Vokasi Unesa Bulletin of Engineering, Technology and Applied Science (VUBETA)
https://journal.unesa.ac.id/index.php/vubeta
Vol. 2, No. 3, 2025, pp. 412~427 DOI: 10.26740/vubeta.v2i3.39105
ISSN: 3064-0768

Design of an Enterprise Network Terminal Security Solution

Muhammad Idris Abubakar[1*], Ajayi Ore-Ofe[2], Abubakar Umar[3], Ibrahim Ibrahim[4], Lawal Abdulwahab Olugbenga[5], Ajikanle Abdulbasit Abiola[6]
[1,2,3,4,5,6] Department of Computer Engineering, Faculty of Engineering, Ahmadu Bello University, Zaria, Nigeria

Article Info

Article history:

Received February 28, 2025
Revised June 10, 2025
Accepted August 10, 2025

Keywords:

Data protection
Enterprise Network
IoT Devices
Terminal Security
VPN Encryption

ABSTRACT

This paper presents a secure enterprise network terminal security solution designed to protect the confidentiality, integrity, and availability of critical data and network resources. It presents a logical approach to creating an enterprise network security architecture with a primary focus on optimizing and enhancing the performance of as data center servers and storage. Traditionally, network infrastructure has primarily focused security measures on core components, such as firewalls and intrusion detection/prevention systems (IDS/IPS). However, the exponential growth of Internet of Things (IoT) devices, Bring Your Device (BYOD) policies, and remote workforce trends has shifted the threat landscape, making network terminals key vectors for malicious access, with critical end devices often being the ultimate targets. This study presents a comprehensive framework that prioritizes terminal-level security by integrating existing encryption techniques, specifically a double-layer VPN tunnel architecture, to enhance data transmission confidentiality. A significant contribution of the paper lies in its structured classification of network terminals into thoughtful, intelligent, and dumb categories based on capability and memory—an approach that supports tailored security implementations. The framework also outlines contingency measures for securing data center endpoints in the event of a breach scenario. The novelty of this work lies in its focused protection strategy for terminals within enterprise environments, bridging the security gap between endpoints and core infrastructure. The proposed solution demonstrates the potential to reduce exposure to ransomware and targeted attacks through layered defenses and a proactive disaster recovery and business continuity (DR&B) strategy, despite limitations in real-world simulation due to resource constraints.

1. INTRODUCTION

Networks are vulnerable devices due to their basic feature of facilitating remote access and data communication. The information in the networks needs to be kept secure and safe to provide an effective communication and sharing device in the web of data. Due to the challenges and threats to data in networks, network security is one of the most critical considerations in information technology infrastructures. As a result, security measures are implemented in the network to decrease the probability of hackers accessing the secured data. The purpose of network security is to protect the network and its components from unauthorized access and abuse, thereby providing a safe and secure communication environment for users [1]. The Internet of Things (IoT) refers to a system of connected devices that can communicate with each other and share information with users through the internet. Information security focuses on protecting data and systems from unauthorized access, use, disclosure, or damage. It also involves managing user registration and removing access when needed, and safeguarding personal information to ensure privacy and security. Together, IoT and information security play a key role in enabling safe and reliable communication while protecting sensitive data from potential threats [2].

*Corresponding Author
Email: idrismakr@gmail.com

Leading cloud network environments such as Amazon Web Services, Microsoft Azure, IBM Cloud, VMware, and Google Cloud are widely used for their advanced features. However, these platforms remain vulnerable to attacks from ransomware groups, botnets, and advanced persistent threats (APTs) due to poor security practices, misconfigurations, and internal weaknesses. Third-party applications further increase these risks by introducing bugs or zero-day vulnerabilities that attackers can exploit to gain access to sensitive data. Without proper verification, these applications can originate from within the network, potentially being linked to an APT, posing significant security challenges for organizations [3]. Over the past decade, the number of IoT devices available worldwide has increased rapidly. Currently, the total number of these devices is close to 25 billion, and it is expected to reach 50 billion by the year 2025. This growth highlights the expanding role of IoT technology in various industries and daily life [4].

Information security, often referred to as InfoSec, is crucial for safeguarding both digital and physical information within organizations. It covers a wide range of areas, including cryptography, mobile technology, social media, and networks that store sensitive financial, personal, and corporate data. The main objectives of InfoSec are to ensure the confidentiality, integrity, and availability of this information. Due to its broad nature, InfoSec involves implementing various security measures across these domains to safeguard critical information effectively [5]. It is essential to establish a clear security policy for the marketing information system to protect the confidentiality, accuracy, and accessibility of the data. This ensures that reliable information is available to support the development of effective marketing strategies, which can meet customer needs and expectations in a timely and satisfactory manner [6]. Libraries and information systems face significant risks related to security and safety. Addressing these challenges can be achieved by adopting modern technologies and setting practical standards to ensure protection and reliability [7].

Information security can be understood across technical, formal, and informal levels. In computer systems, various measures are used to protect software, devices, and data. These include tools such as firewalls, speech analysis, digital signatures, and other techniques designed to safeguard the system from potential threats [8]. Information security has become a critical concern for both individuals and organizations due to the increasing rate of cybercrimes. These crimes often target individuals and include personal data breaches, phishing, identity theft, credit card fraud, extortion, impersonation, malware, ransomware, and crimes involving children. To address these challenges, research in information security has focused on understanding why users fail to take adequate precautions to protect themselves from such threats and how they can be encouraged to adopt adequate security measures [9]. Several studies have shown that insiders remain the most vulnerable point in information security. Despite various measures put in place to prevent attacks, hackers still manage to access sensitive information. Cyber-attacks do not always start with software alone, as software relies on hardware and human factors within a security system. Insiders and hardware weaknesses provide opportunities for unauthorized access. With the rise of remote work and cloud-based systems, the risk has grown significantly, requiring a more focused and adaptable security approach to address these emerging threats [10]. Physical isolation plays a key role in safeguarding classified information systems by preventing unauthorized access and data leakage from the network. Currently, physical isolation is achieved using security tools like firewalls, intrusion detection systems, unauthorized connection prevention, host monitoring, and auditing solutions [11]. Cyber attackers are constantly adapting their methods and strategies to evade the security systems that targeted organizations have implemented. Their operations have become more organized, and financial gain now serves as a significant driving factor behind their actions [12]. Many real-world examples indicate that attackers often rely on straightforward methods to compromise systems [13]. Additionally, identifying a cyberattack can frequently take a considerable amount of time, allowing attackers to exploit the system undetected. During this delay, the system remains vulnerable, and the damage can increase significantly while the breach goes unnoticed [14].

This paper contributes to the ongoing research in information security by proposing a novel approach to strengthening cloud-based IoT environments through an integrated framework that addresses both external threats and insider vulnerabilities. By analyzing current gaps and evaluating security mechanisms within modern network systems, the study presents enhanced strategies aimed at improving the resilience of interconnected systems against evolving cyber threats. The findings of this paper aim to support the future development of more secure, scalable, and adaptive security infrastructures.

1.1 COMPREHENSIVE THEORETICAL BASIS

In today's digital world, every business or organization needs to create its own corporate network. It helps employees at all levels work faster and more efficiently, but it also brings risks, especially when it comes to protecting the company’s sensitive information [15]. Network technology involves the combination of when needed, and safeguarding personal information to ensure privacy and security. Together, IoT and information security play a key role in enabling safe and reliable communication while protecting sensitive data from potential threats [2].

