A Novel Approach to Enhance Cyber Resilience by Combining the Zero Trust Security Model and MITRE ATT&CK Matrix Strategy

P. Ramya, Badapu Yaswanth, Anem Nithish Kumar,
Ambati Harikrishna and Arikatla Balagurunath Reddy
Department of Computer Science and Engineering, Mahendra Engineering College, Tamil Nadu, India

Keywords: Cyber Resilience, Zero Trust, Threat Elimination, ZTM, Data Security, MITRE, ATT, CK Matrix, Cyber Threat, CTES.

Abstract: Cyber threats have grown exponentially with the digital information era, changing cyberspace. We suggest merging the Zero Trust (ZT) security paradigm with the MITRE ATT&CK matrix to improve cyber resilience, an organization's ability to recover quickly from a cyber-attack or security event. Public sector organizations are vulnerable to the Advanced Persistent Threat (APT), but this research also examines phishing, ransom ware, and insider threats. These threats exploit a company's computer and network vulnerabilities. The ZT model's "never trust, always verify," which ensures that all network traffic is examined equally, emphasizes micro-segmentation, continuous authentication, and least privilege. Research reveals that combining the ZT and ATT&CK models may increase a company's cyber threats, and the study provides metrics for doing so. The Cyber Threat Elimination Strategy (CTES) encompasses all of these indicators and is cross-validated using the Zero Trust Model to assess its success. The study introduces a new cybersecurity paradigm, emphasizes the Zero Trust model's importance in modern security strategies, and shows that organizations can proactively assess the changing cyber threat landscape to ensure a secure and resilient digital future. ZT and the MITRE ATT&CK matrix must be merged since current security measures cannot handle the complexity and sophistication of cyber-attacks. Integrating the two models helps discover research gaps and give practical responses, strengthening an organization's cyber defenses.

1 INTRODUCTION

The accelerating development of the digital ecosystem crosses conventional industrial borders, attaching various elements of everyday life to its ever-integrating web, all mirroring the increasing notion of cyberspace in the fabric of the modern society. While digital innovation promotes connectedness, yet enterprises are faced by new challenges related to more advanced and pervasive cyberattacks. Naga Vinod Duggirala, 2024; Chunwen Liu, et al., 2024, Given that cyberattacks have the capacity to cripple infrastructure, invade privacy, and pose a threat to national security, it is imperative, now more than ever, to formulate an effective cybersecurity plan. This study examined the effectiveness of the Zero Trust security model with the MITRE ATT&CK framework in advancing cyber-resiliency. Cyber-resilience ensures business continuity from any sort of cyber threat: the ability of an organization to foresee, respond, recover, and adapt in relation to that threat. Zillah Adahman, et al., 2023, Emphasizing continuous verification of all network traffic, irrespective of source, the Zero Trust model is a radical departure from conventional perimeter-based security. Shaikh Ashfaq, et al., 2023, The latter intends to provide a solid framework to protect digital assets against the ever-growing cyber risks, emphasizing micro-segmentation, continuous authentication, and the principle of least privilege. Onome Edo, et al., 2022; Nisha T N, et al., 2023; Naeem Firdous Syed, et al., 2022, This method, besides, does bring a different view to a cybersecurity field by merging the strategic recommendations from the Zero Trust model and that from the MITRE ATT&CK architecture. While such integration helps fend off the tactics used in cyberattacks, it concurrently enhances cyber resilience by allowing organizations to analyze and foresee cyber risks. This research aims to study how this integration can fortify an organization's defenses against cyberattacks. Naeem Firdous Syed, et al., 2023; Yiliang Liu, et al.,

Ramya, P., Yaswanth, B., Kumar, A. N., Harikrishna, A. and Reddy, A. B.
A Novel Approach to Enhance Cyber Resilience by Combining the Zero Trust Security Model and MITRE ATT&CK Matrix Strategy.
DOI: 10.5220/0013874600004919

In *Proceedings of the 1st International Conference on Research and Development in Information, Communication, and Computing Technologies (ICRDICCT'25 2025) - Volume 1*, pages 857-865
ISBN: 978-989-758-777-1

2024, The aim of this paper is to contribute to the ongoing discussion about cybersecurity and propose for enterprises a strategic roadmap to cope with the complex digital threat landscape by discussing practical ideas to manage and implement such security policies.

