Journal of Theoretical and Applied Information Technology
15th April 2025. Vol.103. No.7
© Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ZERO TRUST ARCHITECTURE WITH SINGLE SIGN ON METHOD ON ENHANCE SECURITY AND USER ACTIVITY MONITORING

KAMALUDIN NUR[1], BENFANO SOEWITO[2]

[12]Department of Computer Science, BINUS Graduate Program-Master of Computer Science, Bina Nusantara University, Jakarta, Indonesia

E-mail: [1]kamaludin.nur@binus.ac.id, [2]bsoewito@binus.edu

ABSTRACT

The rise of cyberattacks due to weak internet access controls has led to increased data breaches and financial losses. This study proposes the integration of Zero Trust Architecture (ZTA) with Single Sign-On (SSO) to enhance network security while simplifying user authentication and monitoring. ZTA enforces strict verification for each access request, mitigating risks from phishing and brute force attacks. Despite its advantages, ZTA presents challenges, particularly in integrating with legacy systems and managing infrastructure complexity. This research evaluates ZTA implementation through network topology analysis, identity-based access control, segmentation, and Multi-Factor Authentication (MFA) to prevent unauthorized access. The integration of SSO improves authentication efficiency while maintaining security. Authentication performance is a critical factor in ZTA adoption. The results confirm that integrating ZTA with SSO facilitates real-time monitoring, enhances rapid threat response, and improves overall network security, providing a viable cybersecurity solution for modern organizations. Furthermore, this research evaluates authentication response time, aiming for an optimal range of 30-40 MS to ensure system efficiency and security. The study records an authentication time of 30.03 ms, network latency of 29.28 MS, and real-time notifications to IT staff delivered within 2.66 seconds. In live trials with a 200 Mbps bandwidth, the system detected 11 anomalies within 3 hours, demonstrating its effectiveness.

Keywords: *Zero Trust Architecture, Single Sign-On (SSO), Authentication, Network Security, User Activity Monitoring*

1. INTRODUCTION

This In the era of rapid digital transformation, protecting information system and sensitive data has become an increasingly complex challenge. The growing sophistication and frequency of cyberattacks have compelled organizations to adopt more adaptive and resilient security approaches. Effective cybersecurity requires a holistic strategy encompassing policies, technology and operational practices to establish comprehensive security framework. By implementing such an approach, organizations can ensure that data the integrity, confidentiality, and availability remain safeguarded [1][2].

Network security is a fundamental aspect of cybersecurity, encompassing policies and practices aimed at preventing, detecting and mitigating unauthorized access, misuse, modification or disruption of computer networks and associated resources [3]. To achieve an optimal level of security, organizations can implement risk-based controls and enhance monitoring mechanisms to strengthen detection and response capabilities against various threats [4].

On of the most widely used authentication methods in information security is password-based authentication, which requires users to enter credentials, including a username and password, to gain access to a system. Although this method is relatively easy to implement, it has several security vulnerability, such as susceptibility to phishing attacks, brute force attacks and the use of weak or easily guessable passwords [5]. Moreover, as users accumulate multiple digital accounts, managing and remembering numerous passwords becomes increasingly challenging. This often leads to poor security practices, including password reuse or insecure credential storage [6].

The absence of robust verification and authentication mechanisms significantly heightens the risk of cyberattacks. As malicious actors can exploit vulnerabilities within authentication systems to gain unauthorized access and engage in harmful activities. Consequently, the implementation of stronger authentication mechanisms is essential to

mitigate security risks and enhance system resilience against cyber threats [7].

The Zero Trust Architecture (ZTA) has emerged as a widely adopted approach among organization to strengthen authentication security. ZTA mandates the enforcement of stringent authentication, authorization, and data encryption across all access layers. The principle of least privilege ensures that users are granted only the minimum access necessary to perform their tasks. Furthermore, organizations must implement continues monitoring to detect and respond to suspicious activities in real-time [8].

In this context, the NIST 800-207 framework, which outlines the Zero Trust Architecture (ZTA), introduces a modern security paradigm that eliminates implicit trust assumptions inherent in traditional network model. NIST 800-207 underscores the principle of "Never Trust, Always Verify", mandating that every access request undergo continuous verification without exception [8]. While the Zero Trust approach enhances security compared to traditional perimeter-based security models, its implementation poses several challenges [9].

One of the main challenges in adopting Zero Trust is the complexity of IT infrastructure, which consists of numerous interconnected devices in a dynamic business environment. This creates difficulties in integrating security systems, managing identities and access, and monitoring user and device activities [10]. Furthermore, transitioning to Zero Trust can disrupt business processes, increase implementation costs, and cause dissatisfaction among end users [11].

The successful implementation of Zero Trust Architecture (ZTA) is significantly influenced by various factors, including national culture, organizational culture and information security practices. Studies indicate a positive correlation between cultural factors and the adoption of the Zero Trust model, where organizations that integrate cultural aspects into their cybersecurity strategies tend to implement ZTA more effectively [12].

Extensive research has been conducted on the implementation of Zero Trust Architecture across various sectors, including government and private enterprises, to enhance information system security against increasingly complex cyber threats. A study conducted by Bimo Yuliato, Muhammad Quraisy, Anggriyana Daulay, and Ayu Puspitasari demonstrated that Promox serves as the primary virtualization platform in Zero Trust Security implementation, ensuring that each access request undergoes strict verification before authorization is granted. Furthermore, the integration of Cloudflare strengthens server infrastructure security by implementation a Web Application Firewall (WAF), Distributed Denial of Service (DDOS) protection, and stringent access control mechanisms, thereby enhancing system resilience against evolving cyber threats [13].