Leading cloud network environments such as Amazon Web Services, Microsoft Azure, IBM Cloud, VMware, and Google Cloud are widely used for their advanced features. However, these platforms remain vulnerable to attacks from ransomware groups, botnets, and advanced persistent threats (APTs) due to poor security practices, misconfigurations, and internal weaknesses. Third-party applications further increase these risks by introducing bugs or zero-day vulnerabilities that attackers can exploit to gain access to sensitive data. Without proper verification, these applications can originate from within the network, potentially being linked to an APT, posing significant security challenges for organizations [3]. Over the past decade, the number of IoT devices available worldwide has increased rapidly. Currently, the total number of these devices is close to 25 billion, and it is expected to reach 50 billion by the year 2025. This growth highlights the expanding role of IoT technology in various industries and daily life [4].

Information security, often referred to as InfoSec, is crucial for safeguarding both digital and physical information within organizations. It covers a wide range of areas, including cryptography, mobile technology, social media, and networks that store sensitive financial, personal, and corporate data. The main objectives of InfoSec are to ensure the confidentiality, integrity, and availability of this information. Due to its broad nature, InfoSec involves implementing various security measures across these domains to safeguard critical information effectively [5]. It is essential to establish a clear security policy for the marketing information system to protect the confidentiality, accuracy, and accessibility of the data. This ensures that reliable information is available to support the development of effective marketing strategies, which can meet customer needs and expectations in a timely and satisfactory manner [6]. Libraries and information systems face significant risks related to security and safety. Addressing these challenges can be achieved by adopting modern technologies and setting practical standards to ensure protection and reliability [7].

Information security can be understood across technical, formal, and informal levels. In computer systems, various measures are used to protect software, devices, and data. These include tools such as firewalls, speech analysis, digital signatures, and other techniques designed to safeguard the system from potential threats [8]. Information security has become a critical concern for both individuals and organizations due to the increasing rate of cybercrimes. These crimes often target individuals and include personal data breaches, phishing, identity theft, credit card fraud, extortion, impersonation, malware, ransomware, and crimes involving children. To address these challenges, research in information security has focused on understanding why users fail to take adequate precautions to protect themselves from such threats and how they can be encouraged to adopt adequate security measures [9]. Several studies have shown that insiders remain the most vulnerable point in information security. Despite various measures put in place to prevent attacks, hackers still manage to access sensitive information. Cyber-attacks do not always start with software alone, as software relies on hardware and human factors within a security system. Insiders and hardware weaknesses provide opportunities for unauthorized access. With the rise of remote work and cloud-based systems, the risk has grown significantly, requiring a more focused and adaptable security approach to address these emerging threats [10]. Physical isolation plays a key role in safeguarding classified information systems by preventing unauthorized access and data leakage from the network. Currently, physical isolation is achieved using security tools like firewalls, intrusion detection systems, unauthorized connection prevention, host monitoring, and auditing solutions [11]. Cyber attackers are constantly adapting their methods and strategies to evade the security systems that targeted organizations have implemented. Their operations have become more organized, and financial gain now serves as a significant driving factor behind their actions [12]. Many real-world examples indicate that attackers often rely on straightforward methods to compromise systems [13]. Additionally, identifying a cyberattack can frequently take a considerable amount of time, allowing attackers to exploit the system undetected. During this delay, the system remains vulnerable, and the damage can increase significantly while the breach goes unnoticed [14].

This paper contributes to the ongoing research in information security by proposing a novel approach to strengthening cloud-based IoT environments through an integrated framework that addresses both external threats and insider vulnerabilities. By analyzing current gaps and evaluating security mechanisms within modern network systems, the study presents enhanced strategies aimed at improving the resilience of interconnected systems against evolving cyber threats. The findings of this paper aim to support the future development of more secure, scalable, and adaptive security infrastructures.

1.2 COMPREHENSIVE THEORETICAL BASIS

In today's digital world, every business or organization needs to create its own corporate network. It helps employees at all levels work faster and more efficiently, but it also brings risks, especially when it comes to protecting the company’s sensitive information [15]. Network technology involves the combination of hardware and software, such as drivers, network adapters, cables, and connectors, along with the transmission of data through communication lines to create a functioning network. Local area networks (LANs) operate on

the same packet-switching method used in global networks for transmitting data, ensuring consistency in how traffic is managed and transferred [16]. Network topology refers to the arrangement and connection of different components, such as computers, cables, and other devices, within a data communication network. It describes both the physical setup and the process of transferring information from one device to another across the network. Network topologies can be thought of as the blueprint of the network, illustrating how devices are interconnected. Different types of network topologies exist, such as Bus, Star, Mesh, Ring, Hybrid, and Wireless topologies. Sometimes, a network may even combine more than one type of topology to meet specific needs [17].

Network security systems comprise a set of technologies, tools, and practices designed to protect computer networks from unauthorized access, cyber threats, and data breaches. These systems work together to create a layered defense that ensures the confidentiality, integrity, and availability of network resources. Security protection design is not only related to the deployment of physical (hardware and software) equipment but extends to cyber laws and policies governing the use of IT resources in any organization [18].

A firewall is a technology used to regulate connections between different networks, helping to block unauthorized access from external networks to internal systems and resources. By doing so, it protects internal networks and systems from potential threats and attacks. This technology combines both hardware and software to filter and screen potential risks actively, ensuring the network remains secure. Serving as the first line of defense, a firewall intercepts external attacks to provide essential protection for computer network security [19]. Figure 1 illustrates the connection and interaction between the Firewall, the Intranet, and the Internet in a network setup. Traditional firewalls, once the backbone of network security, are struggling to keep up with the complexity of modern threats. This challenge has led to the rise of next-generation firewalls (NGFWs) [20]. Firewalls are categorized into two main types: network firewalls and host-based firewalls. Network firewalls work on network hardware and are used to secure the connection between different networks. On the other hand, host-based firewalls focus on filtering traffic directly to individual devices or hosts, ensuring they are protected from unwanted access [21]. A firewall serves as a protective barrier, filtering traffic between internal networks and external, often less secure, networks. Its primary role is to safeguard networks from external threats while ensuring security policies allow authorized users to access necessary resources without difficulty. The effectiveness of a firewall depends on factors such as its placement and the type of data it protects, highlighting the importance of striking a balance between security and ease of access for users [22].

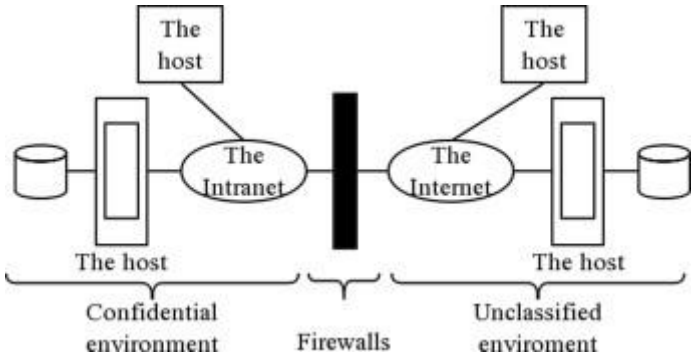

Figure 1. Connection schematic of a Firewall, Intranet, and Internet [19]

Firewalls are commonly used to secure networks, but they have limitations as they can only detect threats coming from outside the network. Over the years, the frequency and complexity of network attacks have increased significantly, prompting a growing interest in Intrusion Detection Systems (IDSs) as an alternative approach to network security. IDSs are tools designed to monitor network activity and identify malicious actions, such as data theft, protocol violations, or unauthorized access. Unlike firewalls, IDSs are effective at detecting both internal and external threats, including previously unknown attacks. However, many of the methods used in current IDSs struggle to handle the evolving and complex nature of cyberattacks. As attackers continue to develop more sophisticated techniques, existing network security measures often prove inadequate, underscoring the need for innovative methods and improvements in security technologies [23]. An Intrusion Detection System (IDS) is designed to identify and alert users about any unauthorized access or use of a computer system, helping to protect sensitive information and maintain system security [24]. IDS plays a vital role in ensuring security by working in conjunction with firewalls to manage and respond to various types of security threats effectively [25]. The first step in protecting a network involves implementing prevention methods, such as verifying user identity, encrypting data, securing the routing of information, and controlling

access. However, if an intrusion bypasses these measures, the next layer of defense is an Intrusion Detection System (IDS), which works to stop both internal and external threats from causing harm to network resources [26]. An Intrusion Prevention System (IPS) builds on a detection system by not just identifying potential attacks but also taking action to stop them when they are suspected. It works proactively to prevent security threats by analyzing data patterns, monitoring network traffic, and comparing behavior against stored records to identify any unusual activity. When an attack is detected, the IPS blocks the harmful data to protect the system [27]. Intrusion prevention works by actively adjusting network settings or resources to address and reduce identified threats [28]. The ability of IPS to both identify and block intrusions represents a significant shift in how intrusions are managed, transitioning from merely detection to active prevention [29]. Intrusion Detection Systems (IDSs) are essential when it becomes clear that IPS or security measures, such as encryption, access controls, firewalls, and similar tools, are insufficient to fully address the challenges of computer and network security [30].