This study suggests tangible steps to be taken toward understanding how to implement the Zero Trust paradigm with the MITRE ATT&CK framework in order to help organizations make themselves stronger against cyberattacks. The purpose of this multi-sectioned article is to improve corporate cyber resilience through workforce integration of the Zero Trust paradigm with the MITRE ATT&CK methodology. The general research objectives and rationale for the integration are explained in Chapter I. Chapter II will contain a theoretical characterization of the MITRE ATT&CK Framework and Zero Trust Model. In Chapter III, the methodology of the integration process must be laid out. Chapter IV deals with the practical implementation of the integration framework in an organization. The integration is validated through empirical evidence in Chapter V. Chapter VI discusses the implications of these findings in terms of strengthening cyber resilience. Chapter VII compares the integration approach with earlier investigations to illustrate how innovative and effective it is. Chapter IX discusses the limitations of this study. Chapter X details the contributions of this study. Finally, Chapter XI will generalize our findings and set out directions for further research.

2 RELATED WORKS

Conventional perimeter-based security solutions are no longer sufficient to safeguard contemporary organizational infrastructures in this age of more sophisticated and frequent cyber-attacks. With the rise of remote work, cloud computing, and mobile devices, enterprises are quickly embracing digital transformation and implementing a new security paradigm: Zero Trust Security. Assuming that any and all network communication, whether it originates from within or outside the organization, might be malicious is central to the Zero Trust cybersecurity strategy. All users, devices, and system interactions within a company's network are subject to constant surveillance under this paradigm, which also mandates stringent identification verification and restricted access. FNU Jimmy, 2024, Key components of Zero Trust Security, including Multi-Factor Authentication (MFA), micro-segmentation, Identity and Access Management (IAM), and least privilege access, are described in this study, which delves into its concepts and design. By delving into the reasons for this model's adoption, the article shows how Zero Trust overcomes the shortcomings of traditional security measures, such as their susceptibility to insider attacks and illegal network lateral movement. This article provides a thorough analysis of Zero Trust Security and how it may be used to strengthen cyber defenses in today's complicated digital landscape. It offers practical advice to enterprises who are trying to update their security measures.

Organizations in many different sectors are switching to zero trust cybersecurity from older, perimeter-based approaches. However, a new management strategy is needed for the complicated task of implementing zero trust, which differs from conventional perimeter-based security. Organizations may improve their zero-trust cybersecurity planning, assessment, and management with a well-defined set of key success factors (CSFs). In response, we polled a group of twelve cybersecurity specialists in three-round Delphi research to ascertain their consensus on the CSFs for zero trust cybersecurity implementation. The multi-dimensional CSF framework comprises eight components: identity, endpoint, data, network, infrastructure, visibility, analytics, if/platform, and orchestration and automation. Our intention was to design a framework enabling the evaluation of an organization's zero trust maturity levels, based on such CSFs. William Yeoh, et al., 2023, From both the theoretical and the practical point of view, the study advanced our understanding of enforcing the zero trust across diverse dimensions and at the same time offers a real-world framework for organizations to follow. This will be useful for the stakeholders of zero trust cybersecurity efforts applied by organizations in formulating, assessing, or applying the course of action.

When it comes to cybersecurity, the Zero Trust paradigm has emerged as a fresh perspective that questions traditional perimeter-based approaches. Sandeep Reddy Gudimetla, 2024, By analyzing the concepts underlying access restriction and continual trust testing for internal and external network traffic, this article discusses the implementation and efficacy of Zero Trust systems. This research delves at the potential applications of technologies like as encryption, continuous identification, micro-segmentation, and identity-based access restrictions in environments where trust is thin. The benefits and drawbacks of Zero Trust implementations are

investigated in this article by reviewing empirical evidence and looking at real-life case studies. According to the results, Zero Trust is effective in preventing both internal and external assaults on a network. This makes it a proactive and flexible security architecture that can be used with modern networks.

Cyber threats, especially those made more sophisticated by AI developments, are becoming more complicated and sophisticated, and conventional security measures are not keeping up. Brady D. Lund, et al., 2024, The zero-trust cybersecurity methodology, which helps businesses reduce their exposure to risk by adhering to the "never trust, always verify" philosophy, is described in this article. This paper delves into the practical implementation of zero-trust principles in settings like schools and libraries, where a lot of information is exchanged. It emphasizes the significance of three practices: continuous authentication, least privilege access, and breach assumption. The former takes into account the possibility of a breach and uses multiple checkpoints to limit its spread, while the latter ensures that users only have access to what they specifically need. This research determines possible directions of research that can contribute to the protection of vulnerable organizations.

Hongzhaoning Kang, et al., 2023, The need to adapt to changing security requirements has become increasingly difficult for traditional perimeter-based network security approaches due to the frequency of cross-border access. The guiding principle of this new paradigm in cybersecurity, zero trust, is to "never trust, always verify." Zero Trust is a cybersecurity model that has a new approach following a "Never trust, always verify" principle. By doing away with the lines that normally separate an organization's internal network from its external network, it hopes to mitigate security concerns associated with attacks from within. However, studies on zero trust are in their early stages, and further study is needed to help academics and industry professionals better comprehend the paradigm. This article begins with a discussion of cybersecurity trust before moving on to zero trust's history, ideas, and ideals. Within the framework of zero trust accomplishments and their technological implementations in Cloud and IoT settings, the features, strengths, and shortcomings of the current literature are examined. Lastly, the notion and its existing obstacles are examined to bolster future development and use of zero trust.

