



Zero Trust-X: A Research on a Zero Trust-Based Approach to Enhance Cyber Resilience Using the MITRE ATT&CK Framework

Mariya Augustine¹, Karthiga N², Karthik K. G³, Sanjuna Poopathi⁴, Sowndarya V⁵

^{1,2,3,4}B.E. Computer Science and Engineering (Cyber Security), United Institute of Technology, Coimbatore, Tamil Nadu, India.

⁵Assistant Professor, Department of Computer Science and Engineering (Cyber Security), United Institute of Technology, Coimbatore, Tamil Nadu, India.

To Cite this Article: Mariya Augustine¹, Karthiga N², Karthik K. G³, Sanjuna Poopathi⁴, Sowndarya V⁵, “Zero Trust-X: A Research on a Zero Trust-Based Approach to Enhance Cyber Resilience Using the MITRE ATT&CK Framework”, Indian Journal of Computer Science and Technology, Volume 05, Issue 02 (May-August 2026), PP: 137-144.



Copyright: ©2026 This is an open access journal, and articles are distributed under the terms of the [Creative Commons Attribution License](#); Which Permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Abstract: Traditional perimeter-based cybersecurity models assume implicit trust once users gain network access, making them vulnerable to credential compromise, insider threats, and lateral movement attacks. To address these limitations, this paper proposes **ZeroTrustX**, an integrated cybersecurity monitoring framework that combines Zero Trust Architecture (ZTA) with the MITRE ATT&CK threat intelligence model to enhance organizational cyber resilience through continuous verification and behavior-aware threat detection. The proposed system enforces identity validation, role-based access control, micro-segmentation, and real-time activity monitoring to restrict unauthorized access and detect anomalous behavior across multiple attack stages. A threat simulation engine is incorporated to evaluate system responses against common attack scenarios such as phishing attempts, privilege escalation, insider threats, and lateral movement. Security events are mapped to MITRE ATT&CK tactics and techniques to improve contextual threat visibility and support faster incident response. Experimental evaluation using the developed ZeroTrustX prototype demonstrates improved detection accuracy and reduced attack propagation compared with traditional perimeter-based security approaches. The proposed framework provides a scalable and practical solution for strengthening enterprise security posture through integrated access control and structured threat intelligence mapping.

Key Words: Cybersecurity, Micro-segmentation, MITRE ATT&CK Framework, Role-Based Access Control, Zero Trust Architecture.

I. INTRODUCTION

The rapid evolution of digital infrastructures, cloud computing environments, and interconnected enterprise systems has significantly increased organizational exposure to sophisticated cyber threats. Modern attackers frequently exploit credential compromise, phishing campaigns, insider privileges, and lateral movement techniques to bypass traditional perimeter-based security mechanisms. Conventional cybersecurity architectures rely primarily on boundary protection strategies such as firewalls and intrusion detection systems, which assume that authenticated users inside the network can be trusted. However, this implicit trust model has become ineffective against multi-stage attack campaigns and advanced persistent threats targeting enterprise environments.

To address these limitations, Zero Trust Architecture (ZTA) has emerged as a modern security paradigm that eliminates implicit trust assumptions and enforces continuous identity verification for every access request regardless of network location [1]. By applying least-privilege access policies, role-based authorization mechanisms, and micro-segmentation strategies, Zero Trust models reduce attack surfaces and restrict unauthorized lateral movement across enterprise systems [2]. These capabilities enable organizations to transition from static perimeter defense toward identity-centric security monitoring frameworks.

In addition to identity-aware access control mechanisms, the MITRE ATT&CK framework provides a structured knowledge base of adversarial tactics and techniques derived from real-world cyberattack observations. Mapping security events to ATT&CK techniques such as initial access, persistence, privilege escalation, and lateral movement improves visibility into attacker behavior across multiple intrusion lifecycle stages and supports faster incident response and threat mitigation strategies [3].

