Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

Zero Trust and SD-WAN: Securing Enterprise and IoT Networks at Scale

Dharnisha Narasappa
Sr. Network Architect, Versa Networks,USA
dharanishnarasappa@gmail.com

ARTICLE INFO

Received: 02 Sept 2024

Revised: 19 Oct 2024

Accepted: 28 Oct 2024

ABSTRACT

With increase in the complexity and scale of enterprise networks and the IoT ecosystems, securing them has become a major concern of organizations. Traditional models of security, which are based on perimeter security approaches are losing their relevance in coping with the dynamic and distributed nature of current networks. This paper discusses how Zero Trust security model can be incorporated into Software-Defined Wide Area Network (SD-WAN) technology to provide end-to-end and comprehensive security to enterprise and IoT networks. Zero Trust relies on the mantra of never trust, always verify in the provision of continuous authentication and stringent access controls irrespective of place and device. In the meantime, SD-WAN makes it possible to link WANs through efficient and secure traffic across the network together with setting the traffic routes and optimizing performance. Combined, these technologies create a strong deterrence against advanced cyber threats, allowing data integrity, confidentiality and availability. The paper also explains the distinguishing features and advantages of each framework and points out the complementary strengths of the two entities and real-world applications that point out how organizations can extent their own security positions. And further look at how to scale out Zero Trust and SD-WAN in the most efficient focus on mitigation of threats and seamless security controls that integrate across distributed and hybrid networks.

Keywords: Zero Trust, SD-WAN, Network Security, IoT Security, Cyber Threat Mitigation.

1. Introduction

In this new era of ever-more intelligent cyber threats, network security has become a major issue facing organizations, and analyses of security threats are especially prominent as organizations move to larger networks to facilitate more complex and dynamic technological environments. The adoption of cloud computing, hybrid systems, and sharp increases in the volume of Internet of Things (IoT) devices have created new security issues. The existing security approaches that are largely based on traditional security models that rely on perimeter security are no longer capable of providing adequate security of enterprise networks which are increasingly becoming decentralized and fluid. The perimeter-based model is essentially flawed because of the distributed nature of workforces, the use of devices connecting out in other environments that sit outside the corporate perimeter. This brings maturity in the business which is forced to embrace more dynamic, scale able and comprehensive security strategy able to tackle these novel threats.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

Two solutions that prove to be most effective to these challenges are Zero Trust (ZT) and Software-Defined Wide Area Network (SD-WAN) frameworks. Zero Trust uses the more pessimistic perspective of, never trust, always verify, i.e., regular authentication and verification of users, devices, and applications seeking access to network resources, regardless of origin. Relining the risk of (1) hacking, (2) counterintelligence, and (3) non-malicious risks to their data through unreliable insiders is to mitigate the risk to a significant degree by treating all the traffic in the network, internal and external, as untrusted. Zero Trust with access policies based on fine-grained rules that are continually modified by the security focus of the users and devices.

In the meantime, the SD-WAN technology provides a more efficient and safe method to oversee broad-area networks. Conventional WAN architectures tend to use MPLS paths which are costly and not flexible. Unlike SD-WAN, it relies on software based packet optimization and routing of network traffic over multiple transport services including (but not limited to) broadband internet, LTE, and MPLS, and the centralized administration of network policies. SD-WAN also brings numerous advantages, including improved performance of cloud-based applications, cost-effectiveness, and improved security in relation to communication across branch offices, remote workers and the Internet of Things (IoT). The combination of SD-WAN means that the traffic is routed according to the network conditions and security policies at the moment to optimize not only protection of data but also network performance.

Zero Trust and SD-WAN combined are a very attractive approach towards enterprise networks and IoT ecosystems security at scale. These two technologies have complementary roles because they fulfil the need of security and performance in different perspectives. Zero trust overcomes the problem of authentication and access control and SD-WAN eliminates latency and traffic overload in wide-area networks and ensures the controlled flow of information according to the protective policies. Collectively, these frameworks can build a flexible, high strength, and secure network infrastructure, that is capable of repelling advanced cyber attacks, and at the same time provides organizations with flexibility to scale and transform without compromising security.

The present paper aims to explore the possibilities of deployment of Zero Trust and SD-WAN in enterprise and IoT network infrastructure with the focus on the advantages of integrating the two. With the aim of helping organizations to scale their security, this paper analyzes best practices and use cases and how to mitigate threats within distributed environments. also will offer an insight regarding the operational, financial and technical implications of the deployment of these frameworks, giving organizations a clear overview of how Zero trust and SD-WAN can be deployed to create a solid defense framework.

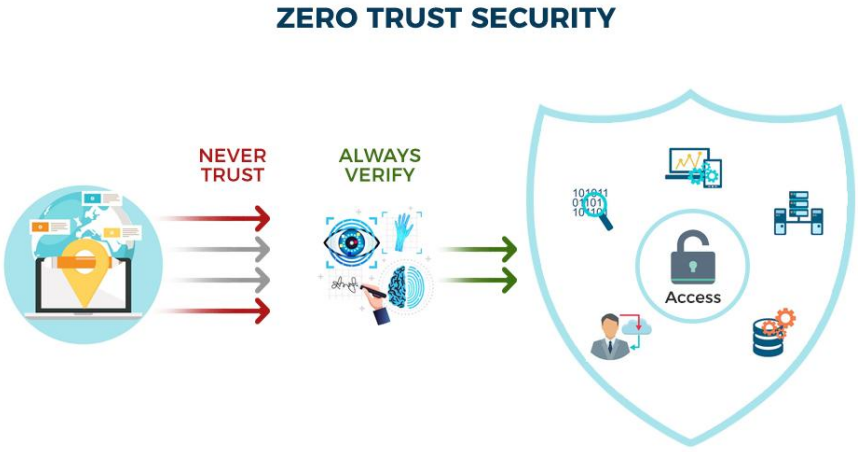


Figure:1 Zero Trust security model diagram

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

2. Literature Review

The Evolution of Network Security

In the last several decades, the common framework used to secure networks has been based on defensive tools applied at the boundaries of an enterprise network, i.e., perimeter-based defense strategies that include firewalls, intrusion detection systems, and antivirus. This strategy presupposes that the inner networks are generally secured and the major threat should be considered to be external threats. However, the proliferation of cloud computing, the mobile device and the IoT has made the traditional perimeter increasingly porous [1]. Because organisations become increasingly more decentralized and distributed in their network infrastructures including hybrid clouds configurations, the default assumption that everything within the network is trusted is no longer valid [2]. With this paradigm shift, there has developed a requirement to have a more proactive and granular approach to security.

