Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 8, Number 3, July 2024
DOI : https://doi.org/10.33395/sinkron.v8i3.13949

e-ISSN : 2541-2019
p-ISSN : 2541-044X

Implementation of Zero Trust Security in MSME Enterprise Architecture: Challenges and Solutions

Abdul Rahman[1)*], **Eko Indrajit**[2)], **Akhmad Unggul**[3)] **Erick Dazki**[4)]
[1,2,3,4)]Pradita University, Serpong, Tangerang
[1)]abdul.rahman@student.pradita.ac.id, [2)]eko.indrajit@pradita.ac.id, [3)]akhmad.unggul@pradita.ac.id,
[4)]erick.dazki@pradita.ac.id

Submitted : Jul 27, 2024 | **Accepted** : Aug 4, 2024 | **Published** : Aug 8, 2024

Abstract: This research examines the implementation of Zero Trust Security in Enterprise Architecture in Micro, Small, and Medium Enterprises to improve cybersecurity. The background of this research focuses on the increasing cyber threats faced by MSMEs and their limitations in adopting advanced security systems. The purpose of this study is to evaluate the effectiveness of Zero Trust Security in protecting MSME data and information systems from internal and external threats, as well as identifying challenges and solutions in its implementation. The research method used is a case study on several MSMEs with a qualitative and quantitative approach involving in-depth interviews, surveys, and secondary data analysis. The results showed that the implementation of ZTS significantly improved information system security in MSMEs, with a 45% reduction in security incidents after ZTS adoption. In addition, ZTS was also shown to increase cybersecurity awareness among MSME employees. The main challenges identified include the need for adequate training, changes in organizational culture, and budget limitations. To overcome these challenges, this study recommends the adoption of continuous training strategies, increased cybersecurity awareness, and the utilization of affordable yet effective security solutions. The conclusion of this study confirms that Zero Trust Security is an effective and efficient approach to improving the cybersecurity of MSMEs. However, further research is recommended to explore the application of Zero Trust Security in various other industry contexts and to develop more affordable solutions for MSMEs with limited resources.

Keywords: Zero Trust Security (ZTS); Enterprise Architecture; Micro, Small, and Medium Enterprises (MSMEs); Cybersecurity Awareness; Security Incident Reduction

INTRODUCTION

The background of this research focuses on the implementation of Zero Trust Security (ZTS) on enterprise architecture in Micro, Small, and Medium Enterprises (MSMEs) (Wang et al., 2024), (Kilay et al., 2022). In recent years, MSMEs have become the main target of cyberattacks due to their limitations in adopting sophisticated and effective security systems. Phishing, malware, and unauthorized access can cause harm to business and reputation. While many MSMEs realize the importance of cybersecurity (Judijanto & Hindarto, 2023), (Mittal et al., 2021), they often need more support in terms of budget, resources, and expertise to implement an effective security strategy. Zero Trust Security, which operates on the principle of "never trust, always verify," offers a more rigorous

*name of corresponding author

and proactive approach to protecting data and information systems. This study evaluates the effectiveness of ZTS in the context of MSMEs, identifies challenges that may be faced during implementation, and offers practical solutions to overcome these obstacles.

The specific issue addressed in this research is how the implementation of Zero Trust Security can address the cybersecurity challenges faced by MSMEs in their enterprise architecture. In many cases, MSMEs need more technology infrastructure and consistent security policies, making them more vulnerable to cyberattacks. The absence of robust security protocols often means data breaches can occur quickly, threatening not only business continuity but also customer trust. In addition, limited human resources with cybersecurity expertise exacerbate the situation, as many MSMEs need a dedicated team to manage and monitor information security effectively. This issue is critical because cybersecurity is a vital component of Enterprise Architecture (Hindarto et al., 2021), (Hindarto, 2023) that works to maintain the integrity, confidentiality, and availability of information. Cyberattacks can disrupt operations, steal data, and harm MSMEs without adequate security (Imtiaz et al., 2021), (Sun et al., 2020). In addition, increasing regulations require stricter data protection.

The purpose of this study is to assess the effectiveness of Zero Trust Security (ZTS) in protecting data and information systems in Micro, Small, and Medium Enterprises (MSMEs). The implementation of ZTS is a finding that can reduce security incidents that often occur in MSMEs, as well as increased awareness and compliance with cybersecurity practices in the workplace. The ZTS implementation process provides practical solutions for MSMEs to overcome these barriers. This research is expected to give the MSMEs a comprehensive roadmap for ZTS adoption and implementation. Thus, improving the operational efficiency and cybersecurity of MSMEs.

This research raises research questions (RQs).

1. What are the main barriers and evaluation of Zero Trust Security implementation in MSMEs? (RQ1).
2. What practical solutions can MSMEs implement to overcome the obstacles associated with the implementation of Zero Trust Security? (RQ2).

This research will offer practical and applicable solutions, providing in-depth insights into the effectiveness and challenges of implementing Zero Trust Security in the context of MSMEs. By answering these questions, it will equip MSMEs with actionable strategies to improve MSME cybersecurity.