Although existing research has explored Zero Trust-based authentication and behavior-driven monitoring independently, limited work has focused on integrating identity-centric access enforcement with structured ATT&CK-based threat intelligence within a unified monitoring platform. To address this gap, this paper proposes **ZeroTrustX**, an integrated cybersecurity monitoring framework that combines Zero Trust authentication principles with MITRE ATT&CK-based threat intelligence mapping to enhance organizational cyber resilience. The proposed system incorporates identity verification, role-based access control, micro-segmentation enforcement, continuous activity monitoring, and a threat simulation engine capable of evaluating

system responses across multiple cyberattack scenarios. Experimental observations demonstrate improved detection capability and reduced attack propagation risk compared with conventional perimeter-based security approaches.

Research Contribution

The primary contributions of this paper are summarized as follows. First, a unified cybersecurity monitoring framework named ZeroTrustX is proposed by integrating Zero Trust Architecture with MITRE ATT&CK- based threat intelligence mapping to enhance cyber resilience in enterprise environments. Second, the framework implements continuous identity verification using role-based access control and context-aware policy evaluation to enforce least-privilege access and reduce unauthorized resource exposure. Third, an application-level micro- segmentation strategy is incorporated to restrict lateral movement across protected system components. Fourth, a threat simulation engine is developed to evaluate system responses against multiple cyberattack scenarios including phishing attempts, insider threats, privilege escalation, and lateral movement activities. Finally, experimental analysis using the ZeroTrustX prototype demonstrates improved detection capability and enhanced threat visibility compared with traditional perimeter-based security approaches.

II. RELATED WORK

Traditional perimeter-based security architectures rely on boundary protection mechanisms such as firewalls and intrusion detection systems to secure enterprise environments. These approaches assume implicit trust for authenticated users within the network and therefore remain vulnerable to credential compromise and insider threats. To overcome these limitations, the concept of Zero Trust Architecture (ZTA) was introduced as a security paradigm that eliminates implicit trust relationships and enforces continuous identity verification for all access requests regardless of network location [1].

The National Institute of Standards and Technology formally defined Zero Trust principles in NIST Special Publication 800-207, which emphasizes continuous authentication, least-privilege access enforcement, and micro-segmentation to reduce attack surfaces and improve enterprise security posture [2].

In addition to identity-centric access control frameworks, the MITRE ATT&CK framework has emerged as a widely adopted threat intelligence resource for analyzing adversarial tactics and techniques based on real-world cyberattack observations. The framework enables structured classification of attacker behavior across multiple intrusion lifecycle stages including initial access, persistence, privilege escalation, and lateral movement [3].

Recent research efforts have explored integrating Zero Trust mechanisms with behavioral threat intelligence models to enhance detection accuracy against advanced persistent threats and credential-based attacks. However, many existing solutions focus primarily on authentication enforcement without incorporating structured ATT&CK- based threat mapping within a unified monitoring architecture [4]. To address these limitations, the proposed ZeroTrustX framework integrates Zero Trust authentication, micro-segmentation enforcement, and MITRE ATT&CK-based threat classification within a single cybersecurity monitoring platform to improve detection capability and strengthen enterprise cyber resilience.

III. PROBLEM STATEMENT AND MOTIVATION

Modern enterprise networks operate in highly distributed environments where users access resources from multiple locations, devices, and platforms. While this flexibility improves operational efficiency, it also increases exposure to sophisticated cyber threats that exploit weaknesses in traditional perimeter-based security models. Conventional security frameworks rely primarily on static authentication mechanisms and boundary protection strategies, which are insufficient for addressing multi-stage intrusion techniques used by modern attackers.

1. Limitations of Perimeter-Based Security Models

Traditional cybersecurity architectures assume that users inside the organizational network can be trusted once authenticated. This implicit trust model creates security gaps that allow attackers to move laterally across systems after gaining initial access through credential compromise or phishing attacks. Intrusion detection and prevention systems deployed at network boundaries are often ineffective against insider threats and privilege escalation attacks occurring within trusted environments [9], [10]. As a result, organizations experience reduced visibility into internal attack propagation and delayed incident response.