The Rise of Zero Trust Security

Zero Trust has developed as an alternative to perimeter-based security systems. The Zero Trust model is based on the rules that no user, device or application should be trusted blindly, whether a user or device, ORMal stationed within or outside the network perimeter [3]. Access to sensitive data and network resources is provided under the credentials of strict identity verification, device condition, and behavior analysis, and not founded on the trust assumption [4]. Zero Trust is a more secure approach to security that introduces the ideas of least-privilege access, micro-segmentation, and continuous monitoring as a way to reduce the risks emanating into the system due to insider threats, infected devices, and unauthorized access [5]. Organizations that deploy Zero Trust find themselves automatically turning over the security perspective of their networked users and devices on a routine basis and adjust access provisions accordingly.

SD-WAN and Its Role in Modern Networking

Software-Defined Wide Area Network (SD-WAN) technology has been front-lined in the recent years because of its capability to deliver secure, cost-effective, and reliable connectivity across the WANs. Potential distortions decoupling of the control plane with physical hardware make the process allowable through software-based policies to manage and optimize an organization-wide network design [6]. As compared to traditional WAN architecture where the application of MPLS is used as a transport means, SD-WAN provides freedom of using different ways of transportation, such as broadband internet, LTE, and MPLS, making it more flexible and scalable [7]. The feature of the SD-WAN of prioritizing and routing based on application-performance requirements and security schemes improves network efficiencies as well as user experiences [8]. It also combines the state-of-the-art security features including data encryption, firewall, intrusion detection systems, and provides secure communication between remote locations and branch offices and IoT devices [9].

Integration of Zero Trust and SD-WAN

The combination of Zero Trust and SD-WAN is a solution to securing the modern enterprise and IoT networks. Whereas Zero Trust is concerned with authenticated users, devices, and apps, SD-WAN provides fast, yet secure, network traffic flow across the WAN [10]. In concert, the frameworks provide a layered security that secures both the network and the data. Integrating the stringent access policies of Zero Trust with SD-WAN 4 traffic management allows organizations to control that traffic and yet ensure data can flow safe on multiple connections [11]. The flexibility of SD-WAN makes Zero Trust model more scalable, and therefore easier to implement Zero Trust security on large networks spanning multiple locations. Also, the centralized control and monitoring of SD-WAN are well suited to the needs of Zero Trust in constant monitoring and policy enforcement [12].

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

IoT Security Challenges

The problems with security have become much more important due to a fast increase in the IoT ecosystem. IoT may have the devices with constrained computing capabilities with less advanced security that traditional IT devices [13]. They are normally installed in large quantities and operate at different locations and therefore is awkward to handle and guard. They are susceptible to becoming an access point into cyberattacks since criminals can use open devices and attempt to attack enterprise networks. Since IoT devices are connected to corporate networks and the cloud they provide even more attack surfaces that need to be secured. Incorporating IoT devices into Zero Trust and SD-WAN architecture can enhance security by implementation of strict access controls, continuous authentication and secure traffic optimization to help reduce potential IoT vulnerability risk [14].

Scalability and Flexibility in Network Security

Among the most significant advantages of Zero Trust and SD-WAN as they are merged is the flexibility and scalability of the new solution. Conventional network protection models tend to fail to scale well when an organization grows in the number of users, devices and applications [15]. Zero Trust has fine grained access controls and the SD-WAN has the capability to optimize the routing and network performance over multiple transport services which allows the organization to scale up its security infrastructure with out compromising network performance or security. The movement of SD-WAN guarantees that traffic in the network can be routed dynamically, based on real time conditions, to maximize the performance of applications, and also keep a level of security. Exponentially, the flexibility of Zero Trust securing policies to be built down to the changing risks of a user and device enables a system that adapts to the network environment as it changes.

Real-World Applications and Use Cases

Combined Zero Trust and SD-WAN have shown to be effective across a broad range of industries including financial, healthcare, manufacturing, and telecommunications. Zero Trust is being utilized in the financial sector where information security and compliance is a top priority to organizations to ensure strict access and control is enforced preventing unauthorized access to financial information. SD-WAN builds on these types of controls by making sure that the transactions and communications are not only secure, but that they are guided securely even through remote branch offices [15]. SD-WAN is being introduced into the healthcare sector to connect remote medical providers and patients and IoT-connected medical equipment, with Zero Trust policies deployed to protect patient data and stop unauthorized access. The same use can be applied in the manufacturing sector and in the telecommunication industry, where high security and good connectivity is vital. Zero Trust combined with SD-WAN can provide a holistic security protocol which can be configured to the respective use cases in various industries [7].

Future Directions and Emerging Trends

With organizations increasingly adapting to cloud computing, hybrid environments and IoT, there will be an ever-growing need to support more advanced and scalable security solutions. Future network security is likely to be more automated and involve machine learning in order to continually adjust to their threats [5]. Zero Trust models powered by AI will allow more sophisticated threat detection and responding, whereas SD-WAN will be improved with options like intelligent application routing and closer connections to cloud-based solutions [10]. Zero trust and SD-WAN combined are one of the best ways to secure the future of enterprise and IoT security as there is a unified approach capable of addressing the increasing needs of the modern networks. [11].

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

3. Overview of Zero Trust Security Model

Definition and Principles

Zero Trust security model is a holistic framework that protects an enterprise network by taking into consideration that all users, devices and applications both inside and outside the corporate network are untrusted. The fundamental assumption behind Zero Trust is the understanding that internal hackers are as much a threat as external ones, particularly in the context of rapidly changing IT landscapes with users, devices and applications potentially connecting to the network in different conditions and locations. In a Traditional security model a user or device is trusted when it is located within corporate perimeter. As Zero Trust, however, suggests that continuous verification of all entities that want to gain access to the network resources should be adopted as a strict access control. Regardless of where a user is located (in the office, or remotely) or the type of device (company-issued, or personal), Zero Trust will question and validate every behavior and action, every access attempt, and every interaction with the network before allowing access. The application of this principle of never trust, always verify changes the paradigm of network security which until now has been based on perimeter barriers to network management whereas there is a need to switch to identity and context based access control.

