.
Reply from 172.20.0.34: bytes=32 time=56ms TTL=127
Reply from 172.20.0.34: bytes=32 time=85ms TTL=127
Reply from 172.20.0.34: bytes=32 time=74ms TTL=127

Ping statistics for 172.20.0.34:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
```

Fig 8 Ping Test Showing Banking Resources Readily Available to Remote Access User

➢ *Network Performance Evaluation*

The performance of the proposed framework was assessed using latency, throughput, and packet loss measurements obtained during the simulation.

Across all communication links, the average network latency was 3.4ms, while the highest observed delay under concurrent traffic conditions was 5.1ms. Throughout the transmission of 1,000 ICMP packets, no packet loss was recorded, and throughput stability remained above 98% for all VPN tunnels.

As summarised in Table 2, the headquarters-to-Branch A connection achieved an average latency of 3.2ms, whereas Branch B recorded 3.6ms. Remote users experienced an average latency of 3.4ms, with throughput remaining consistently above 97.9%.

These results demonstrate that the cryptographic processing introduced by IPSec imposed only minimal communication overhead and did not significantly affect network performance.

Table 4 Latency and Throughput Results

Link	Average Latency (ms)	Throughput (%)	Packet Loss (%)
HQ↔Branch A	3.2	98.8	0.0
HQ↔ Branch B	3.6	97.9	0.0
HQ↔ Remote Users	3.4	98.1	0.0

➢ *Authentication and Encryption Validation*

Authentication was implemented through the Authentication, Authorisation, and Accounting (AAA) framework to ensure that only legitimate users could establish VPN sessions.

Before tunnel establishment, remote users were required to provide valid credentials, after which successful authentication was confirmed using the show aaa session command. The accounting service recorded user logins, logout times, and session activities, thereby providing comprehensive audit trails for network administration and security monitoring.

Encryption performance was validated using the show crypto ipsec sa command, which confirmed that all transmitted packets were encrypted before traversing the simulated public network and successfully decrypted at their respective destinations. Packet counters maintained a 1:1 encryption-to-decryption ratio, demonstrating that data integrity and confidentiality were preserved throughout transmission.

The AAA logs recorded 25 successfully authenticated user sessions, each associated with unique usernames and timestamps, indicating reliable user authentication and effective access control.

➢ *Routing Performance and Network Resilience*

The operation of the Open Shortest Path First (OSPF) routing protocol was verified using the show ip ospf neighbour and show ip route ospf commands.

Results confirmed that neighbouring routers successfully established OSPF adjacencies and maintained synchronised routing tables throughout the simulation period. Dynamic routing enabled the automatic exchange of routing information across GRE tunnels encapsulated within IPSec,

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug878

ensuring efficient communication among all network segments.

To evaluate network resilience, one GRE tunnel was intentionally disabled during operation. OSPF immediately recalculated the routing topology and redirected traffic through the available communication path. Connectivity was restored in less than 2 seconds, with an average reconvergence time of 1.8 seconds, as presented in Table 3.

The rapid recovery demonstrates the effectiveness of integrating GRE with OSPF for maintaining service continuity during network failures.

Table 5 OSPF Failover Performance

Condition	Link Status	Convergence Time (s)	Connectivity Restored
HQ–Branch A Failure	Down	1.7	Yes
HQ–Branch B Failure	Down	1.9	Yes

➢ *Overall Performance Assessment*

The proposed VPN framework consistently demonstrated high levels of security, stability, and operational efficiency throughout the simulation.

Key performance outcomes include:

- 100% VPN tunnel establishment success
- Average network latency of 3.4ms
- Throughput stability exceeding 98%
- Zero packet loss during transmission of 1,000 packets
- Average OSPF reconvergence time of 1.8 seconds
- Successful authentication of all authorised users
- Reliable encrypted communication across all network segments

These findings indicate that the integration of IPSec, GRE, OSPF, and AAA provides an effective solution for secure enterprise networking while maintaining excellent communication performance.

V. FINDINGS

The simulation results demonstrate that the proposed VPN architecture satisfies the fundamental security objectives of confidentiality, integrity, availability, authentication, and network resilience. IPSec successfully protected transmitted information through robust encryption and hashing mechanisms, while AAA services ensured that only authenticated users were granted access to network resources.

The incorporation of GRE over IPSec enabled OSPF to perform dynamic routing within encrypted tunnels, overcoming a common limitation of conventional IPSec implementations that rely on static routing. Consequently, the network exhibited improved scalability, automatic route optimisation, and rapid recovery following simulated link failures.