2. Challenges in Detecting Advanced Persistent Threats

Advanced Persistent Threats (APTs) represent one of the most critical cybersecurity challenges faced by modern enterprises. These threats operate through multi-stage attack strategies that include persistence mechanisms, privilege escalation, and stealthy lateral movement across network zones. Traditional signature-based detection techniques are often unable to identify such evolving attack patterns in real time, leading to prolonged attacker presence within enterprise infrastructures [8]. This highlights the need for behavior-driven monitoring frameworks capable of identifying anomalies across different stages of the attack lifecycle.

3. Lack of Continuous Identity Verification and Access Control Enforcement

Although role-based access control (RBAC) mechanisms provide structured authorization policies for managing user permissions, they are typically implemented without continuous identity verification and contextual monitoring capabilities. Static authorization mechanisms cannot dynamically adapt to changes in user behavior or system conditions, making them insufficient for protecting distributed enterprise environments against credential misuse and unauthorized privilege escalation attacks [11]. Therefore, modern cybersecurity systems require identity-aware access enforcement strategies that continuously validate user

activity throughout the session lifecycle.

4. Absence of Structured Threat Intelligence Integration

The MITRE ATT&CK framework provides a comprehensive classification of attacker tactics and techniques across multiple intrusion lifecycle stages such as initial access, persistence, privilege escalation, and lateral movement. However, many existing enterprise monitoring solutions do not effectively integrate ATT&CK-based threat intelligence with identity-centric security architectures. As a result, organizations lack structured visibility into adversarial behavior patterns required for proactive threat detection and response [3]. Integrating ATT&CK-based mapping with monitoring frameworks can significantly improve contextual awareness of cyber threats.

5. Motivation for the Proposed ZeroTrustX Framework

To address the limitations of traditional security architectures, Zero Trust Architecture (ZTA) introduces continuous authentication, least-privilege access enforcement, and micro-segmentation strategies for protecting enterprise systems against unauthorized access and lateral movement threats. As defined in NIST Special Publication 800-207, Zero Trust principles enable organizations to strengthen cybersecurity resilience by eliminating implicit trust assumptions within network environments [2].

Motivated by these requirements, this paper proposes the **ZeroTrustX framework**, which integrates Zero Trust authentication mechanisms with MITRE ATT&CK-based threat intelligence mapping to enhance threat visibility and detection accuracy across enterprise infrastructures. The proposed approach combines identity verification, role-based authorization, activity monitoring, and structured adversarial behavior classification to improve cyber resilience against evolving threat landscapes.

IV. PROPOSED SYSTEM ARCHITECTURE

The proposed **ZeroTrustX framework** integrates Zero Trust Architecture principles with MITRE ATT&CK-based threat intelligence mapping to provide a continuous monitoring environment capable of detecting anomalous activities across multiple stages of enterprise network access. Unlike traditional perimeter-based security approaches, the proposed architecture eliminates implicit trust assumptions and enforces identity-aware authorization mechanisms supported by structured threat classification workflows.

The architecture consists of multiple functional layers that collectively provide authentication enforcement, activity monitoring, segmentation control, and threat intelligence mapping for improving enterprise cyber resilience.

1) User Access and Identity Verification Layer

The first layer of the ZeroTrustX framework handles authentication requests from users attempting to access enterprise resources. Each access request undergoes identity verification before authorization decisions are applied. Continuous validation mechanisms ensure that access privileges are dynamically evaluated rather than granted permanently after initial login. This approach aligns with Zero Trust principles defined in modern enterprise security frameworks [2].

2) Role-Based Access Control Layer

After identity verification, access permissions are assigned using role-based access control (RBAC) policies that restrict user privileges based on predefined authorization levels. RBAC mechanisms reduce unauthorized access risks by enforcing least-privilege access policies across protected system components. Structured access management models improve accountability and prevent privilege escalation attacks within enterprise environments [11].

3) Zero Trust Policy Decision Engine

The policy decision engine evaluates contextual parameters such as authentication status, role attributes, and behavioral indicators before granting access to requested resources. Instead of relying on static authorization mechanisms, this component continuously monitors session activity to ensure compliance with security policies throughout the access lifecycle. Dynamic policy enforcement reduces exposure to credential misuse and insider threats.