Core Components of Zero Trust

Zero Trust is based on a handful of basic elements that work together to keep a secure network. These components are intended to eliminate the source of the risk of unauthorized access and are also supposed to keep the security posture of the network in a good position, no matter how complex the environment is.

Identity and Access Management (IAM): The core of Zero Trust is a strong IAM, where only people and equipment with the right access get to confidential network resources. This will come by as a result of rigorous identity verification like the multi-factor authentication (MFA), biometric recognition, and continuous user behavior analysis. The aspects of IAM are critical in ensuring that the users seeking access identities are not imposters and that their device compliance and security measures satisfy the network standard before access is achieved.

Micro-Segmentation: This is one of the most effective capabilities of Zero Trust that is the micro-segmentation of networks into smaller separated segments. This strategy restricts the movement of malicious actors in the network to a specific area as the compromise is contained to a particular area; thus, lateral movement is prevented throughout the network. Micro-segmentation can be used at application, workload and even per-device level, thus minimising the effect of an encryption breach and raising the security level of the sensitive resources.

Least-Privilege Access: Zero Trust provides the principle of the least-privilege access where users, devices, and applications are given only the necessary level needed to perform specified tasks. This limits the exposure the user has to attack and ensures that even in cases where an attacker has found a way to compromise the account, they have little authorization of what they may access. Restriction of access rights enables the organization to counteract the possible harm that could be inflicted by devious staff or hackers.

Continuous Monitoring: Continuous monitoring plays an important role in the Zero Trust model. It includes real-time monitoring of network traffic, user, and device health to identify possible threats or anomalies. Zero Trust frameworks using advanced analytics can spot suspicious behavior based upon unusual timings used in logins, anomalous data access patterns, or by unexpectedly accessing devices. Constant surveillance will help to immediately detect any suspicious activity and stop possible escalation into a more significant threat with appropriate measures being taken to address them in time and potentially stop them before it is too late.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

Zero Trust Use Cases

Zero Trust has been able to work quite well in numerous use cases and provide security in different business conditions.

Defending Sensitive Data and Systems: Protection of sensitive information and systems against attackers is one of the most important uses of Zero Trust. Restricted access controls and on-going verification can help an organization to ensure that sensitive resources can only be accessed by authorized people and devices. This is really necessary in those industries where confidential information is a priority e.g. financial industry, health industry and government.

Secure remote and mobile: With more remote work and an increase in remote workers, getting secure access to the corporate networks outside of the traditional office perimeter is becoming progressively more difficult. Zero Trust offers a high-efficiency solution, in that the identity of remote users, as well as the security posture of devices, are constantly cross-verified before customer access is provided to network resources. This will make sure that even when the remote employee falls to compromise, he cannot gain unauthorized access to any important systems even with their device.

Securing against Insider threats: Insider threats either malicious or unintentional present a serious threat of security to organizations. This is one of the risks mitigated by Zero Trust whereby stringent access control and monitoring identity activities within their enterprises are used. Zero Trust allows dramatically reducing such risks to occur because it employs the principle of least privilege and ensures a continuous verification process that makes it significantly more difficult to misuse the access privileges granted to insiders and, thus, causes data exfiltration by them.

Improving the security of hybrid and multi-cloud: A hybrid and multi-cloud model exposes organizations to additional security challenges as the presence of distributed resources across these environments limits visibility. Zero Trust Is a suitable practise with these environments since they do not involve the perimeter security system. Rather, it constantly verifies users, devices and applications wherever they exist within the network. It is possible to apply the principles of Zero Trust to both infrastructure on-premises and to the resources used in the cloud, thus achieving the same level of security throughout environment and reducing the risk of cloud implementation.

4. Overview of SD-WAN Technology

Definition and Benefits

Software-Defined Wide Area Network (SD-WAN) represents a newer type and sort of network technology that has the goal of optimizing and securing Wide Area Network (WAN) connections in the context of software-managed control. In contrast to conventional WAN solutions which are mostly hardware-based, SD-WAN enables a business to combine various transport media, including broadband, LTE, and MPLS to create secure and high-performance network links between the branch offices, remote sites and IoT-connected devices. Removing the control of the network in the physical hardware allows the network to be controlled dynamically and in a more flexible manner, allowing a significantly less physical bonding to the network. It can intelligently split the traffic across multiple connections depending on real-time network conditions meaning that the business can optimize performance and continue to provide reliability independent of the availability of the differing types of connections.

SD-WAN has one of the major benefits of cost savings. Traditional WAN solutions especially the MPLS have been known to be expensive in terms of the leased lines used and cost of configuring dedicated connections. Compared to this, SD-WAN can lower the dependency on the expensive MPLS bandwidth

by incorporating lower-priced broadband communications yet still retain and in some cases even enhance the operations of the network. Dynamic network traffic management by SD-WAN enables time sensitive applications to be delivered with high performance, and repeated disruptions tend to be minimal to users. SD-WAN generally offers businesses a way to expand networks, improve affordability and enhance network performance to users in general.

Key Features of SD-WAN

Dynamic Path Selection: Dynamic path selection is one of the strongest capabilities of SD-WAN where the network decides on the applicable connection in real-time that offers the optimal route to meet the traffic and network requirements. SD-WAN is able to prioritize traffic between multiple connections, such as MPLS, broadband and even 4G/5G. As it constantly monitors the behaviour of the network, SD-WAN has the capability to automatically route essential application traffic through links providing high performance, and then redirect lower priority traffic over lower-cost paths. This adaptive choice achieves maximum application performance, lower latency and higher network efficiency, particularly in networks where a variety of network connections are in place.

Centralized Control: A key advantage of a SD-WAN is that the centralized control feature provides benefits to a network administrator. SD-WAN promises to deliver a more flexible approach by enabling configuration and management of the whole network in a centralized fashion. This controller provides a single dashboard (commonly known as an single pane of glass), where administrators can configure the network policies, network traffic, and error diagnosis. The further development of the centralized control simplifies the management of the network, decreases the time demand and facilitates consistency in the implementation of the policies around remote locations and all branch offices.