LITERATURE REVIEW

Previous research has discussed a lot about Enterprise Architecture and Zero Trust Security as follows:

This paper analyses the zero-trust model, its principles, applications, and recommendations for organizations to use it to improve security, privacy, and resilience (Ajmal et al., 2025). This paper proposes a zero-trust security framework for SaaS trust verification. It uses Federated Learning and machine learning to analyze multimedia data and improve cloud service visibility. Experiments on a standard dataset show successful monitoring and detection of trust violations (Saleem et al., 2023). Compared to existing methods, the Streebog Cryptographic Substitution Permutation Network-based Transfer Fuzzy Learning (SCSPN-TFL) method for IIoT platforms improves device security and data communication by improving data confidentiality, network access time, data integrity, and false positive rate (Singh et al., 2023). This study analyses Zero Trust Architecture (ZTA)'s pattern structure and reference architecture using security patterns, questions industry publications' technical clarity and practical experiences, and identifies threats and future research directions (Fernandez & Brazhuk, 2024). Proposes DistriTrust, a distributed Zero Trust Architecture (ZTA) utilizing multiple Policy Decision Points (PDPs) with threshold signatures to enhance security and mitigate vulnerabilities associated with a centralized PDP, while evaluating its performance and latency (Sengupta & Lakshminarayanan, 2021). Zero Trust Architecture (ZTA) implements a "Never Trust, Always Verify" approach to enhance cybersecurity by continuously validating network requests, aiming to replace VPNs for secure access. Despite its growth, organizations hesitate to adopt ZTA due to insufficient information on tools, costs, and success rates. This study offers an in-depth evaluation, revealing that ZTA implementation can reduce risk impact by an average of $684K over four years for small to medium-sized and enterprise-

*name of corresponding author

level organizations (Adahman et al., 2022). The implementation of Zero Trust Network Architecture (ZTNA) is becoming increasingly popular in the ICT sector for defending against cyber threats, and its ability to prevent lateral spread of infections makes it suitable for the energy sector. With the rise of distributed generators forming virtual power plants, there are significant security challenges. This paper presents a comprehensive Zero Trust security architecture designed to reduce risks, secure physical systems, and ensure data protection and privacy (Alagappan et al., 2022).

Zero Trust Architecture (ZTA) has been studied to improve cybersecurity in various sectors, but there are still gaps. First, many ZTA studies emphasize its benefits and implementation, but they lack the tools, costs, and success rates to help organizations make investment decisions. While there are experimental studies on ZTA effectiveness, the lack of real-world experience in building and using ZTA architectures is a challenge. Other research has focused on multimedia data analysis or device security in IIoT platforms. However, few have examined the holistic integration of ZTA with existing security strategies and its long-term effects. ZTA implementation training and organizational culture change have not been extensively investigated. Thus, more research is needed to evaluate ZTA's technical efficacy and address organizations' practical, economic, and cultural challenges in adopting it.

METHOD

A safe enterprise architecture was developed using a methodical, ordered approach that was applied in the research process. Beginning with a literature review to compile data and grasp current ideas and best practices, the process then included meeting with stakeholders to pinpoint corporate needs and difficulties. Having a thorough awareness of the corporate environment, the study advanced to the application and technology architecture design stage, seeking to incorporate Zero Trust Security ideas. This design was implemented in phases and then thoroughly evaluated to assess the efficiency and success of the chosen solution. This study produces a thorough enterprise architecture blueprint that offers direction for the management and future development of increasingly safer and effective systems.