To optimize authentication mechanisms within the Zero Trust framework, the implementation of Single Sign-On (SSO) serves as a practical approach to facilitate user access to multiple applications and systems using a single set of credentials. This approach mitigates the complexity of password management while enhancing user convenience [14]. However, to achieve a higher level of security, SSO authentication must be reinforced with additional security measures, such as Multi Factor Authentication (MFA), to strengthen system resilience against potential cyberattacks [15].

As an integral component of Zero Trust implementation, organizations are required to establish robust identity, credential, and access management systems, along with an integrated asset management framework. This encompasses the deployment of multi factor authentication to safeguard access to organizational resources, thereby ensuring that only authorized users can access sensitive information [16].

Previous studies have extensively discussed network architecture aspects or identity-based authentication without considering integration with Single Sign-On (SSO) mechanisms. On the other hand, research on SSO has primarily focused on enhancing user experience without evaluating the security risks arising from single access mechanisms. Studies by Bimo Yulianto, Muhammad Quraisy, Anggriyana Daulay, and Ayu Puspitasari have highlighted the benefits of Zero Trust Architecture (ZTA) in strengthening system security. However, no comprehensive approach has been proposed to integrate ZTA and SSO into a balanced framework that ensures both authentication efficiency and the principle of least privilege in cybersecurity. Therefore, a gap remains in the literature regarding the combination of these approaches in real-world operational contexts.

The increasing complexity of cybersecurity threats necessitates the adoption of more robust authentication mechanisms. Zero Trust Architecture (ZTA) eliminates implicit trust by enforcing continuous verification, thereby enhancing security. However, integrating ZTA with Single Sign-On (SSO) presents significant challenges, particularly in terms of authentication latency, system

compatibility, and user experience. While prior research has explored ZTA and SSO separately, there is a lack of comprehensive studies examining their combined implementation and its impact on both security and system efficiency. To address this gap, this study aims to analyze the effect of ZTA-SSO integration on authentication latency, compare the effectiveness of Zero Trust-based security models with traditional security systems in mitigating cyber threats, and identify optimal integration mechanisms that maintain compatibility with legacy infrastructure.

To address these challenges, this study is guided by the following research questions: (1) How does the integration of ZTA with SSO impact authentication latency and overall system efficiency? (2) How does a Zero Trust-based authentication model compare with traditional security models in mitigating cyber threats? (3) What are the optimal mechanisms for integrating ZTA and SSO while ensuring compatibility with legacy infrastructure?. By addressing these research questions, this study provides empirical insights and a structured framework for organizations seeking to implement a Zero Trust authentication model that balances security, efficiency, and user experience.

To address the gap in the literature on ZTA-SSO integration, this study adopts an experimental approach to evaluate the impact of ZTA implementation on various authentication metrics. The evaluation includes an analysis of authentication time, network latency, anomaly detection efficiency, and system response in real-world operational environments. Additionally, this study develops a real-time user activity monitoring system designed to detect anomalies and automatically notify the IT team, enabling more responsive threat mitigation.

Compared to previous studies that primarily emphasize the theoretical benefits of Zero Trust Architecture (ZTA), this research provides an empirical analysis of its real-world performance, systematically comparing Zero Trust-based security models with traditional security systems. Unlike prior work that discusses ZTA in conceptual terms, this study quantifies the trade-offs between enhanced security enforcement and authentication latency, offering data-driven insights for practical adoption.

Furthermore, this study proposes a novel adaptive ZTA model that integrates seamlessly with legacy systems, addressing a critical gap in previous research where ZTA implementation often disregards compatibility with existing infrastructures. By identifying key security-performance thresholds and evaluating implementation challenges, this research introduces best practices for organizations transitioning towards Zero Trust. These best practices include incremental deployment strategies, optimized authentication workflows, and risk-based policy enforcement, ensuring organizations can adopt ZTA without excessive operational disruptions. In doing so, this study contributes not just incremental knowledge but also actionable recommendations for scalable and efficient Zero Trust deployment in enterprise environments.

While this study contributes by providing best practice guidelines for organizations seeking to adopt Zero Trust Architecture (ZTA), several limitations should be considered. One of the main constraints is that the testing environment is limited to specific scenarios, which may not fully represent the complexity of real-world operational conditions. Additionally, the experimental approach requires further expansion through long-term studies to understand the sustained impact of ZTA-SSO integration on system security. Therefore, future research can explore further optimization of anomaly detection algorithms and the effectiveness of dynamic access control mechanisms within the Zero Trust architecture.

2. RELATED WORKS

With the advancement of Internet of Things (IoT), Cloud Computing, and Big Data technologies, the integration between medical systems and information technology has become increasingly interconnected, leading to a heightened risk of network security threats. A study conducted by Zhiqiang Wang, Xinyue Yu, Peiyang Xue, Yunhan Qu, and Lei Ju [17] emphasizes the implementation of a Zero Trust security system in medical information systems through the development of a dynamic access control module based on Role-Based Access Control (RBAC). This module incorporates the calculation of user behavior risk scores and trust levels to ensure secure access to medical data while dynamically assessing user behavior risk and trustworthiness.

Furthermore, the study conducted by Muhammad Mujib, Riri Fitri Sari (supervisor), Kalamullah Ramli, Yohan Suryanto, and Ruki Harwahyu [18] developed a Zero Trust security model based on micro-segmentation to mitigate internal attacks on internet packet traffic. This model utilizes small network segments responsible for transmitting data packets in isolation, which were subsequently tested through a testbed simulation using Cisco Application Centric Infrastructure. The system performance evaluation includes the

measurement of Round Trip Time (RTT) and the effectiveness in preventing port scanning and distributed denial-of-service (DDoS) attacks.