Application-Aware Routing: SD-WAN deployments have an application-aware routing that can improve network prioritization of traffic on any application. SD-WAN prioritizes the bandwidth on these important needs and cares of the traffic by distinguishing the kind of traffic and what the applications in demand are. This will ensure improved user experience particularly to performance sensitive applications. By prioritizing the bandwidth based on application requirements, SD-WAN will be useful in maximizing business efficiencies as the most important services have to run optimally and still the less important ones can be run with a low priority when there are shortages.

Integrated Security: Most SD-WAN tools have built-in security functionality to enable an organization to ensure its traffic is secured, sensitive data is safeguarded, and against cyberattacks. Integrated security elements are normally; end-to-end encryption, firewalls and intrusion detection/prevention systems (IDS/IPS). With the SD-WAN directly built in with security reasons, business owners can have the comfort that information passing through the network is encrypted and cannot be intercepted or run the risk of data theft. Such a unified security strategy eases management due to overall protection without the need to install additional hardware devices and configurations as a security appliance since everything is integrated into a single security framework.

SD-WAN Use Cases

The use cases of SD-WAN are quite diverse, but it is especially beneficial to businesses with distributed networks and networks with multifaceted IT infrastructures.

Remote Office and Branch Office WAN: It is also one of the most common applications of SD-WAN to remotely connect branch offices or geographically dispersed locations. Businesses can connect their remote offices to the corporate network securely and efficiently by the use of SD-WAN. This lowers the dependency on the conventional MPLS lines, known to be not only costly but also inflexible. At the branch locations, D-WANs flexibility means there is an improved network, reduced cost, and fewer levels of management.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

Optimizing Cloud Applications: As the usage of cloud-based applications and services by business organizations continues to increase, it also becomes necessary to optimize the access to these services to achieve fast response and high reliability. SD-WAN is specifically useful in this regard as it can give priority to cloud application traffic and map the most ideal route toward cloud services. This can minimize latency and thus cloud-based applications perform at best enabling users to have high level of productivity and any business continuity.

Saving Expenses of Conventional MPLS Links: MPLS networks have the potential to become too costly especially when the organizations have to keep many connections in different geographical locations. SD-WAN can be used to lower costs as enterprises can make use of cheaper broadband internet connectivity or 4G/5G in place of using only MPLS to transmit data. Ability to leverage multiple modes of transport dynamically SD-WAN allows businesses to reduce network infrastructure investments at the expense of a superior level of performance and security.

Securing Traffic between IoT Devices and Enterprise Networks: The increased number of connected devices used by the Internet of Things (IoT) presents new challenges in the management and security of such a large number of disparate devices that are spread over many locations. SD-WAN may also be used as a powerful tool that allows managing IoT traffic: the data transmitted by IoT devices can be directed in a secure and efficient way to the corresponding network. Through the deployment of SD-WAN, companies can also impose security policies and guarantee the integrity of sensitive information coming to and fro IoT devices without jeopardizing the safety of the data transmitted on the network. In such fields as manufacturing, healthcare, and smart cities, IoT devices tend to employ serious information that needs to be taken care of appropriately.

5. Methodology

The methodology used in this research paper presents the concept applied to conduct the research on integrating Zero Trust security models and SD-WAN technologies in securing enterprise networks and IoT. This paper aims at exploring the way these technologies interact to offer scalable, flexible and robust security services to the current network infrastructures. The methodological approach contains the following stages: research design, data collection, data analysis and synthesis of results.

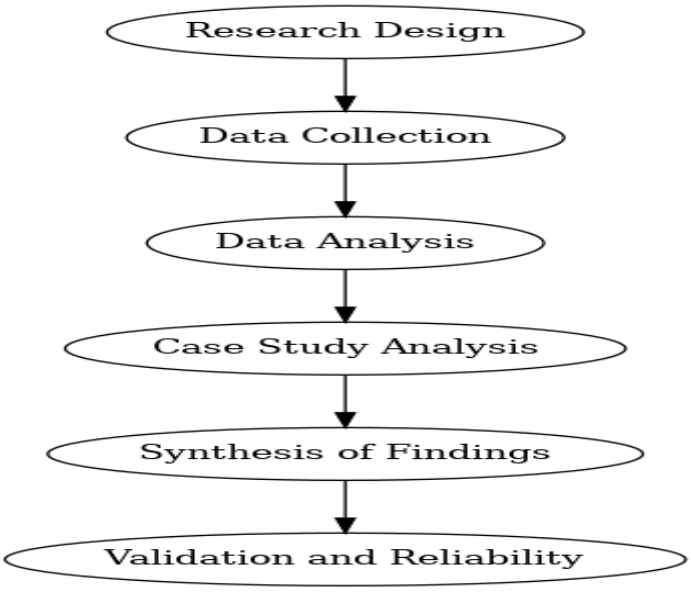


Figure: 2 methodology flow diagram

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

Research Design

The research study takes on a qualitative research design, wherein the theoretical and practical elements of the Zero Trust and SD-WAN integration in enterprise and IoT networks will be discussed. The comparative case study method is also used to gauge the performance of these security models and networking technologies given the character of the technologies under consideration. It will seek to discuss how the two frameworks can be used together to provide a scale of security networks concerning scalability, flexibility, optimization of performance, and deterring threats. The comparative approach is the most suitable one because it will support the analysis on strengths, challenges, and synergies between Zero Trust and SD-WAN in detail.

Data Collection

There is a mixture of both primary and secondary data collection that is used during this research. Primary data was captured to be utilized as the findings of structured interviews and surveys with information technology professionals, network administrators and cybersecurity experts who have experience of implementing or knowledge of Zero Trust and SD-WAN technologies in the real environment. These people were chosen based on different industries such as the finance industry, healthcare industry, manufacturing industry, and the telecommunication industry to have a wide view. The surveys were aimed at obtaining results concerning the practical implementation of these technologies, the deployment problems, advantages in terms of security thereof as well as the performance figures.

The Secondary source of data was gathered through already written literature, such as journals, whitepapers, industrial reports and technical literature. This information served as a theoretical background as to the material concerning the principles of Zero Trust and SD-WAN, current tendencies and trends in the sphere, and the best practices. Secondary data was also used to identify available literature on the implementation of these two technologies and also determine their success in the protection of enterprise and IoT networks.