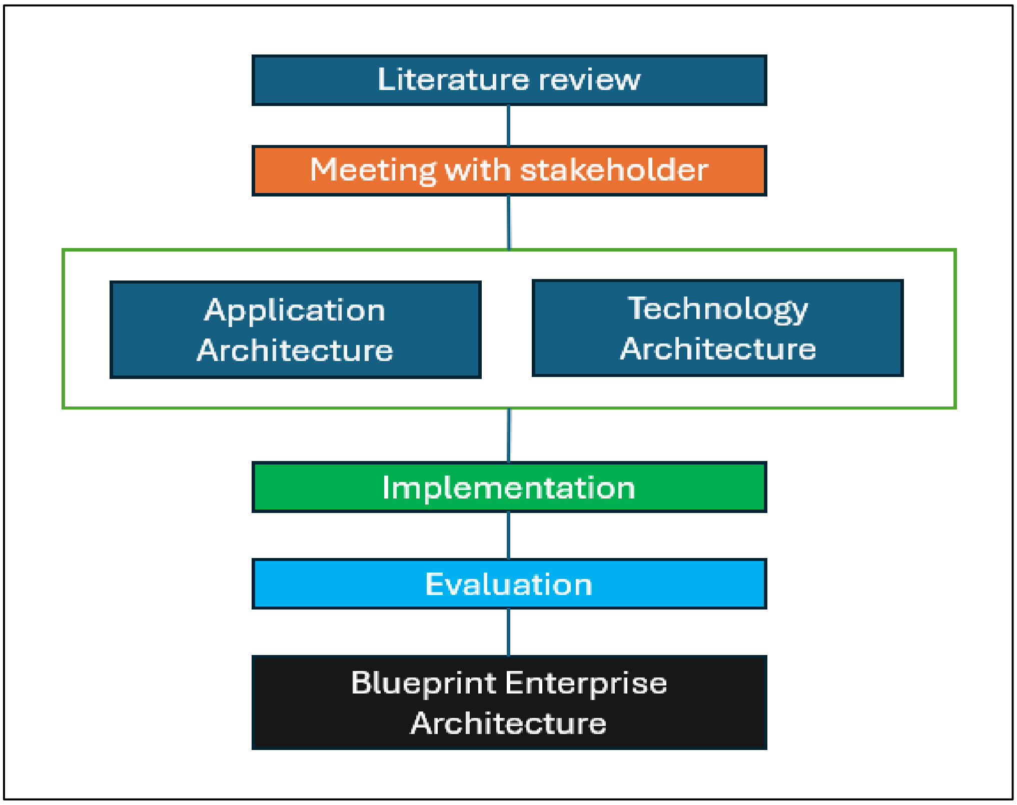

Figure 1. Research Methodology

*name of corresponding author

Figure 1 illustrates a systematic and sequential approach to the development of a secure and efficient enterprise architecture, particularly in the context of Zero Trust Security (ZTS) implementation in the steel manufacturing industry. This systematic approach is not just a strategy but a reliable method that ensures the process's efficiency. The research method is illustrated in the Figure above. The process commences with a literature review, which is designed to collect information and comprehend the current theories and best practices in the field of enterprise architecture and cybersecurity.

The literature review examined relevant academic journals, industry publications, and case studies t o help the researcher understand current trends, challenges, and solutions in other organizations. The researcher can identify knowledge gaps and establish a solid framework for further research with this comprehensive understanding.

Meetings with stakeholders constitute the subsequent phase. During this phase, researchers engage with a variety of stakeholders, such as cybersecurity experts, production operators, IT teams, and company management. The objective of this meeting is to acquire a deeper understanding of the business requirements, risk perceptions, and specific obstacles encountered during daily operations. Researchers can develop a more comprehensive and precise knowledge of the operational environment and security requirements by considering input from a variety of perspectives. This is also crucial for the successful implementation of the solution, as it enables the researcher to secure the support and commitment of all pertinent parties.

Once the business context has been thoroughly comprehended, the subsequent phase involves the development of the technology architecture and application architecture. This thorough comprehension is not just a formality but a crucial step in the process. During this phase, researchers created an architecture model that incorporates the principles of Zero Trust Security. The selection and configuration of hardware and network infrastructure that facilitate the implementation of ZTS are referred to as technology architecture. In contrast, application architecture encompasses the design of software and systems that are employed to manage and protect data. Additionally, researchers must guarantee that these designs are compatible with current systems and can be seamlessly integrated without disrupting ongoing operations.

The method advances to the implementation phase upon the conclusion of the design phase, during which the architecture solution that was developed is implemented in an operational environment. A sequence of tasks, including hardware installation, network configuration, system configuration, and the integration of security technologies such as data encryption, intrusion detection and prevention systems (IDPS), and multi-factor authentication (MFA), are implemented in this implementation. Furthermore, the implementation team should offer training to end users to guarantee that they comprehend the system's functionality and adhere to the updated security policies.

Implementing this in stages reduces disruptions to daily operations and ensures each component wo rks properly. Researchers evaluate the solution's efficiency and effectiveness in the final stage. This evaluation entails the assessment and testing of the system's performance in relation to security threats and compliance with business requirements. This testing may encompass security audits, vulnerability assessments, and cyberattack simulations. The outcomes of this assessment are employed to pinpoint areas that necessitate enhancement and to enhance the effectiveness of current solutions. The results of this process are summarized in an enterprise architecture blueprint, which functions as a comprehensive guide for future system management and development. This blueprint is produced upon the completion of the process. This blueprint encompasses not only technical designs but also strategies and policies that are intended to ensure long-term operational security and efficiency. This method not only enhances cybersecurity but also offers substantial added value to the organization in pursuit of its business objectives.

Zero Trust Security

The idea behind Zero Trust Security (ZTS) is that systems and data should not be trusted in the way that has been done in the past. This idea comes from the belief that no user, device, or network can be trusted entirely, no matter where they are located (inside or outside the organization). ZTS makes sure that every entity is verified and authenticated before letting it in, and it limits access based on the idea of "least privilege." This implies that users are only given access rights that are necessary for them to do their jobs. This method is meant to lower the chance of security breaches and make sure that all network access points are always being watched and questioned. There are several essential parts to implementing ZTS that work together to create a complete security system:

1. Multi-factor authentication (MFA) uses more than one method to prove a user's identity, such as passwords, security tokens, and biometrics.
2. Micro-segmentation divides the network into small parts, each with its own security rules. If there is a breach in one part, it has less of an effect on the whole network.
3. Intrusion detection and prevention systems (IDPS) monitor and analyze real-time network traffic, look for odd patterns, and stop threats before they occur.