Virtual Private Networks (VPNs) are a standard tool for ensuring security and reliability in online activities. However, their effectiveness depends heavily on having a stable network connection. When the connection is unstable or weak, VPNs can disconnect, leading to issues such as lost data and interrupted sessions, which can result in a frustrating user experience [31]. A virtual private network (VPN), as shown in Figure 2, is designed to meet the security and privacy needs of an organization, focusing on four key principles: compatibility, availability, security, and manageability. The concept of a VPN originated from intranet systems, with the primary goal of preventing unauthorized users from accessing the network [32].

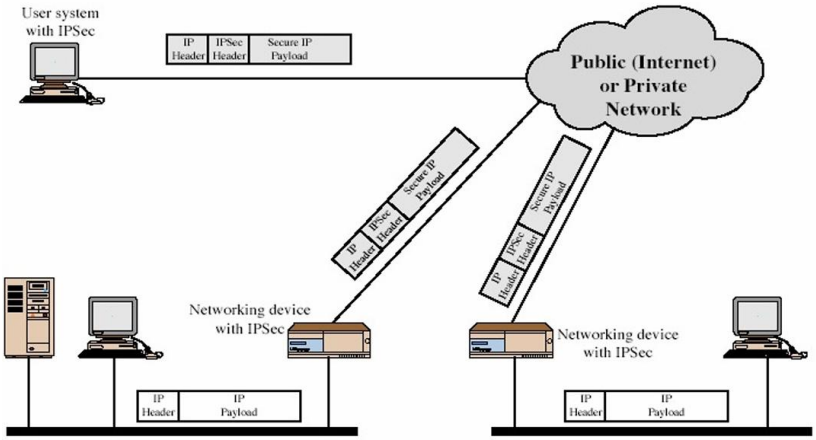

Figure 2. Basic structure that supports a VPN network [32]

DoS attacks aim to disrupt the connection between a target and its users, making the network inaccessible. They overwhelm server resources such as bandwidth, memory, and CPU power, eventually causing the entire network to fail. This often forces the targeted system to shut down and restart [33]. A DDoS attack can be compared to a traffic jam that clogs a highway, preventing regular traffic from reaching its intended destination. These attacks can take various forms, including bandwidth flooding, which overwhelms the network with excessive data, and connection flooding, which overloads the system by creating an excessive number of connections simultaneously [34]. A computer can only be completely secure if it is turned off, locked away, and buried deep underground—but even then, there's no guarantee. DDoS attacks, for example, are often driven by various motives such as revenge, blackmail, political agendas, testing hacking skills, or rivalry among cloud providers, as shown in Figure 3 [35]. People are not naturally inclined to become attackers; instead, they are driven by specific motivations. These motivations can be grouped into four main categories. Some attackers are motivated by financial gain, utilizing advanced skills to exploit systems while remaining undetected. Others, driven by curiosity and a desire to test their expertise, target systems to identify vulnerabilities and evaluate security measures. A third group acts out of frustration or revenge, often with limited skills, seeking to settle personal grievances. Lastly, highly skilled individuals, frequently associated with military or terrorist organizations, engage in cyber warfare to advance the interests of their country or group [36].

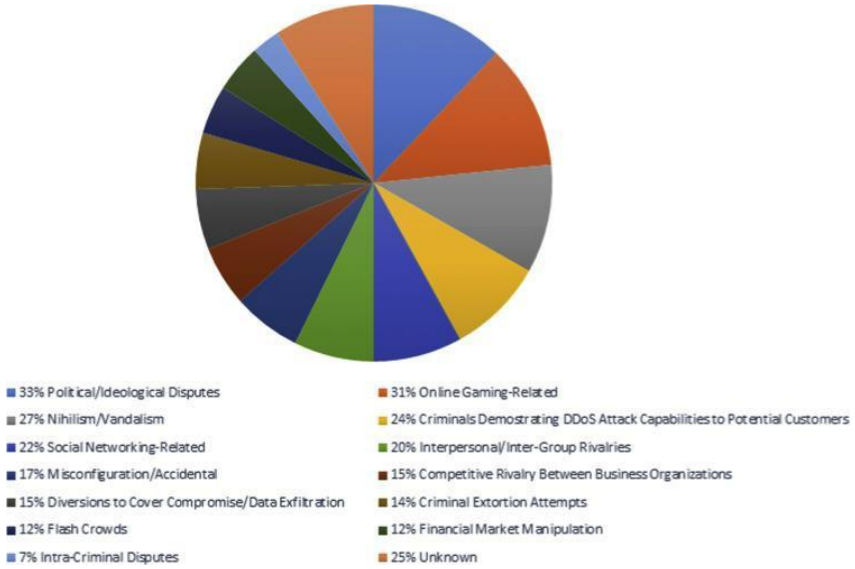

Figure 3. Motives behind DDoS attacks [35]

The concept of the "Internet of Things" (IoT) was introduced in 1999 by Kevin Ashton, a British technology innovator. He used the term to explain how objects in the real world could be linked to the Internet using sensors. Ashton specifically highlighted how connecting RFID tags, commonly used in supply chains, to the Internet could help monitor and manage goods automatically, without relying on human input [37]. Pretz describes the Internet of Things (IoT) as a network where devices, or "things," are linked wirelessly using smart sensors. These devices can communicate and operate independently without requiring direct human input [38]. The Internet of Things (IoT) is expanding the reach of the Internet by connecting everyday objects through embedded systems, enabling them to interact with people and with one another. This creates a vast and decentralized network of devices. Over the past few years, IoT has drawn significant interest from researchers and professionals worldwide [39]. Contemporary Internet of Things (IoT) systems require elevated service standards and robust quality of service, prompting the widespread adoption of machine learning (ML) and artificial intelligence (AI) techniques throughout the entire data lifecycle—from initial data acquisition by IoT sensors to its final application by end-users. This fusion of innovative technologies within IoT frameworks has given rise to a new concept known as Intelligent IoT (IIoT), which has significantly advanced the development of applications in areas such as digital healthcare, automated transport systems, and next-generation industrial environments [40].

2. METHOD

To access the terminal ecosystem, it is essential first to identify network endpoint devices, commonly referred to as terminals. These include computer terminals such as desktops, personal computers like laptops, smartphones, tablets, thin clients, point-of-sale terminals, ATMs, ticketing machines, interactive kiosks, data center terminals (such as servers and storage), IP phones, and various other bring-your-own-device (BYOD) gadgets, including smartwatches. Terminals can be categorized based on their capability—intelligent, thoughtful, or dumb terminals—and their memory capacity, as either light or heavy terminals. The combination of capability and memory capacity determines the potential security threats posed by a terminal and influences the type of security protocols or encryption methods it can handle. Assessing current terminal security involves implementing measures such as endpoint protection using antivirus and anti-malware software, access control mechanisms to limit resource access by identifying terminals through IP or MAC addresses, multi-factor authentication (MFA) for added security layers, and the use of virtual private networks (VPNs) for encrypted connections. Other essential practices include applying regular security patches and updates, deploying intrusion detection and prevention systems (IDPS), managing mobile devices through Mobile Device Management (MDM), preventing unauthorized data transfer with data loss prevention (DLP) tools, and using behavioral analytics to detect unusual activities. Exploring the latest security solutions for modern networks involves combining strong access controls, secure software development practices, timely security updates, real-time threat intelligence systems, robust encryption for data protection, and comprehensive security awareness training for employees. Organizations should collaborate with peers and regulatory bodies, adhere to compliance requirements, and conduct ongoing security assessments and audits to stay ahead of evolving

threats. Maintaining security is a continuing process that requires constant vigilance, regular updates, and proactive measures to ensure the protection of terminals and networks.