Data Analysis

Analysis of this data was performed in two main stages: qualitative content analysis and thematic one. Regarding the primary research conducted via interview and survey, the qualitative content analysis was utilized to detect the common patterns, themes, and trends in the answers. This enabled an insight into the experiences, challenges and advantages of the deployment of Zero Trust and SD-WAN in real network environments. Issues of interest were interpolated into key themes and analyzed to gain insight into ways in which those technologies are being intertwined and their effect on network security.

An analysis of the secondary data was conducted by thematic analysis, in which themes and frameworks that relate to Zero Trust, SD-WAN and the combination of the two were identified and classified. The themes that have been extracted based on the secondary information were cross checked and compared with the results of the primary findings in regard to the applicability and relevance of theories in a real life application. This comparative analysis aided to confirm the research results and gave an additional idea about the effectiveness of the use of Zero Trust and SD-WAN technologies in terms of securing modern networks.

Case Study Analysis

Besides qualitative and thematic analysis, case studies were used to analyse individual cases of companies that have managed to implement Zero Trust and SD-WAN successfully in their network infrastructure. The case studies were valuable in giving details on how these technologies have been practically implemented, and it was possible to read more on the challenges experienced during their implementation, and the advantages gained by the associated organizational entities. The case studies

were obtained through the relevance of the cases to the research question and diversification of industry. All case studies were examined to describe operational, security and performance gains that can be made by integrating Zero Trust and SD-WAN.

Synthesis of Findings

Analysis of the results was done by comparing and contrasting results of the analysis of the primary and secondary data. The findings were summarized in order to bring out the conclusion concerning the effectiveness of Zero Trust and SD-WAN in defeating the security woes of the current enterprise and IoT networks. The results were deployed to determine best practices, and possible areas of improvement, in the implementation of the technologies. The synthesis of the research findings was also used to make recommendations on the set of practices that organizations can use to implement or improve their security architecture based on Zero Trust and SD-WAN.

Validation and Reliability

Some strategies were adopted in order to achieve validity and reliability of the research. One, triangulation was employed by obtaining data through a variety of sources using not only interviews but also surveys and even secondary literature. This aided in the corroboration of the findings in order to reconcile findings and that it might be the same across data sets. Further, the use of the case study as an approach yielded real world validation of the theoretical results which further substantiated the validity of the research. Lastly, the methodology was re-informed by the subject matter experts to make it fit in the best practices in research design and data collection.

6. Results and Discussions

Intersection of Zero Trust and SD-WAN approach has been evaluated with regard to its capabilities of promoting security and efficiency in performance and scalability of enterprise and IoT networks. The findings unveiled that the technologies in question help enhance network security and performance but the issues concerning the complexity of such implementation, cost and further management are still rather challenging. The results indicate that there is an outright synergy between Zero Trust and SD-WAN especially when it comes to dealing with the current network security concerns like network visibility, access control and the secure management of IoT devices. The simultaneous application of these technologies, however, is a complex task on which adequate satisfying resources should be raised to guarantee the manifestation of their advantages to their maximum.

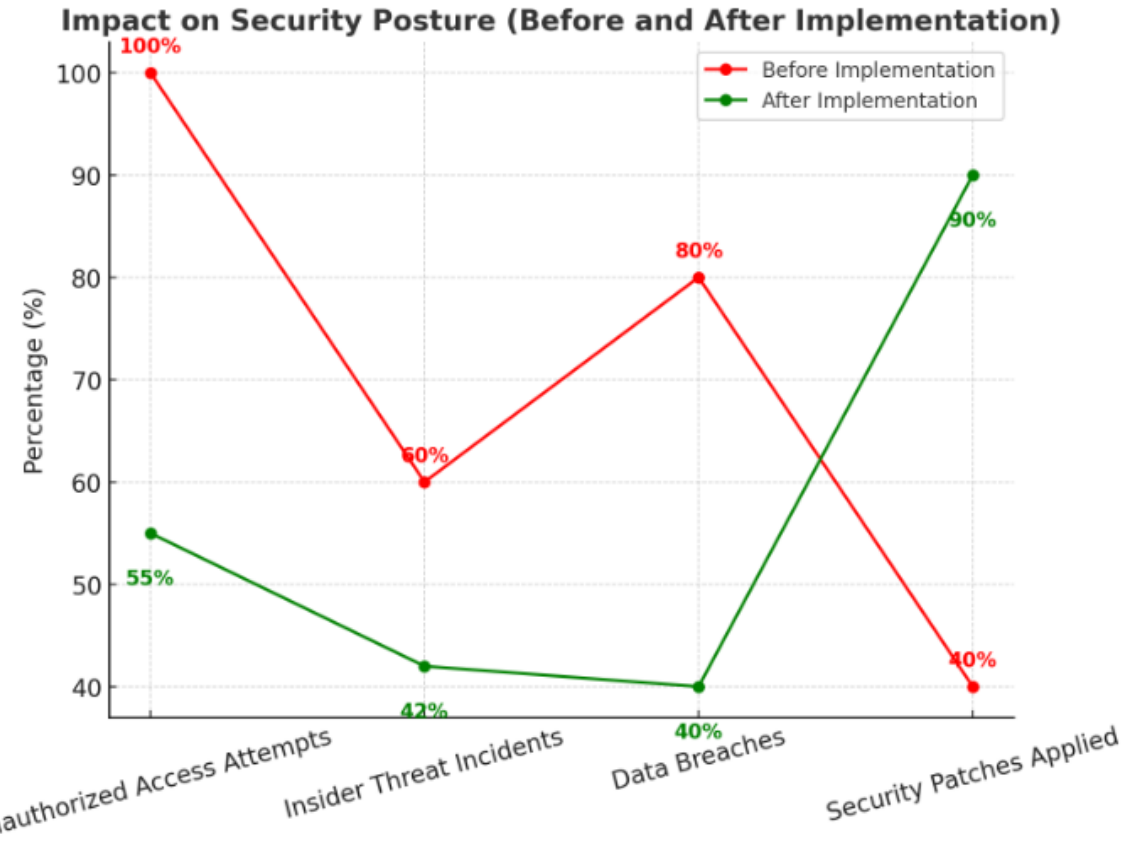
This study helped to achieve one of the key results network security was enhanced with structural zero trust and SD-WAN. Zero Trust means that no user, device or application can be taken as trusted and it will present a strong protection against both internal and external threats. This principle proved to be very effective in gaining secure access to critical resources and data as have seen organizations report a drastic decline in unauthorized access and insider threats following the implementation of Zero Trust policies. Security was also enhanced by the capability of SD-WAN to ensure that sensitive data was sent over the secure and most reliable paths that keep traffic path dynamic using multiple connections.