4) Micro-Segmentation Layer

The micro-segmentation layer divides enterprise infrastructure into smaller logical security zones to prevent unauthorized lateral movement between system components. Even if attackers gain initial access to one segment, segmentation policies restrict their ability to traverse across protected resources. Micro-segmentation significantly reduces attack propagation risks in distributed enterprise environments [5].

5) Activity Monitoring and Threat Detection Layer

This layer continuously monitors user activity, authentication logs, and behavioral anomalies to detect suspicious access attempts. Monitoring mechanisms identify repeated login failures, unauthorized privilege escalation attempts, and abnormal system interactions that may indicate potential security incidents. Behavior-based monitoring improves detection accuracy compared with traditional signature-based intrusion detection approaches [10].

6) MITRE ATT&CK Threat Mapping Layer

Detected anomalies are mapped to adversarial tactics and techniques defined in the MITRE ATT&CK framework to provide structured visibility into attack progression across different lifecycle stages. This mapping enables security administrators

to classify threats according to attacker objectives such as persistence, privilege escalation, and lateral movement, thereby improving contextual threat understanding and response efficiency [3].

7) Alert Generation and Response Layer

The final layer generates real-time alerts when suspicious activities are detected within the monitoring environment. Security administrators receive notifications through the centralized dashboard interface, enabling rapid mitigation of potential threats before they propagate across enterprise systems. Automated alert generation improves incident response time and strengthens organizational cyber resilience.

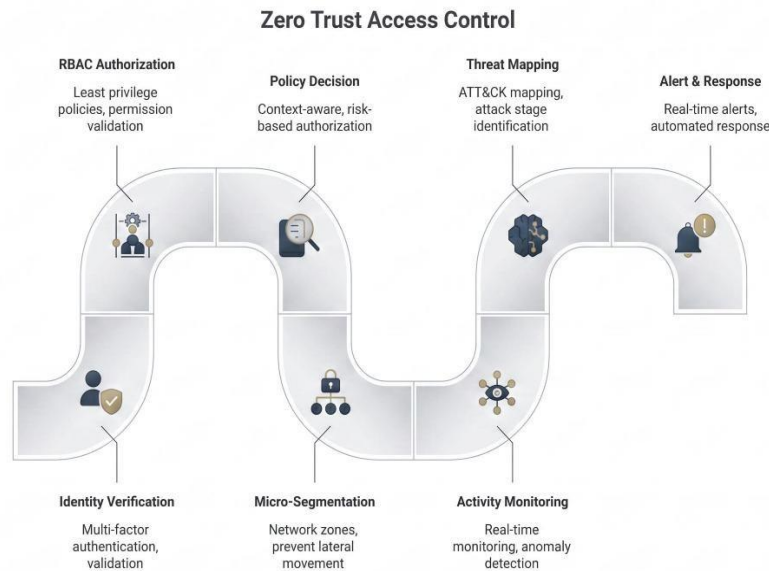


Fig. 1. Proposed ZeroTrustX architecture integrating Zero Trust access control with MITRE ATT&CK-based threat intelligence mapping.

V. METHODOLOGY

The proposed **ZeroTrustX framework** follows a structured workflow that integrates Zero Trust authentication mechanisms with MITRE ATT&CK-based threat intelligence mapping to provide continuous monitoring and detection of anomalous user behavior within enterprise environments. Unlike traditional perimeter-based security approaches, the methodology enforces identity-aware access control and behavior-driven threat classification throughout the session lifecycle.

The workflow of the proposed system consists of multiple sequential stages that collectively improve visibility into attacker activities and reduce unauthorized access risks.

1) User Authentication and Identity Validation

The first stage of the methodology involves verifying user identity before granting access to protected system resources. Authentication requests are evaluated using secure credential validation mechanisms to ensure that only authorized users can initiate sessions within the monitoring environment. Continuous identity verification aligns with Zero Trust principles that eliminate implicit trust relationships inside enterprise infrastructures [2].

2) Role-Based Access Control Enforcement

After identity validation, access privileges are assigned based on predefined role-based access control (RBAC) policies. RBAC ensures that users can only access resources corresponding to their authorization level, thereby enforcing least-privilege security principles. Structured access control models reduce the likelihood of privilege escalation and unauthorized resource exposure in distributed systems [11].