The gap analysis identifies several areas that require improvement to enhance terminal security, the focus of this paper. First, terminals need to be categorized to ensure security techniques and policies are effectively designed and implemented to fit their specific requirements. Second, supply chain security presents a challenge, as terminal devices often depend on components or software from third-party vendors, making it essential to secure the entire supply chain to prevent potential attacks through compromised elements. Lastly, servers and storage devices, which serve as endpoints within data centers, require special attention to enhance the overall security of critical data center components. Addressing these gaps will contribute significantly to improving terminal security.

The methodology focuses on developing a comprehensive security solution for terminals to address previously identified gaps. This involves ensuring the core principles of cybersecurity: confidentiality, integrity, and availability. Confidentiality ensures that sensitive information is accessible only to authorized individuals, safeguarding it from unauthorized third parties. Integrity guarantees that data remains unaltered both during and after submission, while availability ensures that systems, networks, and applications are always operational and accessible when needed. Achieving these goals requires categorizing terminals into three categories: witty, intelligent, and dumb, based on their processing capabilities, storage, and threat levels. Smart terminals require moderate security measures due to their intermediate capabilities. Intelligent terminals demand robust encryption and security protocols because of their advanced processing abilities. Dumb terminals pose minimal threats given their lack of processing power. To secure communication between terminals and intranet components, an L2TP and IPSec tunneling VPN is implemented. This model leverages double tunneling for enhanced security. The L2TP tunnel planning is outlined in Table 1, which specifies the IP addresses, security zones, and configurations required for a seamless VPN setup. Similarly, the IPSec tunnel planning, detailed in Table 2, highlights the use of pre-shared keys, peer authentication, and secure configurations across firewalls and servers. The security network diagram illustrating this communication model is shown in Figure 4.

Table 1. L2TP VPN tunnel planning sheet

ITEM	DATA	DESCRIPTION
FW1	Int GE0/0/2 IP address: 20.1.1.1/24 Security zone: Untrust	
Terminal	IP address:10.1.1.10/24 Gateway address: 20.1.1.1	The terminal should have an L2TP dial-up client installed
Servers	server1 IP address: 10.1.1.10/24 server2 Ip address: 10.1.1.20/24 Gateway IP address: 10.1.1.1	Servers simulate the Intranet Server
L2TP Planning	Virtual interface: virtual-temptate0 virtual interface address: 192.168.1.1/24 virtual interface zone: Untrust Remote tunnel name: Client Local tunnel name: Client Tunnel authentication password: Password123 Remote address: 192.168.1.10 User name: User1 Password: Test@123	This is the configuration on the Egress firewall
L2TP Planning (Dialup user)	User name: User1 Password: Test@123 Tunnel name: Client Authentication mode: CHAP Tunnel password: Password123	This is the configuration on the terminal (on L2TP dialup client)

Table 2. IPSec VPN tunnel planning sheet

ITEM	DATA	DESCRIPTION
FW1	Int GE0/0/2 IP address: 10.1.1.1/24 Security zone: untrust	config on the Egress firewall (FW1)
	Int GE0/0/1 IP address: 40.1.1.1/24 Security zone: untrust	
	IPSec Planning	The scenario: Site-to-site peer address: 40.1.1.2 Authentication mode: pre-shared key pre-shared key: Test123! Local ID: 40.1.1.1 Peer ID: 40.1.1.2
FW1	Int GE0/0/1 IP address: 10.1.2.2/24 Security zone: trust	config on the internal firewall (FW2)
	Int GE0/0/2 IP address: 40.1.1.2/24 Security zone: untrust	
	IPSec Planning	The scenario: Site-to-site peer address: 40.1.1.1 Authentication mode: pre-shared key Pre-shared key: Test123! Local ID: 40.1.1.2 Peer ID: 40.1.1.1
Servers	server1 IP address: 10.1.1.10/24 server2 Ip address: 10.1.1.20/24 Gateway IP address: 10.1.1.1	Servers simulate the Intranet Server

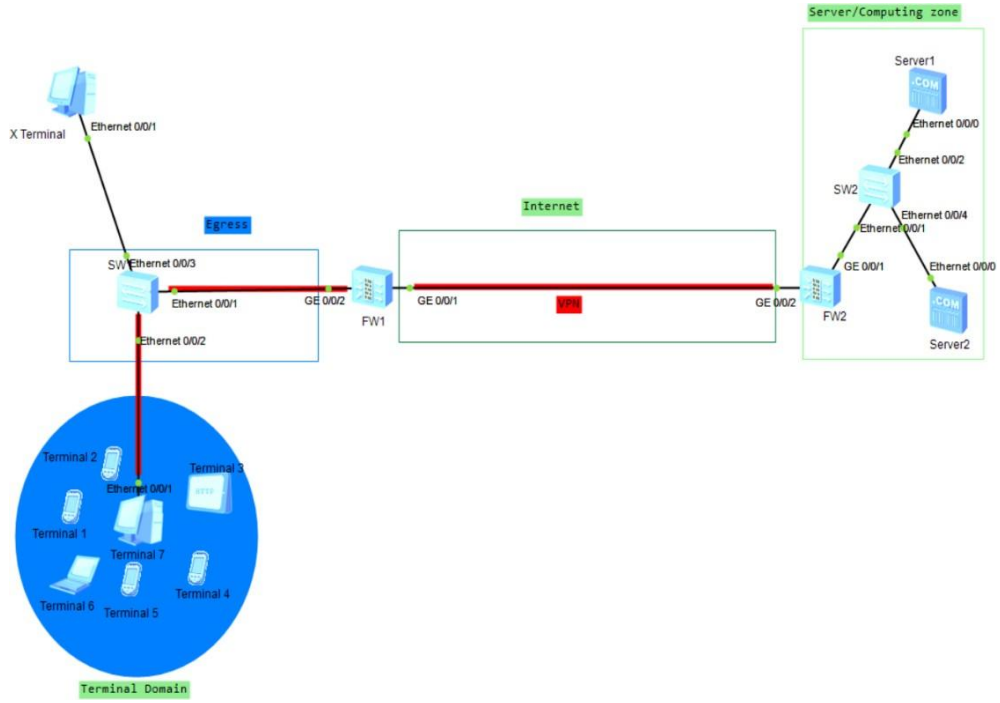

Figure 4. L2TP and IPSec tunnel VPN

Addressing supply chain security involves assessing vendors, ensuring transparency, and verifying the integrity of hardware and software components. Additional measures include mandating signed firmware updates, auditing supply chains, and implementing zero-trust architectures. Secure manufacturing processes and regular security testing help mitigate risks associated with hardware vulnerabilities. Moreover, employee training ensures those involved in the supply chain understand and adhere to security protocols, further

strengthening the system. For servers and storage devices, which are critical endpoints in a data center, disaster recovery and backup (DR&B) solutions are indispensable. Traditional DR&B setups involve maintaining primary and backup data centers either on the same premises or in geographically distinct locations. Figure 5 shows the architecture for a same-location setup, while Figure 6 depicts the layout for geographically separated centers, ensuring resilience against physical disasters.