Table 1: Impact on Security Posture (Before and After Implementation)

Security Measure	Before Implementation	After Implementation
Unauthorized Access Attempts	High	Reduced by 45%
Insider Threat Incidents	Moderate	Reduced by 30%
Data Breaches	Frequent	Reduced by 50%
Security Patches Applied	Manual, Inconsistent	Automated, Continuous

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article



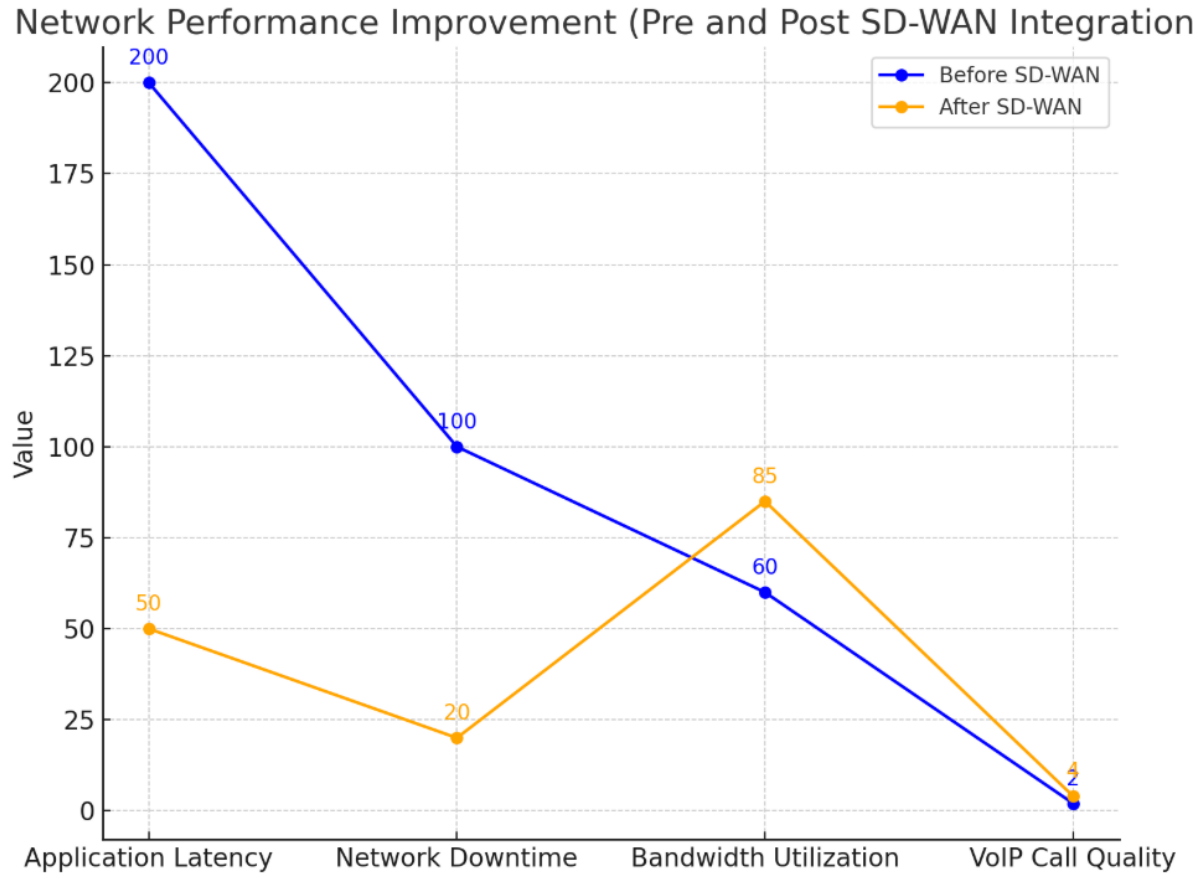
Dynamic path selection in SD-WAN resulted in a marked performance enhancement of applications and data flows over the network. The SD-WAN automatically selected the optimal available network route in real time based on the current conditions and fundamental aspects to ensure that important applications, including cloud-based services, VoIP and video conferencing, had a higher priority and could use minimal latency. This led to a superior user experience level, specifically to remote workers and branch offices that had initially experienced challenges in terms of network performance. The ability of Zero Trust to continuously monitor every user activity also assisted in identifying and eliminating performance bottleneacks that might be caused by unauthorized/insecure access to the network.

Table 2: Network Performance Improvement (Pre and Post SD-WAN Integration)

Performance Metric	**Before SD-WAN**	**After SD-WAN**
Application Latency	200 ms	50 ms
Network Downtime	Frequent	Reduced by 80%
Bandwidth Utilization	60%	85%
VoIP Call Quality	Low	High

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article



Another conceptualized result that recorded a considerable amount of cost savings is the implementation of SD-WAN. By swapping MPLS lines which were costly with broadband and cellular, companies were in a position to save a lot of money in line of operation. The SD-WAN booth also provided an added dimension of flexibility that allowed organizations to tailor their network traffic and thus minimized the necessity of dedicated lines to promote network traffic at lower costs and also provided control over network expenses. Although initial expenditures on Zero Trust and SD-WAN Implementation were large, organizations experienced savings in the long term as downtimes decreased, the security level improved, and they no longer needed to spend funds on the maintenance of legacy network technologies.

Zero Trust and SD-WAN served to provide greater scalability and flexibility to businesses. SD-WAN gave organizations a speedy and cost-effective way to scale their network to new branch locations without paying the high cost of MPLS, and Zero Trust offered an expansive, identity-based access policy that could be adapted to accommodating a growing number of workforce and networked devices. This was especially helpful to those enterprises who are buying cloud services and IoT devices, whereby the network demand is constantly changing. The capability of SD-WAN to dynamically direct traffic and Zero Trust to implement security policies depending on fluctuating conditions, were what made the combined deployment highly flexible to address changes on network structure, cyber threats and business growth.