3) Policy Evaluation and Context-Aware Authorization

Following role assignment, the Zero Trust policy decision engine evaluates contextual parameters such as user roles, session attributes, and behavioral indicators before granting access permissions. Dynamic policy enforcement ensures that access decisions are continuously verified instead of relying on static authentication mechanisms, which improves resistance against credential misuse attacks [2].

4) Micro-Segmentation-Based Resource Protection

To prevent attackers from moving laterally across network zones after initial compromise, the system applies micro-segmentation strategies that divide enterprise infrastructure into smaller logical protection domains. Segmentation policies restrict unauthorized traversal between protected components and significantly reduce attack propagation risks in enterprise environments [5].

5) Continuous Activity Monitoring and Behavioral Analysis

The monitoring module continuously analyzes authentication logs, session activity, and interaction patterns to identify suspicious behavior such as repeated login attempts, unauthorized access requests, and abnormal privilege usage. Behavior-driven monitoring improves anomaly detection accuracy compared with traditional signature-based intrusion detection techniques [10].

6) MITRE ATT&CK Threat Mapping

Detected anomalies are mapped to adversarial tactics and techniques defined in the MITRE ATT&CK framework to provide structured visibility into attacker behavior across multiple stages of the intrusion lifecycle. This mapping enables classification of threats such as persistence attempts, privilege escalation, and lateral movement activities, thereby improving situational awareness for security administrators [3].

7) Alert Generation and Administrative Response

In the final stage, the system generates real-time alerts when suspicious activities are detected within the monitoring environment. These alerts are displayed through the administrative dashboard interface, enabling rapid investigation and mitigation of potential threats before they escalate into security incidents. Automated alert generation improves response efficiency and strengthens enterprise cyber resilience against evolving attack strategies.

VI. IMPLEMENTATION OF ZEROTRUSTX

The proposed **ZeroTrustX framework** was implemented as a prototype web-based cybersecurity monitoring system designed to demonstrate the integration of Zero Trust authentication principles with MITRE ATT&CK-based threat intelligence mapping. The implementation focuses on enforcing identity-aware access control, monitoring user activity, and classifying simulated attack scenarios to improve enterprise threat visibility and response capability.

The system architecture consists of multiple functional modules that collectively provide authentication enforcement, role-based authorization, threat simulation, activity monitoring, and alert generation capabilities.

1) Authentication and Identity Verification Module

The authentication module enables users to securely register and access the monitoring platform using credential-based identity verification mechanisms. Each user is assigned predefined authorization roles during registration to ensure controlled access to protected resources. Continuous identity verification ensures compliance with Zero Trust security principles by eliminating implicit trust relationships within the system environment [2].

2) Role-Based Access Control Implementation

Role-based access control policies were implemented to restrict system privileges according to predefined authorization levels. Administrative users are granted access to monitoring dashboards and threat analysis modules, while standard users are limited to controlled system interactions. RBAC enforcement ensures least-privilege access and prevents unauthorized privilege escalation attempts within the monitoring environment [11].

3) Threat Simulation Engine

The ZeroTrustX framework incorporates a threat simulation module that enables administrators to evaluate system responses against multiple cyberattack scenarios. Simulated attack types include phishing attempts, insider threats, privilege escalation activities, and lateral movement behaviors. These simulations generate structured activity logs that support behavioral monitoring and ATT&CK-based threat classification workflows [3].

4) Activity Monitoring and Log Management Module

User interactions within the system environment are continuously monitored to detect anomalous behavioral patterns. The monitoring engine records authentication attempts, access requests, and simulated threat activities in a centralized log database for further analysis. Behavioral log monitoring improves detection capability compared with traditional signature-based intrusion detection mechanisms [10].

5) MITRE ATT&CK Threat Mapping Integration

Detected anomalies are mapped to adversarial tactics and techniques defined in the MITRE ATT&CK framework to provide structured classification of attack behavior across multiple intrusion lifecycle stages. This mapping improves contextual awareness of attack progression and supports rapid identification of potential security incidents [3].