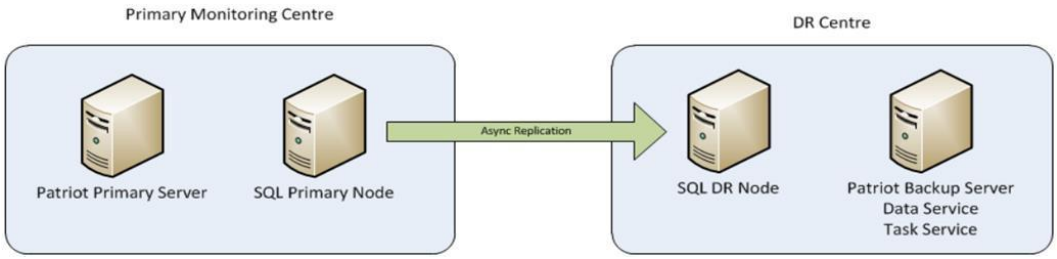

Figure 5. Primary and backup DR for the same location setting

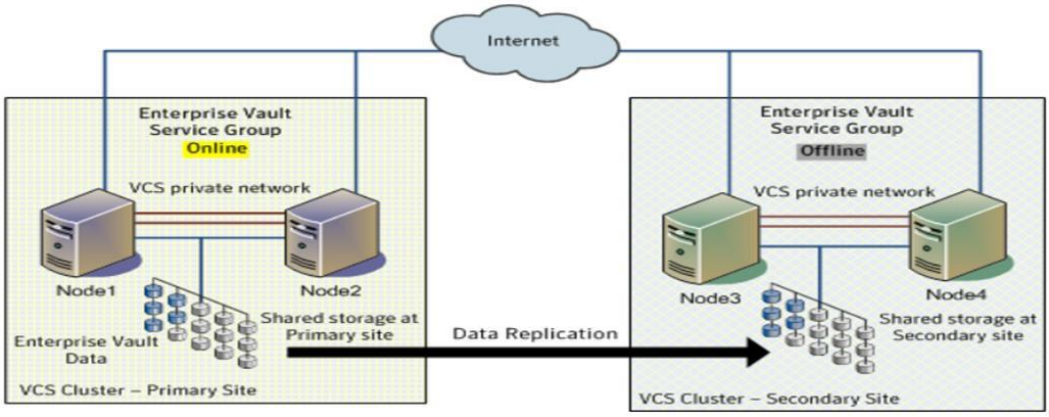

Figure 6. DR&B DC for different location settings

Advanced DR&B solutions introduce an isolation zone between the primary and secondary data centers, ensuring a seamless transition in the event of a disaster. This preventive layer enhances security by containing threats before they reach critical backups, as illustrated in Figure 7. Lastly, implementing security policies and procedures is crucial for protecting network terminals and ensuring organizational compliance. These include acceptable terminal use guidelines, user access management protocols, physical security measures, and password policies. Training employees on cybersecurity awareness and promoting vigilance against potential threats play a critical role. Regular audits, data backup, and a structured approach to incident response ensure the secure and efficient use of network terminals while mitigating risks. This methodology combines technical solutions, structured planning, and organizational policies to build a safe and resilient system for managing terminals and associated components.

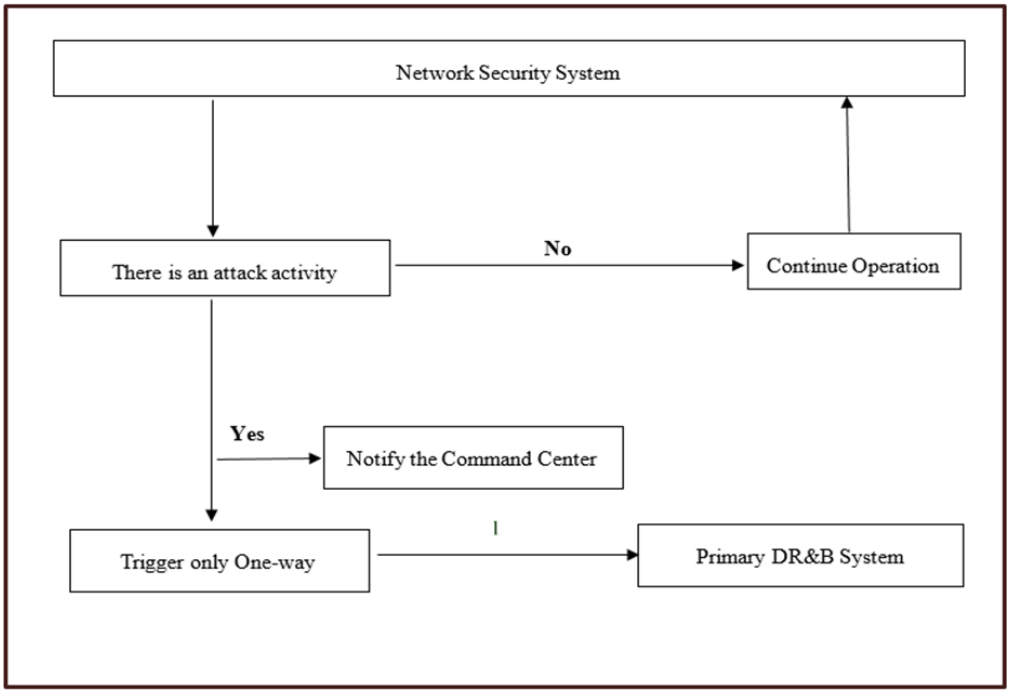

Figure 7. Advance DR&B security work flow diagram

```
Tunnel Interface Information
---------------------------
Tunnel ID   Type      Source IP      Destination IP  Status
-----------------------------------------------------------
1          L2TP     192.168.1.2    192.168.1.1     Up
2          L2TP     192.168.1.1    192.168.1.2     Up
101         IPsec      40.1.1.2       40.1.1.1       Established
102         IPsec      40.1.1.1       40.1.1.2       Established
```

Figure 8. VPN tunnels established on FW1

3. RESULTS AND DISCUSSION

The results of this study focus on addressing terminal security in contemporary enterprise networks, highlighting the need for comprehensive solutions tailored to current challenges. Terminals connected to enterprise networks vary in type, including lightweight and heavyweight categories, and may be classified as clever, intelligent, or dumb terminals. The security measures currently applied to these terminals include access control, multi-factor authentication, intrusion detection and prevention systems, and VPNs. These measures often work independently or in combination to secure terminals against potential threats, as outlined earlier in the study. Exploration into the latest security solutions reveals the necessity of focusing not only on technological safeguards but also on effective security policies. Endpoint security plays a pivotal role in protecting enterprise networks by reducing risks from malicious actors while ensuring the confidentiality, integrity, and availability of critical data. This study identifies gaps in current terminal security measures and proposes strategies to address them. The identified gaps include the categorization of terminals, security vulnerabilities in the supply chain, and specific challenges in protecting server and storage devices within data centers. To mitigate these issues, innovative solutions, such as isolation zones for data centers and targeted approaches to terminal categorization, were developed.

While the technical aspects of the proposed system have been thoroughly examined, it is equally essential to contextualize its effectiveness in relation to real-world security threats. In comparison to common vulnerabilities faced by enterprise networks—such as sophisticated phishing attacks, insider threats, and zero-day exploits—the proposed system demonstrates a more adaptive and layered defense structure. This comparative analysis highlights that although the study addresses known technical gaps, its real strength lies in proposing scalable measures that mirror the complexity of threats in practical settings. Consequently, the

findings contribute not only to theoretical advancements but also offer actionable insights for enhancing terminal security resilience in dynamic, real-world environments.