Meanwhile, Amrit Niraula [19] expands the concept of Zero Trust Architecture (ZTA) to protect enterprise networks and resources by implementing Ring Oscillator Physical Unclonable Functions (ROPUFs). This technology enables the establishment of a Zero Trust-based peer-to-peer communication network by leveraging blockchain infrastructure and decentralized storage through the InterPlanetary File System (IPFS). By utilizing file hashing mechanisms obtained from IPFS, any data modifications within the system are documented in activity logs accessible to all users, thereby enhancing transparency and information security.

Additionally, the study conducted by Javier Jose Diaz Rivera, Afaq Muhammad, and Wang-Cheol Song [20] highlights the effectiveness of the Distributed Authentication Mechanism (DAM) based on blockchain in addressing the weaknesses of centralized authentication systems. This model implements Zero Knowledge Proofs (ZKP) and decentralized authentication to eliminate the risk of Single Point of Failure, which is commonly found in centralized authorization systems. In the DAM model, the authentication process is distributed across multiple validator nodes within the blockchain network, where each node functions as an authenticator that collectively generates and verifies user authentication. Consequently, this system offers enhanced security against data manipulation threats and unauthorized access.

3. METHODOLOGY

The existing intenet access management mechanism remains perimeter based, wherein user authentication is conducted only once at the point of network entry. Upon successfully authenticated, users are granted broad access to system resources without subsequent validation. As depicted in Figure 1, this model inherently assumes that all entities within the internal network are highly trustworthy, thereby negating the necessity for continuous authentication post initial access. Furthermore, the implemented access control policies remain static and have yet to incorporate a dynamic, risk based evaluation approach. Consequently, this increases the potential risk of unauthorized access exploitation, particularly by malicious threats.

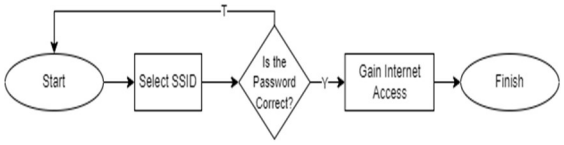

Figure 1: Current Internet Access

To enhance internet access security, the Zero Trust Architecture (ZTA) approach will be implemented by adopting the least privilege access model and identity based access control with dynamic policies. In this design, as illustrated in Figure 2, internet resources can only be accessed by verified users who comply with the established security policies. The system manages access rights by implementing Single Sign-On (SSO) authentication integrated with application services and Gmail, thereby improving authentication efficiency and security. Furthermore, the system periodically evaluates each access request to ensure compliance with applicable security policies, enabling more adaptive and proactive risk mitigation. If a security policy violation is detected, the system will block the website and send an email notification to the IT officer.

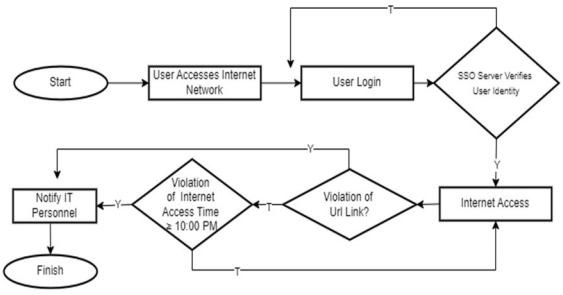

Figure 2: Proposed Internet Access

The system automatically collects and analyzes user activity data to detect anomalies in behavioral patterns. If suspicious or deciant activity is identified, the system sends an alert notification via email to IT personnel for further investigation, subsequently, the system records the details of the anomaly incident in the incident logging system as part of the documentation and evaluation process for information security. This process is continuously repeated to ensure ongoing monitoring of user activities, as illustrated in Figure 3.

Journal of Theoretical and Applied Information Technology
15th April 2025. Vol.103. No.7
© Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

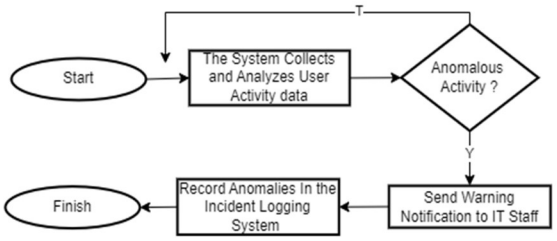

Figure 3: Monitoring User Activity

To support the implemtation of a Zero Trust Architecture integrated with external services such as application APIs, Gmail, and user activity monitoring systems, a local network design must incorporate Zero Trust security protocols and robust authentication mechanisms, as illustrated in Figure 4. The firewall functions as a control mechanism and filters data traffic to prevent external threats, while the proxy server acts as an intermediary between users and the internet ti enhance security and filter malicious content. Within the local network infrastructure, Cisco switches are used to connect user devices, such as PCs and access points, with each switch assigned a unique IP address to enable efficient traffic management. Users can connect to the network via wired or wireless connections, providing flexible access and improving communication efficiency within the system.