3 METHODOLOGY

3.1 Theoretical Structure

System resilience and cyber security are two overlapping issue categories. Cyber resilience analysis may make use of several metrics that were originally developed for other areas. Rather than measuring mission assurance, security metrics often center on security practices and capabilities (i.e., capabilities supporting the security objectives of confidentiality, integrity, availability, and accountability) or metrics relating to asset loss. Figure ES-3 shows that most metrics for system resilience are based on a time-based model of disruption and recovery, which presupposes that detection and reaction can be executed promptly. However, when sophisticated cybercriminals plan attacks, these tasks become much more difficult.

The following are the limitations presented in the existing approaches, such as:

- The integration of very stringent access controls of Zero Trust with the specific TTPs as per MITRE ATT&CK matrix is not going to be easier to implement as it needs considerable skills and resources, given the complexity in implementation. It could certainly add to associated costs and prolonged timelines for implementations, even more for organizations lacking matured security infrastructures.
- The integration between Zero Trust and MITRE ATT&CK would require monitoring, updating, and maintaining them. Keeping ATT&CK updated with threat intel poses a burden on IT budgets and resources, along with constant verification and monitoring of user, device, and network activities.
- Both Zero Trust and MITRE ATT&CK would require constant monitoring of user activities, endpoints, and network traffic. As a result, security teams would be inundated by a wide array of false positives, alert overloads, and the ingrained need to modify their detection systems, which piled up together could contribute to a considerably huge operational handicap.
- While the MITRE ATT&CK Matrix updates this knowledge of new attack techniques on a regular basis, there are sometimes occasions where, in real time, they cannot really represent the latest, most advanced, or unique threats. This can also create challenges in response to such attacks. Consequently, organizations could find

themselves unable to fortify defenses against attackers who have learned to deploy complicated or unusual means to evade detection.

Zero Trust Model (ZTM) is a highly integrated standard, because of several interactions built along the least privilege concept, guaranteeing access to critical systems only by users and devices with the right authority. This, in addition to the threat detection and hunting capabilities powered by the MITRE ATT&CK matrix, will allow security teams to better detect and respond to malicious activity by effectively comparing real-time behavioral activities to known attack geometries. This is an active model in which the ATT&CK matrix is used to observe the traffic inside the network, user activity, and the behavior of the endpoint, while any detected suspicious behavior would trigger automated responses. In addition, the ability of the system to dynamically assess risks and respond to new threats ensures that protective measures evolve along with the tactics employed by malicious cyber foes. The improved threat detection, containment, and mitigation capabilities from this integration, along with the continuous alignment of protective measures with the latest intelligence on attack techniques, would, as a whole, increase the cyber resilience of the organization.

The proposed approach features are listed below:
(i) Make Zero Trust and MITRE ATT&CK your primary focus to improve cybersecurity.
(ii) Prioritize lowering risk by consistently checking each access attempt.
(iii) The MITRE ATT&CK matrix is used to find cyber dangers and how to lessen their impact.
(iv) Frameworks for detecting and responding to threats are integrated with Zero Trust concepts.
(v) Strives to develop a defensive system that is more proactive and adaptive in the face of cyber threats.
(vi) To improve overall resilience, it is encouraged to conduct real-time monitoring and analysis.
(vii) Offers a holistic view of cybersecurity by combining several models.

Establishing new security standards for organizations and enterprises is the goal of implementing the Zero Trust security paradigm. Continuous authentication and dependability verification take center stage in this paradigm, rather than the more conventional VPN or physical network access. Security solutions with more complex features will eventually supersede older ones, or at least adapt to this new paradigm. This would be firewalls, intrusion detection systems, and authentication systems. The method best adjusts concerning complex and diverse network configurations. Thus, users will have secure access to the organizational resources from any device, any time, and from any location. The first step is to gather information on current security models, attack vectors, and patterns, using the guidelines provided by the MITRE ATT&CK methodology. Zero Trust integration with ATT&CK seeks further security through such data. In the input fall, among other things, access control restrictions; system vulnerabilities; threat intelligence reports; network logs; and other information determine which assets are critical and which are users in specific roles and custom access controls. Furthermore, systemic diagram Figure 1, explains the system flow in detail.