6) Alert Generation and Administrative Dashboard

The administrative dashboard provides real-time visualization of detected threats, user activity patterns, and alert notifications generated by the monitoring engine. Security administrators can monitor system status, analyze simulated attack scenarios, and initiate mitigation responses through the centralized interface. Automated alert generation improves response efficiency and strengthens the overall security posture of enterprise monitoring environments.

VII. EXPERIMENTAL RESULTS AND PERFORMANCE EVALUATION

The performance of the proposed **ZeroTrustX framework** was evaluated using simulated cyberattack scenarios designed to analyze its effectiveness in detecting anomalous user behavior compared with traditional perimeter-based security monitoring approaches. The evaluation focuses on identity verification accuracy, role-based authorization enforcement, behavioral anomaly detection capability, and structured threat classification using the MITRE ATT&CK framework.

The experimental setup included multiple simulated attack scenarios representing common enterprise threat vectors such as phishing attempts, privilege escalation activities, insider threats, lateral movement behavior, and unauthorized access attempts. These scenarios were selected to evaluate how effectively the proposed framework detects threats across different stages of the intrusion lifecycle. Detection performance was compared with conventional perimeter-based monitoring systems that rely primarily on static authentication and signature-based intrusion detection mechanisms.

A) Detection Performance Analysis

Table I presents a comparison between the detection capabilities of traditional security monitoring systems and the proposed ZeroTrustX framework across multiple simulated attack scenarios. The results demonstrate that the ZeroTrustX framework improves detection accuracy by enforcing continuous identity verification, role-based authorization policies, and micro-segmentation strategies combined with MITRE ATT&CK-based threat intelligence mapping.

Attack Scenario	Traditional Security Detection	Zero Trust X Detection
Phishing Attempt	Partial Detection	Detected
Privilege Escalation	Delayed Detection	Immediate Detection
Insider Threat Activity	Limited Visibility	Fully Detected
Lateral Movement Behavior	Not Detected	Detected
Attack Scenario	Traditional Security Detection	Zero Trust X Detection
Unauthorized Access Attempt	Partial Detection	Fully Detected

Table I. Detection Capability Comparison Between Traditional Security Systems and ZeroTrustX Framework

The results indicate that traditional perimeter-based security mechanisms provide limited visibility into insider activities and lateral movement attacks after initial authentication. In contrast, the ZeroTrustX framework continuously monitors session behavior and enforces least-privilege access policies, enabling early detection of suspicious activities before attack propagation occurs.

B) Comparative Detection Performance Over Monitoring Intervals

To further evaluate detection efficiency, the threat detection rate of the proposed framework was compared with conventional monitoring approaches across simulated monitoring intervals. The comparison results are illustrated in Fig. 2, which shows that the ZeroTrustX framework consistently achieves higher detection accuracy due to continuous identity verification and behavior-driven threat classification mechanisms

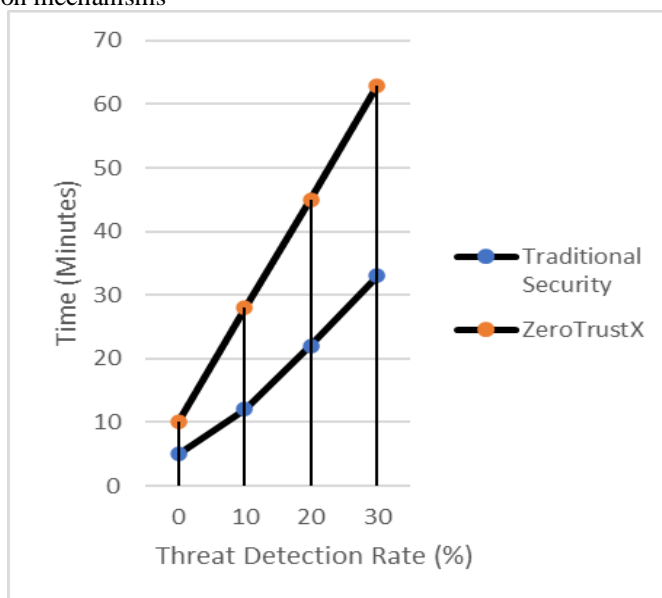


Fig. 2. Detection performance comparison between traditional perimeter-based security mechanisms and the proposed ZeroTrustX monitoring framework across simulated monitoring intervals.