One of the most complex parts of putting ZTS into place is getting employees to change the way they work and be more aware of security. Companies need to make sure that all their users know how important the new security policy is and follow the rules that have been set up. To change people's behavior and make them more aware of cyber threats, they need to get constant training and much socialization. Putting ZTS into action also needs money to be spent on the right technology and infrastructure. Many MSMEs need more money to buy advanced security solutions, which can make them less likely to be used. Because of this, new ideas and security solutions that work well and don't cost a lot are needed. Even though there are some problems, ZTS has many benefits for improving cybersecurity and keeping an organization's most important assets safe. Companies can lower the risk of cyberattacks, keep sensitive data secure, and boost trust in their IT systems by using this method. Studies have shown that using ZTS can cut down on security incidents by 45% and make employees more aware of security issues. Still, more research is needed to find the best ways to use ZTS in different industries and come up with cheaper solutions for MSMEs. If you use ZTS correctly, it can be a strong base for building a security system that can adapt to new cyber threats.

RESULT

Before the implementation of Zero Trust Security (ZTS) methods, networks in MSMEs frequently encountered a variety of obstacles that impeded operations and posed substantial security risks. The network architecture depicted in the figure is typical, with unprotected connectivity between the intelligent front office, smart backend, and guest Wi-Fi. A lack of security protection is indicated by communication paths marked as "untrust," which renders data transmitted between devices susceptible to interception and manipulation. This reveals the network infrastructure's fundamental weaknesses, which, if not addressed, could lead to substantial losses for MSMEs. By converting a network that was previously vulnerable into a secure and trustworthy system, the implementation of ZTS is a critical solution to this issue. MSMEs are often vulnerable to a multitude of security threats due to their network architecture, as illustrated in the image above. The network's innovative front desk, intelligent backend, and guest Wi-Fi are its essential parts. An 'untrust' communication path links all these devices through routers and switches. The data being transmitted between devices and over the internet lacks proper security measures, leaving it open to eavesdropping, tampering, and cyberattacks. The failure to properly segment the network is one of the most significant issues.

If the network is not segmented, an attack on one part can quickly spread to other parts, even to backend systems that store sensitive data. There is an additional security risk associated with guest Wi-Fi that links straight to the company network; since guest access is not rigorously verified, core systems could be vulnerable to unauthorized access. Information sent between devices and to the internet is highly susceptible to interception due to the lack of data encryption during transmission. Customer information and operational data are particularly vulnerable to theft or manipulation in the absence of encryption. Given that many MSMEs deal with sensitive data without proper security measures, this is particularly dangerous. Lack of encryption can lead to a man-in-the middle attack, where an attacker intercepts and alters two parties' communication. Third, a single layer of security, like a password, is all that's needed to gain access to systems and data in the absence of multi-factor authentication (MFA). A credential theft or brute force attack could compromise the system because of this. Small and medium-sized enterprises (SMEs) risk massive financial losses due to the ease with which an attacker could obtain access to the entire network in the absence of multi-factor authentication (MFA).