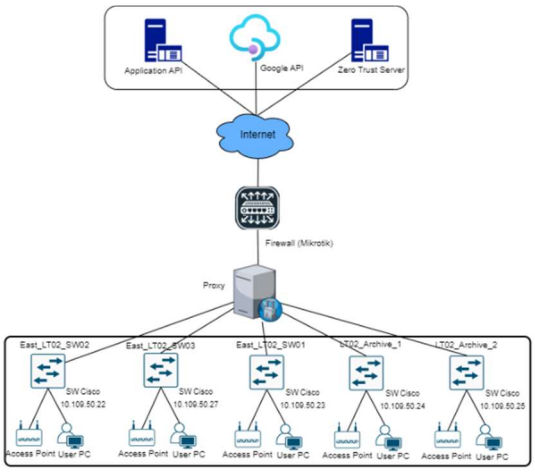

Figure 4: Network Topologi

The next step involves implementing the Zero Trust model within the network, as illustrated in Figure 5, designed to ensure user identity validation, device monitoring, and data traffic management through proxy and firewall mechanisms. Each stage of this process contributes to enhanced security by enabling comprehensive logging and analysis, thereby supporting more effective detection and response to potential security incidents. Furthermore, this approach ensures that every access request made by users is validated based on predefined policies to guarantee comprehensive protection of system resources and prevent unauthorized access.

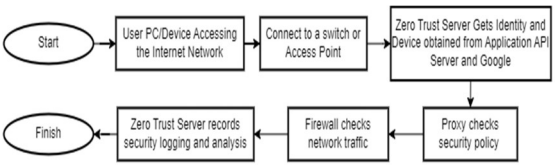

Figure 5: ZTA Network Authentication Process

In application design, it is essential to establish a data flow that systematically represents the relationships between entities within a network while ensuring that verification and authentication processes operate optimally without compromising user experience. This approach aims to minimiza operational system contraints while maintanining security through the implementation of effective and efficient authentication mechanisms. By utilizing a context diagram, as illustrated in Figure 5, the interactions betwwn key components in the implementation of a Zero Trust Architecture (ZTA) with the Single Sign-On (SSO) method can be analyzed more comprehensively, enabling a deeper understanding of the system workflow.

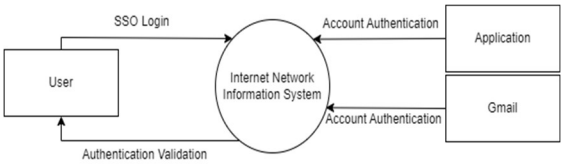

Figure 6: Zero Trust Network Context Diagram

After analyzing the context diagram that illustrates the authentication process flow, the Use Case model can be utilized to systematically describe the implementation of this concept. Figure 7, demostrates how users interact with the system and how Zero Trust Architecture (ZTA) implements the Single Sign-On (SSO) method to securely and effectively manage access and authentication. In the Use Case model, each stage represents a series of interactions between the user and the system to services or applications with an added layer of security protection.

Journal of Theoretical and Applied Information Technology
15th April 2025. Vol.103. No.7
© Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

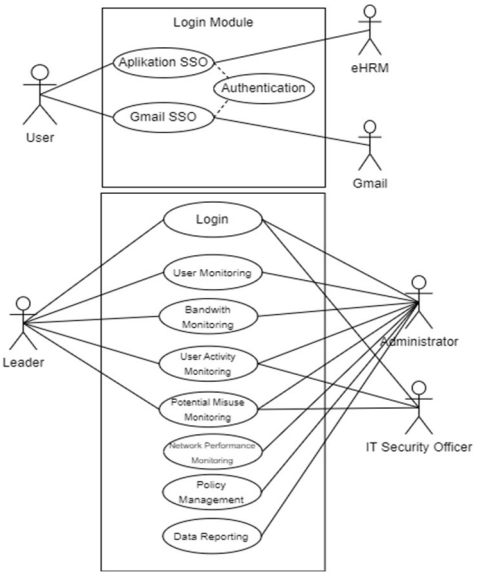

Figure 7: Use Case Diagram User

To support the success of this research, an intuitive interface design that aligns with the organization's needs is required. The interface design of this system is categorized into two, namely for general users and another for administrators. The Zero Trust based internet network portal is designed with the principle of ease of access for users. The portal provides two authentication buttons, each designated for general users and organizational users. This mechanism ensures that users can access internet services through the implemented security policies. The visualization of the Internet network portal design is presented in Figure 8.

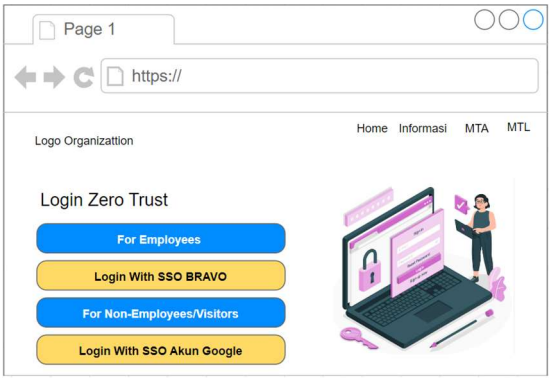

Figure 8: Internet Network Portal Design

After completing the authentication process through the login form, the system will automatically redirect users to an information page that displays connection status and data usage within the Zero Trust environment. On this page, users can obtain essential information such as the IP address in use, connection time, and data usage status. Additionally, the system provides an option to log out easily via the Log Off button, ensuring that user access remains controlled and aligned with Zero Trust principles. The visualization of this information page is presented in Fugure 9.

Figure 9: Information Page Design

Figure 10, illustrates the design of a dashboard specifically developed for administrators as a comprehensive and intuitive interface for security management and monitoring. This dashboard functions as a central control hub, enabling administrators to monitor user activities, manage access rights, and conduct thorough security data analysis. Additionally, the dashboard provides real-time access to security reports and activity logs, facilitating data-driven decision-making for risk mitigation and the implementation of both preventive and corrective actions. The features incorporated into this dashboard support the implementation of the Zero Trust Architecture (ZTA).