The graph demonstrates that detection accuracy improves progressively as monitoring intervals increase, highlighting the effectiveness of integrating Zero Trust access control mechanisms with MITRE ATT&CK-based threat intelligence mapping. Unlike traditional systems that rely on static authentication checkpoints, the proposed framework continuously evaluates contextual session attributes and behavioral indicators, enabling earlier identification of anomalous activity patterns.

C) Impact of MITRE ATT&CK-Based Threat Mapping

The integration of MITRE ATT&CK-based threat intelligence mapping further enhances the detection capability of the proposed framework by providing structured classification of adversarial tactics across multiple intrusion lifecycle stages. Mapping detected anomalies to ATT&CK techniques such as initial access, persistence, privilege escalation, and lateral movement improves contextual understanding of attacker behavior and supports faster incident response decision-making processes.

The combined use of Zero Trust authentication principles and structured threat intelligence mapping significantly improves enterprise monitoring visibility and reduces attack propagation risks compared with conventional perimeter-based security architectures. These improvements demonstrate the effectiveness of the ZeroTrustX framework in strengthening cybersecurity resilience within modern distributed enterprise environments.

VIII. CONCLUSION AND FUTURE WORK

This paper presented ZeroTrustX, an integrated cybersecurity monitoring framework that combines Zero Trust Architecture principles with MITRE ATT&CK-based threat intelligence mapping to enhance enterprise threat detection and response capabilities. The proposed framework eliminates implicit trust assumptions by enforcing continuous identity verification, role-based access control policies, and micro-segmentation strategies to restrict unauthorized lateral movement within protected environments. These mechanisms align with the Zero Trust security model defined in NIST Special Publication 800-207, which emphasizes continuous verification and least-privilege access enforcement for modern enterprise infrastructures [2].

The integration of behavior-driven monitoring with structured ATT&CK-based threat classification enables improved visibility into adversarial activities across multiple stages of the intrusion lifecycle. Mapping detected anomalies to ATT&CK tactics such as initial access, persistence, privilege escalation, and lateral movement improves contextual understanding of attack progression and supports faster incident response decision-making processes [3]. Experimental evaluation using simulated attack scenarios demonstrated that the ZeroTrustX framework provides earlier detection of phishing attempts, privilege escalation activities, insider threats, and unauthorized access events compared with traditional perimeter-based security approaches. These improvements highlight the effectiveness of combining identity-aware access enforcement with structured threat intelligence mapping to strengthen cybersecurity resilience in distributed enterprise environments [7].

Furthermore, the implementation of role-based authorization and micro-segmentation mechanisms significantly reduces attack propagation risks by restricting unauthorized resource access within segmented security zones. These access control strategies improve monitoring accuracy and enhance protection against credential misuse and insider threats across enterprise systems [5], [11].

Future work will focus on extending the ZeroTrustX framework by incorporating machine learning–based anomaly detection techniques for improving predictive threat identification accuracy and adaptive threat classification. Additional enhancements may include integration with real-time network traffic analysis tools, automated incident response orchestration mechanisms, and deployment within cloud-based enterprise environments to evaluate performance under large-scale operational conditions. These extensions will further strengthen the capability of the proposed framework to support intelligent and scalable cybersecurity monitoring in next-generation enterprise systems.

Acknowledgment

The authors would like to express their sincere gratitude to the Department of Computer Science and Engineering (Cybersecurity), United Institute of Technology, Coimbatore, for providing the necessary infrastructure and academic support to carry out this research work. The authors also extend their heartfelt appreciation to their project guide for valuable guidance, encouragement, and continuous support throughout the development of the ZeroTrustX framework. Special thanks are conveyed to the faculty members and peers who provided constructive suggestions that contributed to the successful completion of this research study.