One of the key solutions presented involves a secure VPN tunnel architecture to enhance terminal communication with the network. This model utilizes a double-tunnel system that combines Layer 2 Tunneling Protocol (L2TP) and IP Security (IPsec) tunnels. The L2TP tunnel establishes a connection between the terminal and the egress firewall, while the IPsec tunnel secures communication between the egress firewall and the data center firewall. This dual-tunnel approach significantly improves the security of data exchanges between terminals and internal servers or storage devices. The implementation of this model is demonstrated through a network topology (Figure 4) and the results of connectivity tests, as shown in Figures 8 - Figure 13.

```
[FW1]ping 40.1.1.2
22:45:44  2023/11/18
  PING 40.1.1.2: 56  data bytes, press CTRL_C to break
    Reply from 40.1.1.2: bytes=56 Sequence=1 ttl=255 time=310 ms
    Reply from 40.1.1.2: bytes=56 Sequence=2 ttl=255 time=250 ms
    Reply from 40.1.1.2: bytes=56 Sequence=3 ttl=255 time=230 ms
    Reply from 40.1.1.2: bytes=56 Sequence=4 ttl=255 time=720 ms
    Reply from 40.1.1.2: bytes=56 Sequence=5 ttl=255 time=110 ms

  --- 40.1.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 110/324/720 ms
```

Figure 9. Connectivity test result (FW1 to FW2)

```
PC>ping 10.1.1.10

Ping 10.1.1.10: 32 data bytes, Press Ctrl_C to break
From 10.1.1.10: bytes=32 seq=1 ttl=253 time=156 ms
From 10.1.1.10: bytes=32 seq=2 ttl=253 time=110 ms
From 10.1.1.10: bytes=32 seq=3 ttl=253 time=47 ms
From 10.1.1.10: bytes=32 seq=4 ttl=253 time=46 ms
From 10.1.1.10: bytes=32 seq=5 ttl=253 time=79 ms

--- 10.1.1.10 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 46/87/156 ms
```

Figure 10. Connectivity test result (Terminal7 to Server1)

```
PC>ping 10.1.1.20

Ping 10.1.1.20: 32 data bytes, Press Ctrl_C to break
From 10.1.1.20: bytes=32 seq=1 ttl=253 time=109 ms
From 10.1.1.20: bytes=32 seq=2 ttl=253 time=156 ms
From 10.1.1.20: bytes=32 seq=3 ttl=253 time=156 ms
From 10.1.1.20: bytes=32 seq=4 ttl=253 time=62 ms
From 10.1.1.20: bytes=32 seq=5 ttl=253 time=109 ms

--- 10.1.1.20 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 62/118/156 ms
```

Figure 11. Connectivity test result (Terminal7 to Server2

```
PC>ping 10.1.1.10

Ping 10.1.1.10: 32 data bytes, Press Ctrl_C to break
Request timeout!
Request timeout!
Request timeout!
Request timeout!
Request timeout!

--- 10.1.1.10 ping statistics ---
  5 packet(s) transmitted
  0 packet(s) received
  100.00% packet loss
```

Figure 12. Connectivity test result (X terminal to Server1)

```
PC>ping 10.1.1.20

Ping 10.1.1.20: 32 data bytes, Press Ctrl_C to break
Request timeout!
Request timeout!
Request timeout!
Request timeout!
Request timeout!

--- 10.1.1.20 ping statistics ---
  5 packet(s) transmitted
  0 packet(s) received
  100.00% packet loss
```

Figure 13. Connectivity test result (X terminal to Server2)

In addition to VPN solutions, the study introduces an advanced Disaster Recovery and Backup (DR&B) solution with an isolation zone to protect critical data center components from ransomware and other malicious attacks. This approach incorporates a monitoring system that detects attack activities in the primary data center, triggers a one-way data flow to the isolation zone, and ensures continuous production capability. Meanwhile, the DR site serves as the backup location. The logical workflow of this DR&B solution is depicted in Figure 14. The proposed system is designed to safeguard the network even during active attacks, leveraging customized network security software tailored to counter ransomware and similar threats.

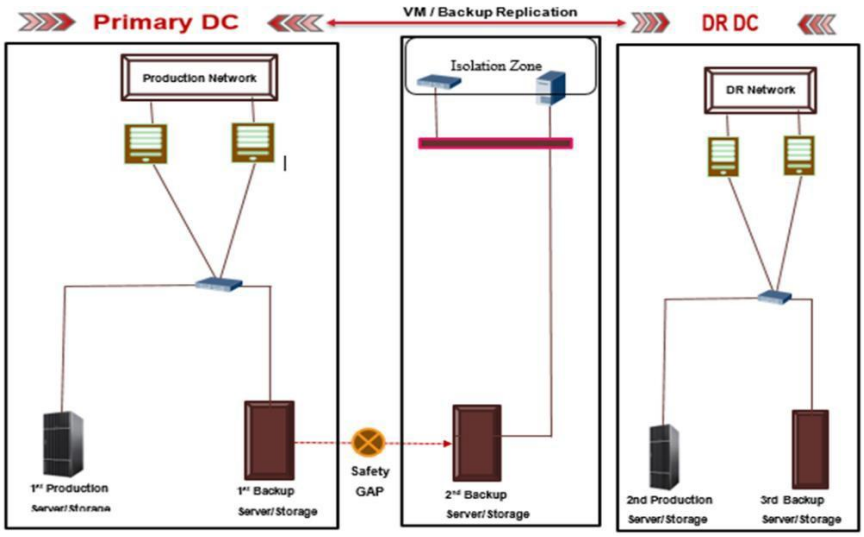

Figure 14. Advanced DR&B solution with the Isolation zone

The effectiveness of the developed solutions is assessed by comparing them with current enterprise security measures. In terms of vulnerability, the dual-tunnel VPN model enhances terminal security by securing communication channels while addressing supply chain vulnerabilities and improving DR&B protection mechanisms. The proposed solutions are also shown to be effective, provided they are fully implemented and aligned with existing standards and practices. Furthermore, the feasibility of these measures is underscored by their foundation in established protocols, offering an improved approach to implementing security technologies in enterprise settings.

4. CONCLUSION AND LIMITATION

This report presents an enhanced framework for designing an enterprise network terminal security solution, with a core focus on improving endpoint security within existing enterprise network infrastructures. The proposed framework leverages a multi-layered security strategy that integrates advanced technological tools with strategic organizational policies, including employee training, proactive threat intelligence gathering, and continuous security monitoring. By adopting these recommended measures, enterprises can establish a secure and compliant environment that ensures the appropriate and safe use of network terminals. Regular security training sessions, awareness campaigns, and routine policy evaluations are essential in cultivating a security-conscious workforce and mitigating risks associated with unauthorized data access or system misuse. Nonetheless, it is acknowledged that security implementations must be context-specific; the effectiveness of the proposed measures depends on terminal types (e.g., smart, intelligent, or dumb terminals), the nature of enterprise operations, and industry-specific regulatory requirements. As such, organizations should assess their unique risk landscape and consult cybersecurity professionals to develop tailored, responsive security postures. Despite its contributions, this study is subject to certain limitations. Due to resource constraints, the advanced Disaster Recovery and Business Continuity (DR&B) component of the framework could not be fully simulated, nor was the framework deployed in a real-world enterprise environment. These factors limit the ability to draw empirical conclusions about its real-life efficacy. Moreover, practical implementation of the framework in large-scale or heterogeneous enterprise environments may present challenges such as compatibility with legacy systems, high initial deployment costs, the need for continuous system updates, and managing user resistance to new security protocols. Scalability concerns also arise when attempting to extend the framework across global networks with varying regulatory landscapes and varying levels of infrastructure maturity. Ensuring consistent policy enforcement and real-time threat detection across all terminal types becomes increasingly complex as network size and diversity grow. Nonetheless, the framework offers valuable insights by categorizing network terminals based on their capabilities and memory capacity, thereby aiding in informed decision-making, such as selecting suitable encryption standards. It also highlights potential supply chain vulnerabilities and presents mitigation strategies. Furthermore, the tailored protection mechanisms proposed for securing data center storage and servers—particularly against ransomware and similar threats—are crucial in today's evolving threat landscape. These contributions are expected to guide researchers, cybersecurity analysts, network engineers, and IT security specialists in the development and management of robust, scalable security solutions across enterprise networks. Future work should prioritize the real-world deployment of the proposed DR&B solution and conduct extensive testing across varied enterprise scenarios to validate the framework's effectiveness, adaptability, and scalability under operational conditions.