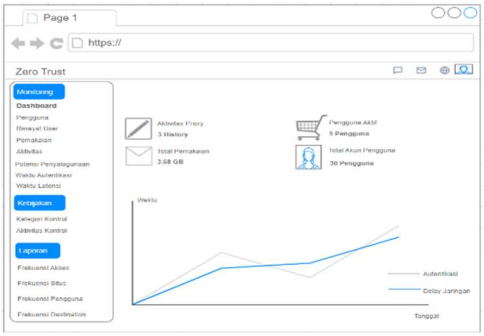

Figure 10. Dashboard Design

This analysis report on internet user activity consists of four main aspects presented in the reporting menu: Access Frequency, Frequently Visited Sites, Users, and Destination. Each aspect serves a specific analytical function in identifying user internet usage patterns, as outlined below:

1. Access Frequency plays a crucial role in analyzing the intensity of internet usage within a specific period, such as during the

morning or afternoon. This analysis includes determining the number of active users within a given timeframe and identifying peak hours with the highest access rates.

2. Frequently Visited Sites function to identify the most frequently accessed URLs or domains by users, providing insights into user preferences and dominant access patterns.
3. Users are analyzed to assess the volume of data traffic consumed by individual users over a specific period, enabling evaluations of network capacity utilization and the potential for excessive system load.
4. Destination serves the primary function of detecting the number and patterns of anomalous domains accessed by users, which may indicate potential security threats or suspicious activities within the network.

With this report, the monitoring and analysis of internet user activities can be conducted more systematically, enabling data-driven decision-making in network management and early detection of potential cybersecurity risks.

To measure the effectiveness of the developed system, testing and performance monitoring are conducted to assess its efficiency, security, and reliability. The evaluation of the Zero Trust architecture implementation using the Single Sign-On method includes an analysis of user authentication time when accessing the internet and the measurement of network latency during data transfer processes. Additionally, the developed application serves as a tool for monitoring user activities and evaluating system performance.

Testing was conducted on 30 (thirty) users to compare the results before and after the implementation of the Single Sign-On method in the Zero Trust architecture. The testing results, presented in Table 1, provide system performance evaluation metrics based on several key parameters, including authentication time, network latency, anomaly notification delivery time, and the number of security policy violations.

Table 1: Efficiency Testing and Evaluation Results

Test Type	Testing Tool	Evaluation Parameter
Authentication Time	Custom scripts	Average authentication time
Network Delay Time	Custom scripts	Average network delay time
Anomaly Notification Delivery	Custom scripts	Average anomaly notification delivery time
Policy Violation Count	Custom scripts	Average anomaly detection time

In addition to performance metric-based evaluation, a user perception analysis was also conducted through a survey on the implementation of Single Sign-On within the Zero Trust framework. Respondents were asked to provide assessments based on their experiences after system implementation, focusing on various security and efficiency aspects, including support for Zero Trust principles, authentication security, user access monitoring, policy-based access control, identity management, as well as efficiency in access monitoring and management.

The survey results were analyzed to gain insights into the perceived changes experienced by users in their work environment while also evaluating the effectiveness of the system in supporting Zero Trust security policies. This analysis serves as a foundation for decision-making regarding future system optimization.

4. RESULT

The research findings indicate that the implementation of Single Sign-On (SSO) within the Zero Trust Architecture (ZTA) framework not only serves as an authentication mechanism but also substantially enhances system resilience against security threats. The application of Zero Trust principles, which emphasize that no entity is automatically trusted, whether inside or outside the network, contributes to improved security without compromising the user experience.

System performance testing was conducted by measuring the average authentication time and network latency using a custom script to ensure system reliability. The test results, presented in Table 2, indicate that authentication in the Zero Trust system exhibits a longer response time compared to the Non-Zero Trust system. This is due to the multi-layered validation process designed to enhance security. In the Non-Zero Trust system, authentication is performed in a more straightforward manner, resulting in a faster response time of 18.1 ms. Conversely, the Zero Trust system requires additional authentication time and latency, amounting to 30.03 ms, which is

significantly longer than that of the Non-Zero Trust system.

Although there is an increase in authentication time, the security benefits gained from the implementation of Zero Trust Architecture are significantly more substantial, particularly in protecting sensitive data from increasingly complex cyber threats.

Table 2: Authentication Time

User	Bravo		Gmail	
	ZT	Non ZT	ZT	Non ZT
1	19	11	31	22
2	17	11	38	25
3	21	11	42	14
4	21	14	20	14
5	27	18	43	20
6	37	17	35	27
7	16	10	25	16
8	29	11	39	26
9	25	17	27	13
10	31	20	29	12
11	38	16	40	25
12	40	14	37	15
13	33	16	23	16
14	38	18	31	12
15	44	21	24	14
16	23	16	31	17
17	26	37	30	12
18	35	15	28	15
19	27	19	40	20
20	39	23	42	36
21	34	30	31	23
22	17	15	29	16
23	22	14	24	20
24	22	14	34	19
25	35	20	14	15
26	33	20	13	9
27	45	25	14	8
28	24	18	46	31
29	27	21	34	16
30	30	24	33	22
$\bar{x}$	**29.17**	**17.87**	**30.90**	**18.33**

Table 3 illustrates that network latency plays a crucial role in determining data transfer efficiency and directly impacts the user experience. In the Zero Trust security architecture, the multi-layer validation process requires each data packet to be thoroughly inspected before reaching its destination, resulting in an increase in the average latency time to 29.29 ms. In contrast, the Non-Zero Trust system exhibits lower latency at 14.24 ms due to a simpler validation mechanism. Although the Zero Trust system introduces higher latency, the additional security layers provide more optimal protection for sensitive data, thereby enhancing the system's resilience against cyber threats.