REFERENCES

1. J. Kindervag, No More Chewy Centers: Introducing the Zero Trust Model of Information Security, Forrester Research. 5(2) (2010) 1–16.
2. S. Rose, O. Borchert, S. Mitchell and S. Connelly, Zero Trust Architecture, NIST Special Publication 800-207, National Institute of Standards and Technology. 8(4) (2020) 1–59.
3. MITRE Corporation, MITRE ATT&CK Framework. [Online]. Available: <https://attack.mitre.org/>
4. J. Ward and B. Beyer, BeyondCorp: A New Approach to Enterprise Security, IEEE Security and Privacy. 12(5) (2014) 62–67.
5. A. Shaghghi, M. Abomhara and G. M. Kjøien, Enhancing Network Security Using Micro-Segmentation Techniques, Computers and Security. 97(2) (2020) 101942.
6. R. Khan, K. McLaughlin and D. Lavery, Cybersecurity Framework for Smart Grid Using Zero Trust Architecture, IEEE Transactions on Smart Grid. 13(2) (2022) 1021–1032.
7. Y. Ahn, J. Kim and H. Lee, Integration of Zero Trust Architecture with MITRE ATT&CK Framework for Threat Detection, IEEE Access. 12(1) (2024) 22345–22358.
8. A. Alshamrani, S. Myneni, A. Chowdhary and D. Huang, A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges and

- Research Opportunities, *IEEE Communications Surveys and Tutorials*. 21(2) (2019) 1851–1877.
9. K. Scarfone and P. Mell, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, NIST Special Publication 800-94. 6(3) (2007) 1–127.
 10. H. Debar, M. Dacier and A. Wespi, *Towards a Taxonomy of Intrusion Detection Systems*, *Computer Networks*. 31(8) (1999) 805–822.
 11. R. Sandhu, E. Coyne, H. Feinstein and C. Youman, *Role-Based Access Control Models*, *IEEE Computer*. 29(2) (1996) 38–47.
 12. D. Ferraiolo, R. Kuhn and R. Chandramouli, *Role-Based Access Control*, *Artech House Computer Security Series*. 4(2) (2003) 1–300.
 13. S. Oh and S. Park, *Task-Role-Based Access Control Model*, *Information Systems*. 28(6) (2003) 533–562.
 14. A. Aldribi, M. Traore and A. Ghorbani, *Cyber Threat Intelligence Sharing: Requirements, Challenges and Solutions*, *Computers and Security*. 92(1) (2020) 101761.
 15. R. Mitchell and I. Chen, *A Survey of Intrusion Detection Techniques for Cyber-Physical Systems*, *ACM Computing Surveys*. 46(4) (2014) 1–29.
 16. A. Singhal and X. Ou, *Security Risk Analysis of Enterprise Networks Using Attack Graphs*, NIST Interagency Report. 7(5) (2011) 1–28.
 17. N. Moustafa and J. Slay, *UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems*, *Military Communications and Information Systems Conference*. 3(2) (2015) 1–6.
 18. E. Bertino and N. Islam, *Botnets and Internet of Things Security*, *IEEE Computer*. 50(2) (2017) 76–79.
 19. S. Yu, *Distributed Denial of Service Attack and Defense*, *Springer Briefs in Computer Science*. 2(1) (2014) 1–91.
 20. P. Cichonski, T. Millar, T. Grance and K. Scarfone, *Computer Security Incident Handling Guide*, NIST Special Publication 800-61. 9(2) (2012) 1–147.
 21. A. G. Rege and M. A. Shaikh, *Cyber Resilience: A Review of Critical Infrastructure Protection Strategies*, *International Journal of Critical Infrastructure Protection*. 25(1) (2019) 100305
 22. P. Mell and T. Grance, *The NIST Definition of Cloud Computing*, NIST Special Publication 800-145. 4(1) (2011) 1–7.
 23. M. Bishop, *Computer Security: Art and Science*, Addison-Wesley Professional. 6(2) (2003) 1–1136.
 24. N. Mavroeidis and S. Bromander, *Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards and Ontologies within Cyber Threat Intelligence*, *IEEE European Symposium on Security and Privacy Workshops*. 5(3) (2017) 91–98.
 25. S. Yu, P. Smith and A. Newell, *Zero Trust Security: An Enterprise Guide*, O’Reilly Media. 10(2) (2021) 1–220.