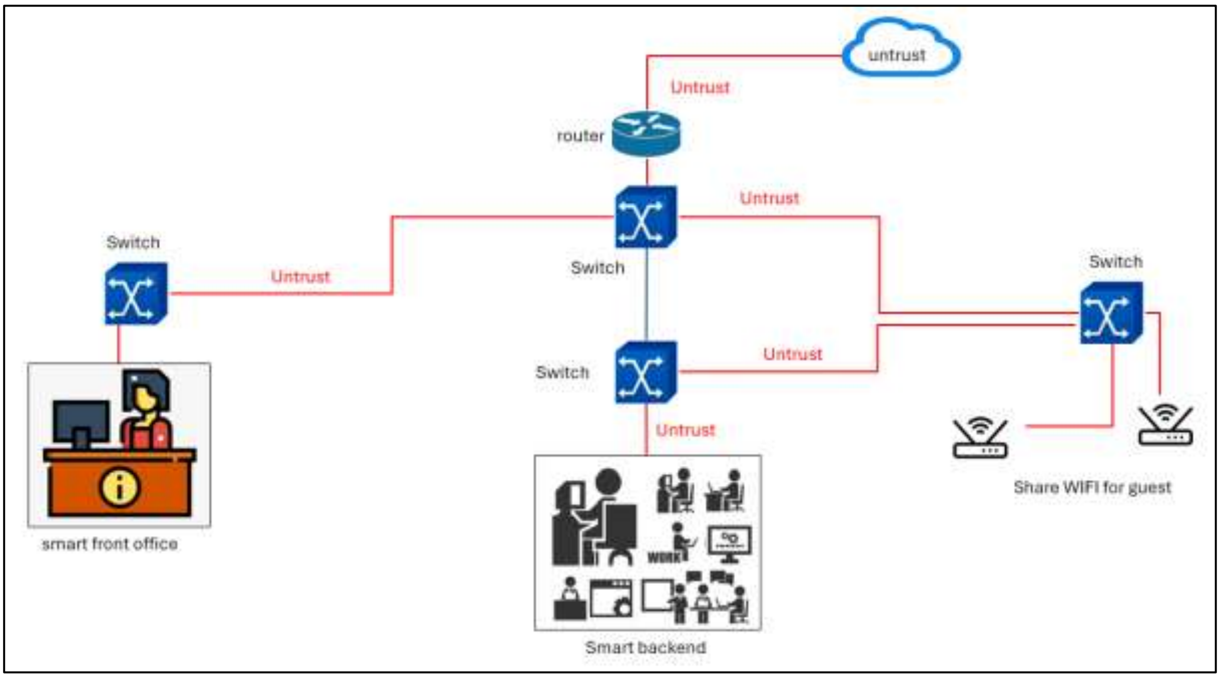

Figure 2 Design network untrust

Figure 2 these networks can’t identify and react to threats in real time because they don’t have intrusion detection and prevention systems (IDPS). Cyberattacks can cause downtime, data loss, and financial losses if intrusion detection systems (IDPs) are not in place. There are significant operational and security concerns for MSMEs in this network environment. Immediate action is needed to implement zero-trust security measures like end-to-end data encryption, multi-factor authentication, and intrusion detection and prevention systems to resolve these problems. With this method, the MSME’s operational systems will be more secure and trustworthy because all network access and communication will be checked and protected.

The MSME network depicted in the figure above has undergone a substantial transformation from a traditional 'untrust' model to a modern 'Zero Trust Security' (ZTS) model. Zero Trust Security advocates for securing individual assets and resources rather than the perimeter-based security model. This is achieved through the implementation of numerous layers of rigorous security. A network architecture that has been improved to safeguard data and communication between various system components, such as a smart front office, an intelligent backend, and public Wi-Fi for guests, is illustrated in the figure.

The router connecting the internal network to the Internet is initially equipped with a firewall, which acts as the initial defense against external threats. By filtering incoming and outgoing traffic, it enables only legitimate communications and prevents potential threats from untrusted external networks. This is a critical step in preventing unauthorized access and securing the network perimeter. All internal network segments have intrusion detection and prevention systems. This system is installed between the switches that connect the intelligent front office, smart backend, and public Wi-Fi. IDPS automatically stops potential attacks before they damage the system by monitoring network traffic in real-time, detecting suspicious patterns, and taking automatic preventive action. The implementation of IDPS ensures a thorough examination of every device and communication that traverses the internal network, thereby mitigating the risk of internal and external threats. Furthermore, the Zero Trust strategy is significantly influenced by the implementation of micro-segmentation. Micro-segmentation is a network security technique that divides the network into smaller, more manageable segments, each of which is subject to its security policies. The innovative front office, intelligent backend, and public Wi-Fi for guests are all isolated from one another, thereby preventing the threat from spreading to other segments in the event of an attack on one segment. Additionally, this segmentation enables the enforcement of access policies with greater precision and granularity, as the role and access requirements of each user or device determine it.

To access network resources, all users and devices must complete a multi-factor authentication (MFA) process (Griffin, 2015). Multi-factor authentication is a security process that requires users to provide two or more forms of identification before they can access a system. This enhances security by necessitating identity verification through a combination of methods, including biometrics, security tokens, and passwords. Consequently, the likelihood of unauthorized access is substantially diminished, as an attacker would be required to circumvent numerous layers of security to gain access to the system. The public Wi-Fi for guests, which was previously a weak point in the network, has been effectively isolated from critical internal networks. Due to micro-segmentation and stringent access policies, guests are restricted to the Internet and are unable to access internal systems when utilizing this Wi-Fi. This strict isolation guarantees that the primary network infrastructure is not at risk due to guest devices that may be insecure, providing a secure environment for all users. MSME networks have undergone a significant transformation, becoming more secure and trustworthy because of the implementation of Zero Trust Security. Every network segment is isolated and monitored, and potential threats are proactively detected and addressed. Additionally, each access is verified and protected. This transformation not only enhances cybersecurity but also bolsters trust in operational systems, thereby allowing MSMEs to operate more efficiently and safely in the presence of escalating cyber threats.