Table 3: Latency Time

User	Bravo		Gmail	
	ZT	Non ZT	ZT	Non ZT
1	35	8	33	11
2	18	11	38	8
3	22	13	24	8
4	22	11	26	12
5	17	12	42	21
6	51	21	30	11
7	20	13	14	12
8	24	13	32	16
9	38	15	27	11
10	32	11	25	35
11	32	10	28	23
12	41	16	39	12
13	31	13	22	12
14	38	11	29	10
15	43	21	24	11
16	29	12	29	14
17	27	12	33	12
18	23	10	27	10
19	25	11	32	16
20	44	13	52	16
21	32	21	35	15
22	8	4	48	11
23	26	10	32	20
24	21	11	31	13
25	35	16	12	13
26	20	11	13	7
27	26	23	14	8
28	22	13	39	39

29	27	21	37	21
30	31	27	30	12
x̄	**28.67**	**13.80**	**29.90**	**14.67**

Table 4 presents the dataset obtained during the live trial period, recording the log data generated by the system. The data indicate that the system successfully sent email notifications to IT personnel with an average delivery time of 2.66 seconds. This average was derived by dividing the total delivery duration by the number of analyzed log entries. These results demonstrate the system's rapid response in issuing alerts related to detected policy violations or anomalies.

Table 4: Average anomaly notification delivery time

Notification Number	Duration	Total Duration	Average Durasi
1-20	15.20	532.46	2.66
21-40	78.46		
41-60	42.81		
61-80	31.15		
81-100	47.53		
101-120	33.83		
121-140	16.57		
141-160	220.71		
161-180	17.09		
181-200	29.12		

In the anomaly detection process, an analysis was conducted on 200 detections from the log dataset. Identical anomalies were consolidated into a single instance, resulting in a total of 11 anomalies requiring further action. The data testing was performed over a three-hour period, with the anomaly detection results recorded in Table 5. The table presents the distribution of detection times based on hours and minutes, along with the total number of detected anomalies for each hour.

Table 5: Average anomaly detection time

Domain	Hours			Total
	8	9	10	
9469210.fls.doubleclick.net	2			2
ad.doubleclick.net	2			2
cc-api-data.adobe.io	1	2		3
dit.whatsapp.net	65	59	6	130
js.monitor.azure.com		14	8	22
locate.measurementlab.net		1		1
sadownload.mcafee.com	4	21		25
sb.scorecardresearch.com	4	1		5
sstats.adobe.com		2		2
stats.g.doubleclick.net	4			4
td.doubleclick.net	4			4
Grand Total	86	100	14	200

In addition to technical testing, a user perception survey was conducted to understand users' perspectives on the changes occurring in the work environment, particularly regarding the implementation of Single Sign-On (SSO) in supporting the Zero Trust policy. This survey involved 30 respondents who were asked to assess the impact of Single Sign-On. The survey results, presented in Figure 10, indicate that the average score across all survey categories was 4.25. This score suggests that the implementation of SSO has had a positive impact in supporting the Zero Trust policy within the work environment.

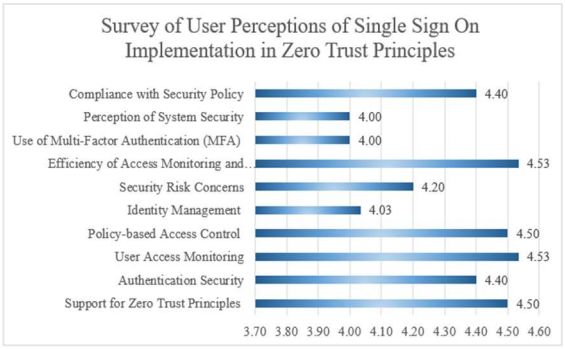

Figure 11: User Perception Survey

Overall, the implementation of Single Sign-On (SSO) has significantly contributed to supporting the Zero Trust policy, particularly in the aspects of access monitoring and management. However, improvements are required in identity management and the implementation of Multi-Factor Authentication (MFA) to ensure a higher level of security and enhance user trust in the system.

This study emphasizes that data analysis plays a strategic role in establishing a solid foundation for policy decision-making based on the Zero Trust concept. The primary contribution of this research lies not only in enhancing system security but also in strengthening the effectiveness of user activity monitoring. Consequently, these findings have implications for optimizing governance that is more transparent, measurable, and controlled, thereby supporting the implementation of adaptive

Journal of Theoretical and Applied Information Technology
15th April 2025. Vol.103. No.7
© Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

and sustainable security principles within information systems. The key findings of this research are as follows :

1. Access Frequency Analysis enables organizations to identify detailed patterns of user activity, as illustrated in Figure 12. The analysis results reveal variations in access patterns, with significant activity peaks observed on January 16 and 17, 2025. These findings provide predictive insights into critical periods, particularly during the morning and afternoon hours, when system infrastructure experiences high loads. Additionally, comparing normal access patterns with actual access behavior allows for the detection of anomalies, such as unusual activity spikes, which may serve as indicators of potential cyber threats. By leveraging this data, organizations can formulate dynamic time-based access restrictions to enhance system resilience and efficiency.