REFERENCES

[1] Dastres, R., & Soor, M., "A Review in Recent Development of Network Threats and Security Measures", *World Academy of Science, Engineering, and Technology International Journal of Computer and Information Engineering*, vol.15, no.1, 2021.

[2] Hussein, M. A., & Hamza, E. K., "Secure Mechanism Applied to Big Data for IoT by Using Security Event and Information Management System (SIEM)", *International Journal of Intelligent Engineering & Systems,* vol.15, no. 6, 2022. https://doi.org/10.22266/ijies2022.1231.59

[3] Sarkar, S., Choudhary, G., Shandilya, S. K., Hussain, A., & Kim, H., "Security of Zero Trust Networks in Cloud Computing: A Comparative Review", *Sustainability,* vol. 14, no. 18, 11213, 2022. https://doi.org/10.3390/su141811213.

[4] Alzoubi, Y. I., Al-Ahmad, A., Kahtan, H., & Jaradat, A., "Internet of Things and Blockchain Integration: Security, Privacy, Technical, and Design Challenges", *Future Internet,* vol. 14, no. 7, 216, 2022. https://doi.org/10.3390/fi14070216.

[5] Rahman, M. M., Faraji, M. R., Islam, M. M., Khatun, M., Uddin, S., & Hasan, M. H, "Gravitating Towards Information Society for Information Security in Information Systems: A Systematic PRISMA Based Review", *Pakistan Journal of Life and Social Sciences (PJLSS),* vol 22, no. 1, 2024. https://doi.org/10.57239/PJLSS-2024-22.1.0089.

[6] Lali, K., & Chakor, A., "Improving the Security and Reliability of a Quality Marketing Information System: A Priority Prerequisite for Good Strategic Management of a Successful Entrepreneurial Project", *Data and Metadata,* vol. 2, pp. 40-40, 2023. https://doi.org/10.56294/dm202340.

[7] Farid, G., Warraich, N. F., & Iftikhar, S., "Digital Information Security Management Policy in Academic Libraries: A Systematic Review", *Journal of Information Science*, 01655515231160026, 2023. https://doi.org/10.1177/01655515231160026.

[8] Alshurideh, M., Alquqa, E., Alzoubi, H., Kurdi, B., & Hamadneh, S., "The Effect of Information Security on e- Supply Chain in the UAE Logistics and Distribution Industry", *Uncertain Supply Chain Management,* vol. 11, no. 1, pp.145-152, 2023. https://doi.org/10.5267/j.uscm.2022.11.001

[9] Mou, J., Cohen, J. F., Bhattacherjee, A., & Kim, J., "A Test of Protection Motivation Theory in the Information Security Literature: A Meta-Analytic Structural Equation Modeling Approach", *Journal of the Association for Information Systems,* vol. 23, no. 1, pp. 196-236, 2022. https://doi.org/10.17705/1jais.00723

[10] Edo, O. C., Tenebe, T., Etu, E. E., Ayuwu, A., Emakhu, J., & Adebiyi, S., "Zero Trust Architecture: Trend and Impacton Information Security", *International Journal of Emerging Technology and Advanced Engineering, vol. 12*, no. 7, 140, 2022. https://doi.org/10.46338/ijetae0722_15.

[11] Sun, L., & Gao, D., "Security Attitude Prediction Model of Secret-Related Computer Information System Based on Distributed Parallel Computing Programming", *Mathematical Problems in Engineering,* vol. 1, 3141568, 2022. https://doi.org/10.1155/2022/3141568.

[12] Rahman, M. R., Hezaveh, R. M., & Williams, L., "What are the Attackers doing now? Automating Cyberthreat Intelligence Extraction from Text on Pace with the Changing Threat Landscape: A survey", *ACM Computing Surveys*, vol. 55, no. 12, pp. 1-36, 2023. https://doi.org/10.1145/3571726.

[13] Apruzzese, G., Anderson, H. S., Dambra, S., Freeman, D., Pierazzi, F., & Roundy, K., "Real Attackers don't Compute Gradients: Bridging the Gap Between Adversarial ml Research and Practice", *IEEE Conference on Secure and Trustworthy Machine Learning (SaTML),* pp. 339-364, 2023. https://doi.org/10.1109/SaTML54575.2023.00031.

[14] Priya, V. D., & Chakkaravarthy, S. S., "Containerized Cloud-Based Honeypot Deception for Tracking Attackers. *Scientific Reports,* vol. 13, no. 1, 1437, 2023. https://doi.org/10.1038/s41598-023-28613-0.

[15] Saigushev, N. Y., Mikhailova, U. V., Vedeneeva, O. A., & Tsaran, A. A., "Information Systems at Enterprise. Design of Secure Network of Enterprise", *Journal of Physics: Conference Series*, vol. 1015, no. 4, p. 042054, 2018. https://doi.org/10.1088/1742-6596/1015/4/042054.

[16] Saigushev, N. Y., Mikhailova, U. V., Vedeneeva, O. A., & Tsaran, A. A., "Information Systems at Enterprise. Design of Secure Network of Enterprise", *Journal of Physics: Conference Series*, vol. 1015, no. 4, p. 042054, 2018. https://doi.org/10.1088/1742-6596/1015/4/042054

[17] Tarkaa, N. S., Iannah, P. I., & Iber, I. T., "Design and Simulation of Local Area Network Using Cisco Packet Tracer", *The International Journal of Engineering and Science,* vol. 6, no. 10, 63-77, 2017.

[18] Michael E. Whitman, Herbert J. l., Principles of Information Security. Latest edition 2019

[19] Jingyao, S., Chandel, S., Yunnan, Y., Jingji, Z., & Zhipeng, Z.," Securing a Network: How Effective Using Firewalls and VPNs are?", *Advances in Information and Communication: Proceedings of the 2019 Future of Information and Communication Conference (FICC)*, vol. 2, pp. 1050-1068, 2019. https://doi.org/10.1007/978-3-030-12385-7_71.

[20] Ahmadi, S., "Next Generation AI-Based Firewalls: A Comparative Study", *International Journal of Computer (IJC),* vol. 49, no. 1, pp. 245-262, 2023.

[21] Mukkamala, P. P., & Rajendran, S., "A Survey on the Different Firewall Technologies", *International Journal of Engineering Applied Sciences and Technology,* vol. 5, no. 1, pp. 363-365, 2020. https://doi.org/10.33564/IJEAST.2020.v05i01.059.

[22] Anwar, R. W., Abdullah, T., & Pastore, F., "Firewall Best Practices for Securing Smart Healthcare Environment: A Review", *Applied Sciences*, vol.11, no. 19, 9183, 2021. https://doi.org/10.3390/app11199183.

[23] Ozkan-Okay, M., Samet, R., Aslan, Ö., & Gupta, D., "A Comprehensive Systematic Literature Review on Intrusion Detection Systems", *IEEE Access,* vol. 9, 157727-157760, 2021. https://doi.org/10.1109/ACCESS.2021.3129336.

[24] Heidari, A., & Jabraeil Jamali, M. A., "Internet of Things Intrusion Detection Systems: a Comprehensive Review and Future Directions", *Cluster Computing,* vol. 26, no. 6, 3753-3780, 2023. https://doi.org/10.1007/s10586-022-03776-z.