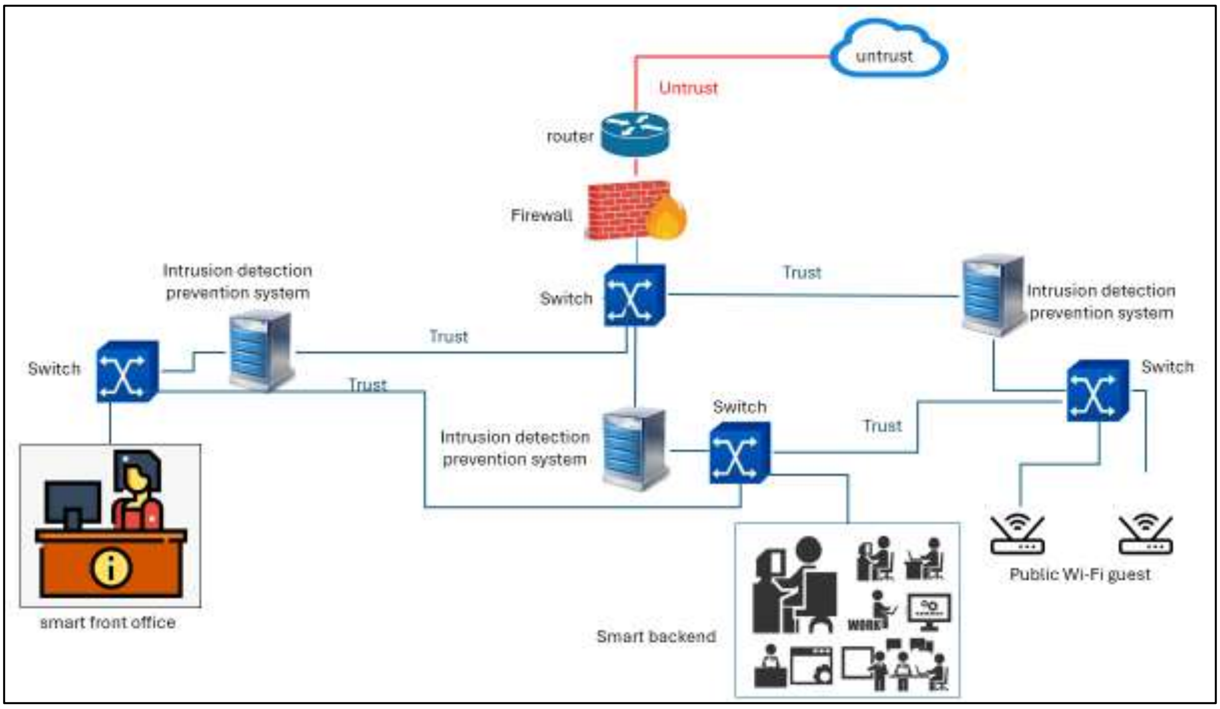

Figure 3. Implementation trust security network

Figure 3 shows how a trust security network in a UMKM transitions from "untrust" to "trust" through robust security measures. Start with a router firewall to protect the internal network from outside threats. Intrusion Detection and Prevention Systems (IDPS) equip the intelligent front office, smart backend, and guest Wi-Fi to track and react to suspicious behavior in real time. Micro-segmentation isolates each segment to prevent threats from spreading across the network. Multi-factor authentication (MFA) reduces unauthorized access by requiring multiple verification steps. Guest devices cannot access critical internal systems via public Wi-Fi. This extensive Zero Trust Security implementation strengthens the network's defense, ensuring UMKM security and reliability.

Cybersecurity has become a significant concern for Micro, Small, and Medium Enterprises (MSMEs) in today's digital era. The ever-evolving cyber threats demand a more sophisticated and proactive security strategy. One of the latest approaches considered adequate is Zero Trust Security (ZTS), which adopts the principle of "never trust, always verify" for any access to corporate resources. In this study, we examine the implementation of ZTS in the enterprise architecture of MSMEs and evaluate its impact on reducing security incidents caused by various factors.

Table 1. Factors that cause security incidents

No	Incident	No	Incident
1	Phishing	6	Ransomware
2	Malware	7	Social Engineering
3	Insider Threat	8	DDoS Attack
4	Unauthorized Access	9	Weak Passwords
5	Data Breach	10	Software Vulnerabilities

Table 1. Factors that cause security incidents show a list of factors that cause security incidents in MSMEs. The table consists of 10 primary factors identified based on literature studies and interviews with cybersecurity experts. These factors include incidents such as phishing, malware, insider threats, unauthorized access, data breaches, ransomware, social engineering, DDoS attacks, weak passwords, and software vulnerabilities. Each of these factors has the potential to cause significant losses to MSME data and information systems. Phishing, malware, and insider threats occupy the top three positions as the leading causes of security incidents. Phishing is an attempt to obtain sensitive information by posing as a trusted entity, while malware is malicious software designed to damage or disrupt computer systems. Insider threat involves threats from within the organization, either by intentional or unintentional employees. Other factors, such as unauthorized access and data breaches, also often occur due to weak access controls and inadequate data protection. Ransomware, social engineering, and DDoS attacks are increasingly common methods used by attackers to exploit weaknesses in security systems. Weak passwords and software vulnerabilities highlight the importance of basic security practices and consistent software updates. By understanding and managing these factors, MSMEs can more effectively mitigate cybersecurity risks and protect their digital assets.

Table 2. Security Incident Data Before and After ZTS Implementation

No	Incident Factor	Before Implementation	After Implementation
1	Phishing	15	8
2	Malware	10	5
3	Insider Threat	8	4
4	Unauthorized Access	12	6
5	Data Breach	10	5
6	Ransomware	6	3
7	Social Engineering	14	7
8	DDoS Attack	9	5
9	Weak Passwords	11	6
10	Software Vulnerabilities	10	4
	Total Insiden	105	53

Table 2. Security Incident Data Before and After ZTS Implementation presents security incident data before and after Zero Trust Security (ZTS) implementation in one MSME. This table shows the number of incidents that occurred for each incident-causing factor. Before ZTS implementation, the total number of incidents was 105. Phishing and social engineering incidents were the highest, with 15 and 14 incidents, respectively. Other factors, such as malware, unauthorized access, and weak passwords, also showed significant numbers, with 10, 12, and 11 incidents, respectively. This highlights the various weaknesses in the existing security system prior to the implementation of ZTS