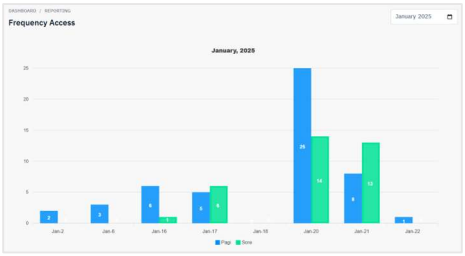

Figure 12: Access Frequency Chart

2. Website Access Patterns analyzed in Figure 13 illustrate access trends in January 2025, with Google dominating at 2,226 accesses, followed by Dropbox with 296 accesses, and YouTube with 181 accesses. Based on this data, the organization can establish policies recognizing the high usage of web services such as Google for productivity and Dropbox for collaboration. However, the high volume of access to certain sites may indicate potential anomalies, including unusual activity or unauthorized access misuse. Additionally, security risks such as data leakage, phishing, and unauthorized access must be anticipated and mitigated through proactive security measures.

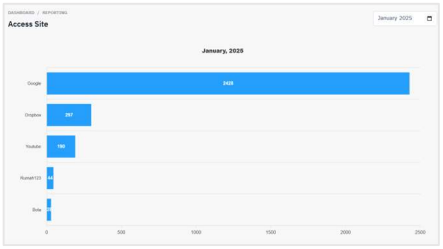

Figure 13: Graph of Access Sites

3. Based on the analysis in Figure 14, organizations can implement structured policies to efficiently manage access and bandwidth usage. Users with high access and bandwidth consumption require optimal allocation and continuous monitoring to maintain service performance. High bandwidth with low access should be audited to prevent potential misuse, while valid activities can be accommodated with customized service packages. Users with high access but low bandwidth consumption should be optimized to handle intensive activities without overloading the network. Meanwhile, low activity users need to be evaluated for potential service simplification or additional training. To enhance network management efficiency, the implementation of Quality of Service (QoS) is recommended to prioritize users who provide strategic contributions to the organization.

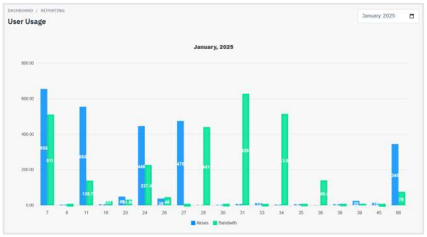

Figure 14: User Internet Usage Chart

4. Figure 15, illustrates network users access activities in January 2025, indicating potential anomalous patterns or suspicious activities, such as dominant access to specific websites or unusual bandwidth consumption. This data can be leveraged to identify users involved in policy violations, thereby assisting in decision-making processes. Possible actions include enhancing real-time monitoring, implementing stricter access controls, and

providing network security training to mitigate potential threats.

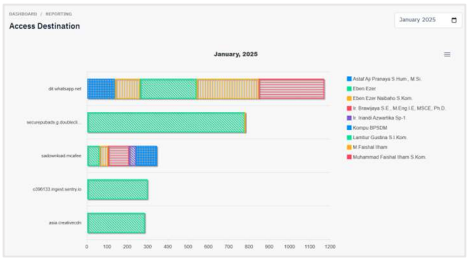

Figure 15: Access Anomaly Destination Chart

5. CUNCLUSION

This study evaluates the implementation of Zero Trust Architecture (ZTA) with Single Sign-On (SSO) to enhance network security and user activity monitoring. The findings indicate that integrating ZTA and SSO improves authentication efficiency and supports real-time anomaly detection. System testing results show an average authentication time of 30.03 MS, network latency of 29.28 MS, and anomaly notification delivery to the IT team within 2.66 seconds. In a test scenario with 200 Mbps bandwidth, the system successfully detected 11 anomalies within three hours, demonstrating its effectiveness in identifying security threats.

As part of our self-evaluation before drawing conclusions, we acknowledge several limitations in this study. The research was conducted on a small scale with only 30 users, making it insufficient to assess the effectiveness of system deployment in large organizations. Additionally, cost analysis was not included, leaving the economic feasibility of the system unverified. Other challenges include the complexity of integrating ZTA with legacy systems and increased latency compared to non-ZTA systems. Furthermore, Multi-Factor Authentication (MFA) requires further optimization to balance security and user convenience.

The key contributions of this study include the development of a Zero Trust-based authentication model integrated with SSO, enhancing both authentication efficiency and network access security. This research also provides a quantitative evaluation of authentication performance and network latency, as well as an analysis of user perceptions regarding SSO implementation within the Zero Trust framework.

For future research, it is recommended to explore strategies for reducing authentication latency without compromising security, such as leveraging artificial intelligence (AI) or authentication caching. Additionally, blockchain technology could be investigated to enhance transparency and security in user access management. Further studies on a larger scale are necessary to assess the system's effectiveness in complex organizations with multi-branch structures or hybrid cloud services.

The findings of this study are expected to serve as a reference for organizations in developing more adaptive and efficient Zero Trust Architecture solutions to address evolving cybersecurity threats.

AUTHOR CONTRIBUTORSHIP

Kamaludin Nur: Conceptualization, Methodology, Software, Formal analysis, Investigation, Resources, Data Curation, Writing – Original Draft, Visualization. Benfano Soewito: Conceptualization, Methodology, Validation, Writing – Review & Editing, Supervision.

DATA AVAILABILITY

To increase the transparency of this paper, the authors have provided data sources. The data is available at the Zenodo Repository, https://doi.org/10.5281/zenodo.15043537 .