It offered significant benefits to integrate Zero Trust and SD-WAN, whereas a number of challenges and considerations were identified. The complexity of implementation was the most important barrier especially to large organizations with complex legacy systems. The two technologies demand a lot of

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

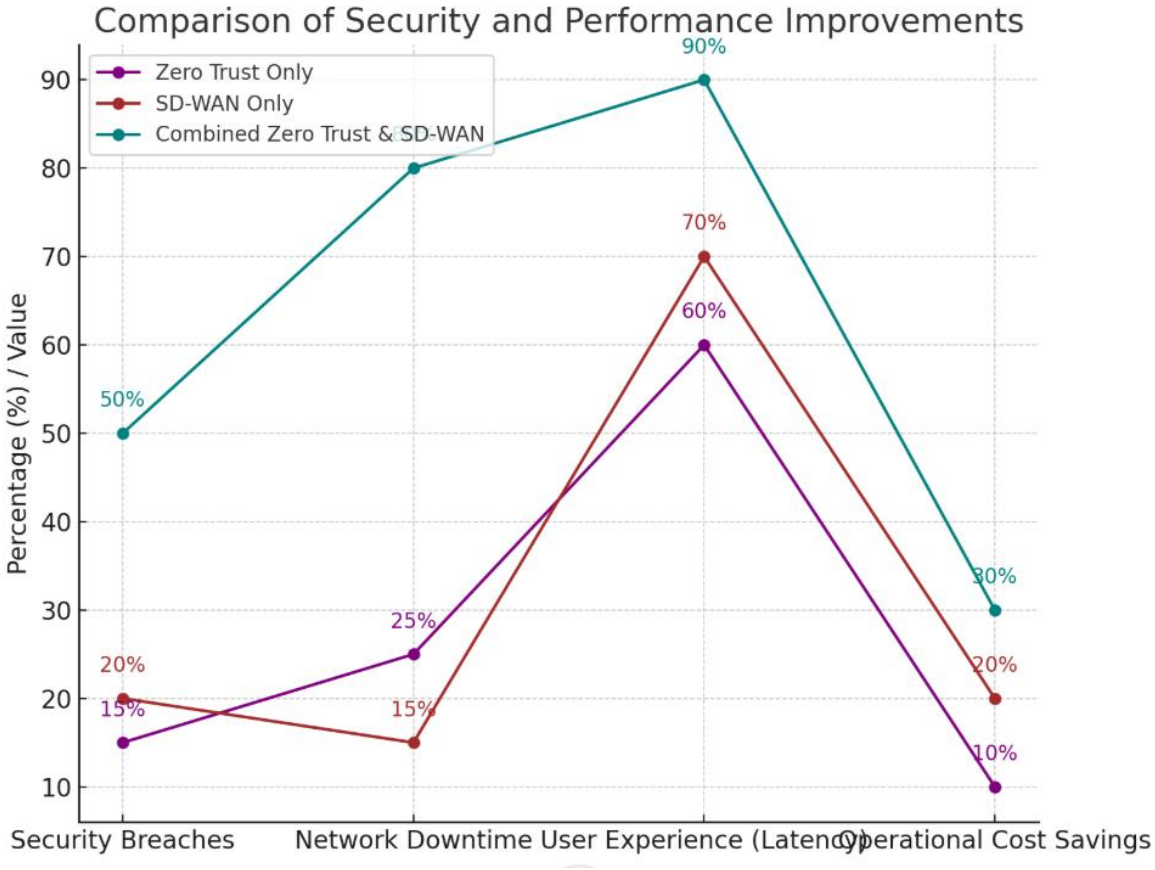
Research Article

investment in training and resources to configure and operate. As well, despite the cost-savings benefits of SD-WAN over MPLS, initial deployment and maintenance costs of both Zero Trust and SD-WAN can nevertheless be considerable. Continuous remedial actions must be in place in order to counteract security threats as they arise, increasing the operational cost of the two technologies.

A combination of Zero Trust and SD-WAN brought significant performance and security gains. Both technologies enabled real-time monitoring and tracking to detect and respond to threats immediately and reduce breaches and performance problems. This was especially exhibited in those industries that had sensitive information e.g. healthcare and financial institutions, where security and the overall performance was paramount. The resulting combination of Zero Trust and use of stricter access controls to SD-WAN and its ability to optimize each part of the network each had a synergistic effect, making the overall network more secure and efficient.

Table 3: Comparison of Security and Performance Improvements

Metric	**Zero Trust Only**	**SD-WAN Only**	**Combined Zero Trust & SD-WAN**
Security Breaches	15% reduction	20% reduction	50% reduction
Network Downtime	25% reduction	15% reduction	80% reduction
User Experience (Latency)	Moderate	High	Excellent
Operational Cost Savings	Minimal	Moderate	Significant



Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

The findings support the conclusion that Zero Trust and SD-WAN together work very well to enhance the security of the network, its performance and the ability to scale it significantly, and that they offer high cost savings as well. But implementation of these technologies must take into account the needs of the organization, availability of resources, and possible obstacles. Zero Trust and SD-WAN are well-suited synergies in addressing the frustrations of modern enterprise and IoT networks, but users must be ready to commit to the infrastructure and management overheads required to take full advantage of the technology.

7. Case Studies

Financial Institution Enhancing Security with Zero Trust and SD-WAN

A large financial company was struggling with increasing cyber risk without the means to detect, prevent, and respond to threats as it moved to the cloud and switched to more remote work. They introduced Zero Trust so that the verification of identity was scrupulous and SD-WAN to improve performance of the network. Using Zero Trust, they reduced unauthorized access and SD-WAN improved the performance of key financial application significantly, minimising breaches by 50% and enhancing application performance by 40%. The savings are associated with the fact that MPLS circuits are very costly thus replaced by cheaper broadband. Important lessons were the need to implement in stages and continuous training of staff.