[25] Lansky, J., Ali, S., Mohammadi, M., Majeed, M. K., Karim, S. H. T., Rashidi, S., & Rahmani, A. M., "Deep Learning-Based Intrusion Detection Systems: A Systematic Review", *IEEE Access,* vol. 9, 101574-101599, 2021. https://doi.org/10.1109/ACCESS.2021.3097247

[26] Khan, K., Mehmood, A., Khan, S., Khan, M. A., Iqbal, Z., & Mashwani, W. K., "A Survey on Intrusion Detection and Prevention in Wireless Ad-Hoc Networks", *Journal of Systems Architecture,* vol.105, 101701, 2020. https://doi.org/10.1016/j.sysarc.2019.101701.

[27] Jayalaxmi, P. L. S., Saha, R., Kumar, G., Conti, M., & Kim, T. H., "Machine and Deep Learning Solutions for Intrusion Detection and Prevention in IoTs: A survey", *IEEE Access,* vol. 10, 121173-121192. https://doi.org/10.1109/ACCESS.2022.3220622.

[28] Girdler, T., & Vassilakis, V. G., "Implementing an Intrusion Detection and Prevention System using Software-Defined Networking: Defending against ARP Spoofing Attacks and Blacklisted MAC Addresses", *Computers & Electrical Engineering,* vol. 90, 106990. https://doi.org/10.1016/j.compeleceng.2021.106990.

[29] Goswami, A., Patel, R., Mavani, C., & Mistry, H. K., "Intrusion Detection and Prevention for Cloud Security", *International Journal on Recent and Innovation Trends in Computing and Communication,* vol. 12, no. 2, pp. 556-63.

[30] Mebawondu, J. O., Alowolodu, O. D., Mebawondu, J. O., & Adetunmbi, A. O., "Network Intrusion Detection System Using Supervised Learning Paradigm", *Scientific African,* vol. 9, e00497. https://doi.org/10.1016/j.sciaf.2020.e00497.

[31] Gentile, A. F., Fazio, P., & Miceli, G., "A Survey on the Implementation and Management of Secure Virtual Private Networks (VPNs) and Virtual LANs (VLANs) in Static and Mobile Scenarios.", *Telecom,* vol. 2, no. 4, pp. 430-445, 2021. https://doi.org/10.3390/telecom2040025

[32] Nagy, Z., & Wali, M. K., "Virtual Private Network Impacts on the Computer Network Performance with Different Traffic Generators", *IOP Conference Series: Materials Science and Engineering,* vol. 881, no. 1, p. 012126). IOP Publishing, 2020. https://doi.org/10.1088/1757-899X/881/1/012126.

[33] Singh, A., & Gupta, B. B., "Distributed denial-of-service (DDoS) Attacks and Defense Mechanisms in Various Web-Enabled Computing Platforms: Issues, Challenges, and Future Research Directions", *International Journal on Semantic Web and Information Systems* (IJSWIS), vol. 18, no. 1, pp. 1-43, 2022. https://doi.org/10.4018/IJSWIS.297143.

[34] Virupakshar, K. B., Asundi, M., Channal, K., Shettar, P., Patil, S., & Narayan, D. G., "Distributed Denial of Service (Ddos) Attacks Detection System for Openstack-Based Private Cloud", *Procedia Computer Science, 167*, 2297- 2307, 2020. https://doi.org/10.1016/j.procs.2020.03.282.

[35] Osanaiye, O., Choo, K. K. R., & Dlodlo, M., "Distributed Denial of Service (DDoS) Resilience in Cloud: Review and Conceptual Cloud DDoS Mitigation Framework", *Journal of Network and Computer Applications,* vol. 67, pp. 147-165, 2016. https://doi.org/10.1016/j.jnca.2016.01.001.

[36] Tripathi, S., Gupta, B., Almomani, A., Mishra, A., & Veluru, S., "Hadoop Based Defense Solution to Handle Distributed Denial of Service (ddos) Attacks", *Journal of Information Security*, vol. 4, no. 3, 2013. https://doi.org/10.4236/jis.2013.43018.

[37] Rose, K., Eldridge, S., and Chapin, L., "The internet of things: An overview", *The internet society (ISOC), vol. 80*, no. 15, pp. 1-53, 2015.

[38] Li, S., Xu, L. D., & Zhao, S., "The internet of things: a survey", *Information systems frontiers*, vol. 17, pp. 243-259. 2015. https://doi.org/10.1007/s10796-014-9492-7.

[39] Xia, F., Yang, L. T., Wang, L., & Vinel, "A. Internet of Things", *International journal of communication systems,* vol. 25, no. 9, 1101, 2012. https://doi.org/10.1002/dac.2417

[40] O. Aouedi et al., "A Survey on Intelligent Internet of Things: Applications, Security, Privacy, and Future Directions," *IEEE Communications Surveys & Tutorials*, vol. 27, no. 2, pp. 1238-1292, 2025. https://doi.org/10.1109/COMST.2024.3430368.

BIOGRAPHIES OF AUTHORS

Muhammad Idris Abubakar is a Regional Service Solution Sales Manager in the Southern Africa Service & Software Marketing and Solution Sales Department at Huawei Technologies. With extensive experience in service solution sales, service management, and solution design, he has played a pivotal role in so many projects across multiple countries in Southern Africa. He is an emerging Mobile Money Solution Architect and a network security research enthusiast, with a keen interest in digital financial services and cybersecurity advancement.

Ajayi Ore-Ofe is a lecturer at the Department of Computer Engineering, Ahmadu Bello University, Zaria, Nigeria. He received his MSc and Ph.D from Computer Engineering in Control Engineering, in 2017 and 2022 respectively. He received his MSc and Ph.D from the department of Computer Engineering in Ahmadu Bello University, Zaria, Nigeria. He is mainly research in control engineering. He can be contacted at email ajayi.oreofe17@gmail.com

Abubakar Umar is a lecturer in the Department of Computer Engineering at Ahmadu Bello University, Zaria, Nigeria. He earned his BEng Degree from Electrical Engineering Department Ahmadu Bello University, Zaria, Nigeria, in 2011, MSc, and Ph.D. degrees from Computer Engineering Department, Ahmadu Bello University, Zaria, Nigeria, in 2017 and 2024. He specializes in various aspects of computer engineering. His primary research focus is in Control Engineering, where he explores the development and optimization of control systems for different applications. He is dedicated to advancing his research and contributing to academic knowledge in this field. He can be contacted via email at abuumar@abu.edu.ng, abubakaru061010@gmail.com

Ibrahim Ibrahim is a student of Computer Engineering at Ahmadu Bello University, Zaria, Nigeria. He has a keen interest in data science and has been actively pursuing knowledge in this field through various platforms. He has completed several courses on DataCamp and Coursera to strengthen his skills in this field. He is actively taking more courses to expand his knowledge in data analysis and machine learning, aiming to apply these skills in practical and research- based projects. He can be contacted via email at eebrahym04@gmail.com

Lawal Abdulwahab Olugbenga is a student of Computer Engineering at Ahmadu Bello University, Zaria, Nigeria. He has a strong interest in system architecture and cloud computing. He is focused on developing his expertise in these areas. His academic journey is centered on understanding the design and structure of computing systems, with a goal to apply this knowledge in both practical and research settings. He can be reached via email at abdulwahabolugbenga@gmail.com

Ajikanle Abdulbasit Abiola is a dedicated student of Computer Engineering at Ahmadu Bello University, Zaria, Nigeria. He has a strong passion for network solutions, with a focus on designing and optimizing systems to improve connectivity and communication. His academic journey is driven by a desire to find practical solutions to networking challenges, including network security, efficiency, and scalability. Through his studies, he aims to develop skills that can be applied to real-world problems in the field of computer networks. He is committed to continuous learning and growth in this area. He can be reached via email at aajikanle@gmail.com