REFERENCES:

[1] L. B. Stallings, William, *Computer Security: Principles and Practice (4th Edition)*. 2018. [Daring]. Tersedia pada: https://www.amazon.com/Computer-Security-Principles-Practice-4th/dp/0134794109

[2] D. A. Sudarmadi dan A. J. S. Runturambi, "Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia," *J. Kaji. Strat. Ketahanan Nas.*, vol. 2, no. 2, hal. 157–178, 2019, doi: 10.7454/jkskn.v2i2.10028.

[3] Y. Afek, A. Bremler-Barr, dan A. Noy, "Eradicating Attacks on the Internal Network with Internal Network Policy," 2019, [Daring]. Tersedia pada: http://arxiv.org/abs/1910.00975

[4] Gartner, "Top Security and Risk Management Trends 2021," Gartner. [Daring]. Tersedia pada: https://www.gartner.com/en/doc/738210-top-security-and-risk-management-trends-2021

[5] M. Security, "what is authentication," Microsoft Security. [Daring]. Tersedia pada: https://www.microsoft.com/id-id/security/business/security-101/what-is-authentication

[6] J. Blocki, S. Komanduri, L. Cranor, dan A. Datta, "Spaced Repetition and Mnemonics

Enable Recall of Multiple Strong Passwords," *22nd Annu. Netw. Distrib. Syst. Secur. Symp. NDSS 2015*, 2015, doi: 10.14722/ndss.2015.23094.

[7] uswatun, "Keamanan Siber di Aplikasi Mobile: Tantangan dan Praktik Terbaik," *csirt.teknokrat.ac.id*, 2024. [Daring]. Tersedia pada: https://csirt.teknokrat.ac.id/keamanan-siber-di-aplikasi-mobile-tantangan-dan-praktik-terbaik/

[8] U. Mattsson, "Zero Trust Architecture," *Control. Priv. Use Data Assets*, hal. 127–134, 2022, doi: 10.1201/9781003189664-11.

[9] Alissa Irei, "7 langkah untuk menerapkan zero trust, dengan contoh nyata," Techtarget.com. [Daring]. Tersedia pada: https://www.techtarget.com/searchsecurity/feature/How-to-implement-zero-trust-security-from-people-who-did-it

[10] Z. R. Wafi, "Tantangan Implementasi Zero Trust Security pada Lingkungan Sistem Informasi Modern dan Solusinya," no. April, 2023, doi: 10.13140/RG.2.2.10376.70408.

[11] Asiva Noor Rachmayani, "Tinjauan Strategis Keamanan Siber Indonesia," hal. 6, 2015.

[12] B. Zyoud dan S. L. Lutfi, "The Role of Information Security Culture in Zero Trust Adoption: Insights From UAE Organizations," *IEEE Access*, vol. 12, no. March, hal. 72420–72444, 2024, doi: 10.1109/ACCESS.2024.3402341.

[13] Tri Yulianto B, Quraisy M, Daulay A, dan Puspita Sari A, "Private Server Design Using Proxmox Platform and Implementation of Zero Trust Model with Cloudflare," no. November 2023, hal. 195–207, 2023, [Daring]. Tersedia pada: https://www.researchgate.net/publication/379957385

[14] G. Guntoro dan M. Fikri, "Perancangan Aplikasi Single Sign-On Menggunakan Autentikasi Gambar," *Digit. Zo. J. Teknol. Inf. dan Komun.*, vol. 9, no. 1, hal. 12–21, 2018, doi: 10.31849/dz.v9i1.648.

[15] M. I. Hussain *et al.*, "AAAA: SSO and MFA implementation in multi-cloud to mitigate rising threats and concerns related to user metadata," *Appl. Sci.*, vol. 11, no. 7, 2021, doi: 10.3390/app11073012.

[16] NIST SP800-53, "Security and Privacy Controls for Information Systems and Organizations," *NIST Spec. Publ.*, hal. 465, 2020, [Daring]. Tersedia pada: https://doi.org/10.6028/NIST.SP.800-53r5

[17] Z. Wang, X. Yu, P. Xue, Y. Qu, dan L. Ju, "Research on Medical Security System Based on Zero Trust," *Sensors*, vol. 23, no. 7, 2023, doi: 10.3390/s23073774.

[18] Y. S. Muhammad Mujib, Riri Fitri Sari, supervisi, Kalamullah Ramli, "Evaluasi Performa Jaringan Pusat Data Berbasis Software Defined Networking dengan Model Keamanan Zero Trust Berbasis Micro-segmentation," Universitas Indonesia, 2020.

[19] A. Niraula, "Zero Trust Architecture for Peer to Peer Communication using Blockchain and Hardware Oriented Security by," *Fish. Res.*, vol. 140, no. 1, hal. 6, 2021, [Daring]. Tersedia pada: http://dspace.ucuenca.edu.ec/bitstream/123456789/35612/1/Trabajo de Titulacion.pdf%0Ahttps://educacion.gob.ec/wp-content/uploads/downloads/2019/01/GUIA-METODOLOGICA-EF.pdf%0Ahttp://dx.doi.org/10.1016/j.fishres.2013.04.005%0Ahttps://doi.org/10.1038/s41598-

[20] J. Jose Diaz Rivera, A. Muhammad, dan W. C. Song, "Securing Digital Identity in the Zero Trust Architecture: A Blockchain Approach to Privacy-Focused Multi-Factor Authentication," *IEEE Open J. Commun. Soc.*, vol. 5, no. March, hal. 2792–2814, 2024, doi: 10.1109/OJCOMS.2024.3391728.