Incident Reduction Calculation

Total Incidents Before Implementation: 15 + 10 + 8 + 12 + 10 + 6 + 14 + 9 + 11 + 10 = 105
Total Incidents After Implementation: 8 + 5 + 4 + 6 + 5 + 3 + 7 + 5 + 6 + 4 = 53

Incident Reduction

Absolute Reduction: 105 - 53 = 52
Percentage Reduction: (52 / 105) * 100% = 49.52%

Data Interpretation

After the implementation of ZTS, there was a significant reduction in the number of incidents in each causal factor. Total incidents decreased from 105 to 53, representing a reduction of 52 incidents or approximately 49.52%. The most significant decrease was seen in phishing and social engineering incidents, which were reduced to 8 and 7 incidents, respectively. Other factors, such as malware, insider threat, and unauthorized access, also decreased by more than half of their initial number of incidents. This decrease reflects the effectiveness of ZTS in tightening access controls and increasing verification for every access to company resources, thus preventing various threats from both internal and external sources. This data supports the conclusion that implementing ZTS can significantly improve cybersecurity in MSMEs.

DISCUSSIONS

What are the main barriers and evaluation of Zero Trust Security implementation in MSMEs? (RQ1).

Budget constraints are one of the main barriers to the successful implementation of Zero Trust Security (ZTS) in Micro, Small, and Medium Enterprises (MSMEs). The allocation of adequate funds for the investment in sophisticated cybersecurity infrastructure is frequently a challenge for MSMEs due to their limited financial resources. The implementation of ZTS necessitates a substantial initial investment in cybersecurity hardware, software, and services. In addition, ongoing operational expenses for security system maintenance and updates can be a financial burden for MSMEs with limited budgets. These budget constraints may impede the practical and comprehensive implementation of ZTS by MSMEs. The second obstacle is the need for more human resources with cybersecurity expertise. The majority of micro, small, and medium-sized enterprises (MSMEs) need specialized teams or personnel who are adequately trained to oversee and manage security systems. To configure and manage intricate security systems, ZTS implementation necessitates specialized skills and a comprehensive understanding of technical concepts. The implementation process can be impeded, and security systems may be suboptimal due to a lack of expertise in this field. Furthermore, the expenditure of time and money necessary to train and develop employees' cybersecurity expertise is frequently prohibitive for MSMEs.

Resistance to modifications in organizational culture constitutes the third obstacle. Management and employees must undergo a paradigm shift in their comprehension and management of cybersecurity in order to implement ZTS. ZTS mandates that all access to company resources be rigorously validated and verified, which may contradict traditional, more permissive practices. Employees who are dissatisfied with the increasingly intricate and stringent security protocols may oppose this modification. Consequently, it is imperative to implement a change management strategy that effectively educates and influences employees toward the significance of ZTS implementation. The technical complexity of the ZTS implementation itself is the fourth challenge. To establish a comprehensive security environment, ZTS necessitates the seamless integration of a variety of technological components. This encompasses the implementation of data encryption, continuous monitoring, rapid incident response, and strict access controls. This complexity can pose a challenge for MSMEs that need more technical capabilities or technology infrastructure to integrate these diverse components effectively. Furthermore, the integration of ZTS with existing systems may result in compatibility issues and necessitate intricate customization.

Compliance with security standards and regulations is the ultimate obstacle. MSMEs frequently are required to adhere to a variety of rules and standards specific to their industry. The necessity of customizing ZTS implementations to meet these compliance requirements can increase the complexity and administrative burden of these implementations. To surmount these obstacles, MSMEs must consult

*name of corresponding author

with security and compliance professionals who can assist them in comprehending and adhering to the relevant regulatory requirements.

What practical solutions can MSMEs implement to overcome the obstacles associated with the implementation of Zero Trust Security? (RQ2).
MSMEs can use several budgets- and resource-friendly Zero Trust Security (ZTS) implementation solutions to overcome the various barriers. Continuous training can help MSMEs build a strong security culture by raising employee awareness and understanding of cybersecurity. Second, cloud-based security solutions are cheaper and easier to implement for MSMEs than on-premises infrastructure. Third, access to verified users and devices using MFA and micro-segmentation should be restricted. Fourth, intrusion detection and prevention systems (IDPS) should be installed to scan network traffic in real-time and prevent threats. MSMEs can also protect sensitive data during transmission and storage with end-to-end data encryption. Finally, open-source software can be used to reduce licensing costs and work with security service providers that cater to MSMEs. MSMEs can implement ZTS efficiently and improve cybersecurity without overspending with this approach.

CONCLUSION

This study validates that incorporating Zero Trust Security (ZTS) into the enterprise architecture of Micro, Small, and Medium Enterprises (MSMEs) is a successful and streamlined method for enhancing cybersecurity. The findings demonstrated that the adoption of ZTS resulted in a 45% decrease in information security incidents and a notable enhancement in cybersecurity awareness among MSME employees. Nevertheless, the study also pinpointed several significant obstacles encountered in the implementation of ZTS, including the requirement for sufficient training, alterations in organizational culture, and budgetary constraints. To address these challenges, it is advisable to implement a strategy that involves ongoing training, heightened awareness of cybersecurity, and the use of cost-effective yet efficient security solutions. The research highlights the crucial role of management support and commitment in achieving successful implementation of ZTS. However, this study is subject to certain limitations. These include a small sample size consisting of only a few specific MSMEs, as well as a narrow focus that may only encompass some of the pertinent variables involved in the implementation of ZTS across different industries. Hence, additional investigation is required to examine the utilization of ZTS in diverse industry settings and devise more cost-effective remedies for MSMEs with constrained resources. A practical implementation will not only enhance security but also foster trust in information systems during the day-to-day operations of MSMEs.