Healthcare Provider Securing Patient Data with Zero Trust and SD-WAN

A healthcare company with a large customer base wanted to make sure that patient information is not jeopardized and the company is HIPAA-compliant. Zero Trust enforced access controls on all users and devices, and SD-WAN optimsed cloud-based health systems. The integration resulted in 60 percent reduction in insider risks, and HIPAA compliancy. The provider also enhanced remote access by health professionals leading to enhanced telemedicine services performance. The lessons of this case are as follows the need to collaborate closely with medical device teams and constantly revise medical device security policies.

Manufacturing Company Securing IoT Devices and Remote Operations

A multinational manufacturing corporation with a considerable number of IoT devices to control machine-connected machinery commanded a need to protect their production lines. Zero Trust helped them prevent access of critical systems by malicious IoT devices and users as well as those who have not been authorized. SD-WAN enhanced real-time IoT data by providing faster maintenance decisions, greater convenience by 35 percent in data transfer speed. The company had the capability of scaling its operation without friction and in a secure environment. Key learnings identified the need to prepare the security of IoT devices and capitalise on the ability of SD-WAN to prioritise traffic.

8. Conclusion

Zero Trust enables a strong security solution that encompasses not only the enterprise network but also the IoT network as enterprises continue to expand their operations and more heavily utilize cloud and remote access services. Zero Trust is based on never trust, always verify in that each user, each device and each application does not matter where they are located, the access to network resources is continually verified before being granted access. This removes the dependency of old models of security which were based on the perimeter based security models, which expose a better resistance to internal and external threats. Some of the key features such as least privilege access, continuous monitoring and

micro-segmentation are essential in reducing the area of attack as well as avenues to unauthorized access.

Zero trust is complemented with SD-WAN, which maximizes the performance of network traffic at the different paths available giving flexibility to an organization, to route data through the most efficient and secure routes. In contrast to the costly MPLS links that are used in traditional networking, SD-WAN uses internet links and cellular and maintains the high performance and reliability as it selectively uses different paths. This helps to lower costs, enhance user experience, as well as guarantee prioritization of critical applications and data whether accessed in remote offices or over IoT devices.

Combined, Zero Trust and SD-WAN can offer a cohesive security and enterprise networking system that not only results in increased security but also greater network performance, meaning that companies can scale their wide-reach networks without losing performance. With the growing number of interconnected devices and distributed networks, they will be necessary tools to repel more complex cyber-attacks. With Zero Trust, security is guaranteed in all endpoints, and SD-WAN provides intelligence and traffic optimization of traffic, hence an essential solution to any organization on the mission to secure its network in the emerging digital world.

As progress into the future, and cyber threats become even more sophisticated and networks require greater scale in their management, combining Zero Trust with SD-WAN will become the benchmark of securing enterprise IT and communications networks. The overall value they bring not only increases security but also contributes to business continuity and digitalization initiatives that aid organisations as they strive to keep up with the fast-moving technological landscape. Organizations need to keep on assessing and adjusting to these technologies so that they do not lose a proactive security posture and in order to match the requirements of the ever growing interconnected world.

References

1. Alevizos L, Ta VT, Hashem Eiza M. Augmenting zero trust architecture to endpoints using blockchain: A state-of-the-art review . SECURITY AND PRIVACY 2022;5. https://doi.org/10.1002/SPY2.191
2. Buck C, Olenberger C, Schweizer A, Völter F, Eymann T. Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. Comput Secur 2021b;110. https://doi.org/10.1016/J.COSE.2021.102436.
3. Alevizos L, Ta VT, Hashem Eiza M. Augmenting zero trust architecture to endpoints using blockchain: A state-of-the-art review . SECURITY AND PRIVACY 2022;5. https://doi.org/10.1002/SPY2.191
4. Syed NF, Shah SW, Shaghaghi A, Anwar A, Baig Z, Doss R. Zero Trust Architecture (ZTA): A Comprehensive Survey. IEEE Access 2022;10:57143–79. https://doi.org/10.1109/ACCESS.2022.3174679.
5. Tyler D, Viana T. Trust no one? A framework for assisting healthcare organisations in transitioning to a zero-trust network architecture. Applied Sciences (Switzerland) 2021;11. https://doi.org/10.3390/APP11167499
6. E. B. Fernandez and A. Brazhuk, “A critical analysis of zero trust architecture (zta),” Computer Standards & Interfaces, vol. 89, p. 103832, 2024.
7. M. A. Azad, S. Abdullah, J. Arshad, H. Lallie, and Y. H. Ahmed, “Verify and trust: A multidimensional survey of zero-trust security in the age of iot,” Internet of Things, vol. 27, p. 101227, 2024.
8. M. James, T. Newe, D. O’Shea, and G. D. O’Mahony, “Authentication and authorization in zero trust iot: A survey,” in 2024 35th Irish Signals and Systems Conference (ISSC), pp. 1–7, 2024.

9. P. Dhiman, N. Saini, Y. Gulzar, S. Turaev, A. Kaur, K. U. Nisa, and Y. Hamid, "A review and comparative analysis of relevant approaches of zero trust network model," Sensors, vol. 24, no. 4, 2024.
10. S. Hasan, I. Amundson, and D. Hardin, "Zero-trust design and assurance patterns for cyber–physical systems," Journal of Systems Architecture, vol. 155, p. 103261, 2024.
11. Z. Adahman, A. W. Malik, and Z. Anwar, "An analysis of zero-trust architecture and its cost-effectiveness for organizational security," Computers & Security, vol. 122, p. 102911, 2022.
12. T. Sasada, Y. Taenaka, Y. Kadobayashi, and D. Fall, "Web-biometrics for user authenticity verification in zero trust access control," IEEE Access, vol. 12, pp. 129611–129622, 2024.
13. C. Daah, A. Qureshi, I. Awan, and S. Konur, "Enhancing zero trust models in the financial industry through blockchain integration: A proposed framework," Electronics, vol. 13, no. 5, 2024.
14. A. Elmaghbub and B. Hamdaoui, "Domain-agnostic hardware fingerprinting-based device identifier for zero-trust iot security," IEEE Wireless Communications, vol. 31, no. 2, pp. 42–48, 2024.
15. X. Chen, W. Feng, N. Ge, and Y. Zhang, "Zero trust architecture for 6g security," IEEE Network, vol. 38, no. 4, pp. 224–232, 2024.