Compared with conventional VPN architectures, the proposed framework provides greater operational flexibility, reduced service downtime, and improved fault tolerance without compromising communication security. These characteristics make the architecture particularly suitable for banking institutions and other organisations that require secure inter-branch communication, reliable remote access, and uninterrupted business operations.

Overall, the results validate the effectiveness of the proposed framework as a practical, scalable, and cost-effective solution for secure banking communications over public network infrastructure.

VI. CONCLUSION

This study presented the design, implementation, and evaluation of a secure Virtual Private Network (VPN) framework for banking communications through the integration of Internet Protocol Security (IPSec), Generic Routing Encapsulation (GRE), Open Shortest Path First (OSPF), and Authentication, Authorisation, and Accounting (AAA) services. The framework was developed and validated using Cisco Packet Tracer to simulate secure communication among a bank's headquarters, branch offices, and remote users.

The simulation results demonstrate that the proposed architecture successfully achieved the study's objectives by providing secure, reliable, and resilient communication across distributed banking networks. The implementation recorded a 100% VPN tunnel establishment success rate, average network latency of 3.4 ms, throughput stability exceeding 98%, zero packet loss during the transmission of 1,000 packets, and OSPF routing reconvergence within an average of 1.8 seconds following simulated network failures. These findings indicate that the integrated framework effectively maintains communication security while delivering excellent network performance and rapid fault recovery.

The incorporation of GRE over IPSec enabled dynamic routing within encrypted tunnels, thereby improving scalability and operational flexibility compared with conventional static VPN configurations. In addition, the implementation of AAA services strengthened access control by ensuring that only authenticated users could establish VPN sessions, while comprehensive accounting records enhanced network monitoring and security auditing.

Overall, the proposed VPN framework provides a practical, scalable, and cost-effective solution for secure inter-branch communication and remote banking operations. By integrating encryption, secure tunnelling, dynamic

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug878

routing, and centralised authentication within a unified architecture, the framework enhances data confidentiality, network availability, and service continuity. Consequently, it offers a viable approach for financial institutions seeking to strengthen the security and resilience of their communication infrastructure while supporting the growing demand for secure remote access.

REFERENCES

[1]. Cheswick, W.R.; Bellovin, S.M.; Rubin, A.D. (2013). "Firewalls and Internet Security: Repelling the WilyHacker",2nded.Addison-Wesley.
[2]. Cisco Networking Academy (2023). "Packet Tracer Network Simulation Tool: User Guide", 2023.
[3]. Cisco Systems (2023). "IPSec VPN Configuration Guide," Cisco White Paper.
[4]. Gupt, R.; Sharma, M. (2022). "Multi-Factor Authentication for Secure VPN Access," Journal of Information Security Research, vol. 19, no.4, pp. 256–264.
[5]. Guzmán, D.S. (2023). "Integration of GRE and OSPF for VPN Reliability," IEEE Access, vol. 11, pp.10430–1044
[6]. Kent, S.; Seo, K. (2015). "Security Architecture for the Internet Protocol," IETF RFC 4301.
[7]. Kumar, A.; Patel, S. (2021). "Enhanced IPSec VPN Model with Dynamic Routing," Proc. IEEE Int.Conf. on Network Security, pp. 55–62.
[8]. Kurose, L.; Ross, J. (2021). "Computer Networking: A Top-Down Approach", 8th ed. Pearson, 2021.
[9]. Porfirio, P. (2024). "ICT-Driven Modernisation in Banking Systems," Banking Technology Review, vol. 18, no.2, pp. 102–110.
[10]. Rose, S.; Borchert, O.; Mitchell, S.; Connelly, S. (2020). "Zero Trust Architecture," NIST Special Publication800-207.
[11]. Singh, S.; Brown, R. (2022). "Assessing Vulnerabilities in Remote Banking Systems," Cybersecurity Trends, vol. 7, no.1, pp.21–34.
[12]. Stallings, W. (2017). "Data and Computer Communications", 10th ed. Pearson Education.
[13]. Thottoli, A. (2023). "Digital Transformation in Financial Institutions: Post-Pandemic Trends," Journal of Financial Innovation, vol. 11, no. 3, pp. 45–56, 2023.
[14]. Whitman, T.; Mattord, H. (2023). Principles of Information Security, 6th ed. Cengage Learning.
[15]. Zhou, H. (2022). "Hybrid Cryptographic Optimisation for VPN Communication," Computer Communications, vol. 191, pp. 10–19.