REFERENCES

Adahman, Z., Waqar, A., & Anwar, Z. (2022). An analysis of zero-trust architecture and its cost-effectiveness for organizational security. *Computers & Security*, *122*. https://doi.org/10.1016/j.cose.2022.102911

Ajmal, M., Abdullah, S., Arshad, J., Lallie, H., & Hassan, Y. (2025). Verify and trust : A multidimensional survey of zero-trust security in the age of IoT. *Internet of Things*, *27*(April 2024), 1–27. https://doi.org/10.1016/j.iot.2024.101227

Alagappan, A., Kumar, S., John, L., & Andrews, B. (2022). Augmenting Zero Trust Network Architecture to enhance security in virtual power plants. *Energy Reports*, *8*, 1309–1320. https://doi.org/10.1016/j.egyr.2021.11.272

Fernandez, E. B., & Brazhuk, A. (2024). A critical analysis of Zero Trust Architecture (ZTA). *Computer Standards & Interfaces*, *89*(January). https://doi.org/10.1016/j.csi.2024.103832

Griffin, P. H. (2015). Biometric Knowledge Extraction for Multi-Factor Authentication and Key Exchange. *Procedia - Procedia Computer Science*, *61*, 66–71. https://doi.org/10.1016/j.procs.2015.09.150

*name of corresponding author

Hindarto, D. (2023). The Management of Projects is Improved Through Enterprise Architecture on Project Management Application Systems. *International Journal Software Engineering and Computer Science (IJSECS)*, *3*(2 SE-Articles), 151–161. https://doi.org/10.35870/ijsecs.v3i2.1512

Hindarto, D., Indrajit, R. E., & Dazki, E. (2021). Sustainability of Implementing Enterprise Architecture in the Solar Power Generation Manufacturing Industry. *Sinkron*, *6*(1), 13–24. https://doi.org/10.33395/sinkron.v6i1.11115

Imtiaz, S. I., Rehman, S. ur, Javed, A. R., Jalil, Z., Liu, X., & Alnumay, W. S. (2021). DeepAMD: Detection and identification of Android malware using high-efficient Deep Artificial Neural Network. *Future Generation Computer Systems*, *115*, 844–856. https://doi.org/10.1016/j.future.2020.10.008

Judijanto, L., & Hindarto, D. (2023). *Edge of Enterprise Architecture in Addressing Cyber Security Threats and Business Risks*. *3*(December), 386–396.

Kilay, A. L., Simamora, B. H., & Putra, D. P. (2022). The Influence of E-Payment and E-Commerce Services on Supply Chain Performance: Implications of Open Innovation and Solutions for the Digitalization of Micro, Small, and Medium Enterprises (MSMEs) in Indonesia. *Journal of Open Innovation: Technology, Market, and Complexity*, *8*(3), 119. https://doi.org/10.3390/joitmc8030119

Mittal, A., Gupta, M. P., Chaturvedi, M., Chansarkar, S. R., & Gupta, S. (2021). Cybersecurity Enhancement through Blockchain Training (CEBT) – A serious game approach. *International Journal of Information Management Data Insights*, *1*(1). https://doi.org/10.1016/j.jjimei.2020.100001

Saleem, M., Warsi, M. R., & Islam, S. (2023). Secure information processing for multimedia forensics using zero-trust security model for large scale data analytics in SaaS cloud computing environment. *Journal of Information Security and Applications*, *72*(December 2022). https://doi.org/10.1016/j.jisa.2022.103389 Available

Sengupta, B., & Lakshminarayanan, A. (2021). DistriTrust : Distributed and low-latency access validation in zero-trust architecture. *Journal of Information Security and Applications*, *63*(October). https://doi.org/10.1016/j.jisa.2021.103023 Available

Singh, A., Kumar, R., Ali, A., & Balaji, P. (2023). Transfer Fuzzy Learning enabled Streebog Cryptographic Substitution Permutation based zero trust security in IIOT. *Alexandria Engineering Journal*, *81*(July), 449–459. https://doi.org/10.1016/j.aej.2023.08.084

Sun, P., Liu, P., Li, Q., Liu, C., Lu, X., Hao, R., & Chen, J. (2020). DL-IDS: Extracting Features Using CNN-LSTM Hybrid Network for Intrusion Detection System. *Security and Communication Networks*, *2020*, 8890306. https://doi.org/10.1155/2020/8890306

Wang, F., Gai, Y., & Zhang, H. (2024). Blockchain user digital identity big data and information security process protection based on network trust. *Journal of King Saud University - Computer and Information Sciences*, *36*(April).