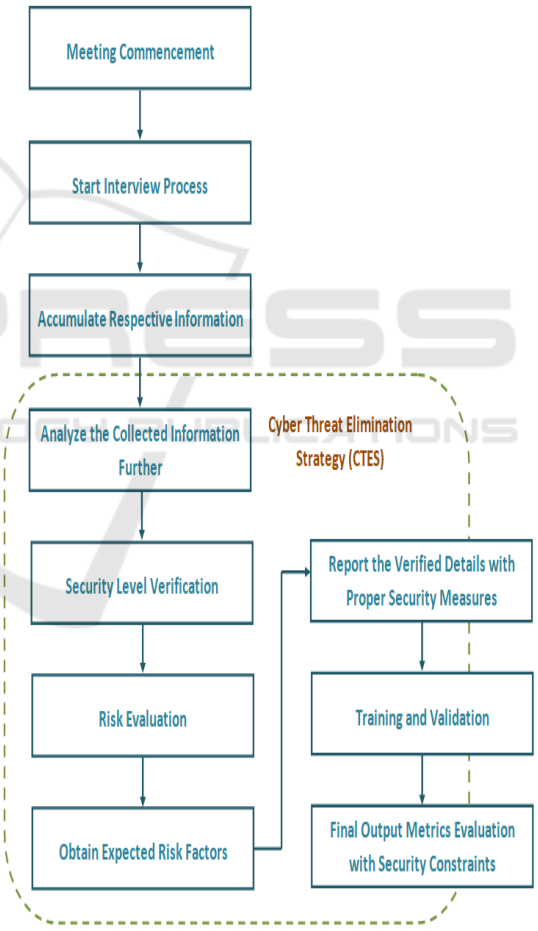

Figure 1: System Flow Diagram.

The integration relies on real-time monitoring to identify anomalous behaviors, thus requiring constant data feeds from endpoints, security tools, and sensors. System configurations, device inventories, and user authentication methods will round off the data input

in building a comprehensive security model. These further stimulate scenarios to evaluate the efficiency of the combined methodology. In essence, an enabling, agile, and self-adjusting input paradigm to build cyber resilience through proactive security framework is the end goal and reports on the state of security, vulnerability scanning, and the effectiveness of implementing the Zero Trust strategy also formed part of the results. It employs the MITRE ATT&CK Matrix to enable detection of threats in real-time and visualization of attack patterns and reactions in dashboards. The outputs are made more user-friendly and let users direct their attention toward concern areas using visual representations such as heat maps and trend graphs. Security event reporting, risk assessment, and post-incident analysis are part of the output and help in making decisions. Suggestions for enhancing further access management, threat detection, and response strategies are provided. In relation to integration, security events are deeply mapped against ATT&CK methodologies to aid in finding the source of an attack. System logs and performance measures provide feedback for repeated fine-tuning of security program deliverables. Ultimately, it provides clear and actionable information to improve cyber resilience and thus support continuous improvement. Every request made by users or access attempts into a system will go through control and authorization based on Zero Trust principles; that concept applies code for real-time monitoring and logging to maintain such integrity. By incorporating aspects of the MITRE ATT&CK Matrix, threats and attack tactics will be matched to better enhance the identification and classification of risks. Risk analysis through pre-defined scenarios, vulnerability analysis, and threat simulations forms part of the code. It identifies potential security threats based on behavioral patterns of network traffic as well as data obtained by endpoints through machine learning techniques. Modular enforcement through coded security rules and policies is based on user role, access requirement, and device condition. The architecture also has flexibility, making it easy to update or add new security measures or threat intelligence streams. There is smooth integration between this code and systems for real-time threat response, as well as security information and event management (SIEM) systems. The code design aims to bring a system environment that is flexible and robust by continuous testing and improvement of the protective measures of the system.

All the necessary tables and fields for a dataset, as well as the design of the business process, are captured in the Dataset Design process. It serves as the center for policy and procedural governance and as the state of the migration to be. This research demonstrates how the approach is implemented through an Android application in another thread. The language, framework, models, alongside all XML, are the tools that the researcher is going to need to design the User Interface. The architecture of the application has been built with the JAVA programming language. This research utilizes Android Studio to write code and it is the backbone of the study. For this design, the author relies on the Android Native Framework. In a nutshell, for an Android app that works with Firebase. In order to provide seamless communication, the author additionally makes use of firebase. One must have access to the internet in order to use this program and clients still need an internet connection to place orders using the application, even though the delivery guy and clients may communicate by phone. With the right setup and mix of hardware and software, the application may become smarter.

4 RESULTS AND DISCUSSION

We conducted independent study on the ZT security approach and the MITRE ATT&CK matrix to determine whether or not these models are effective of a cybersecurity framework. Additionally, we analyzed the impact that the combination of these two approaches has on the enhancement of cyber resilience in government institutions.

4.1 Evaluation of the ZT Cybersecurity Framework

At first, we looked at implementing the ZT model independently. Network traffic security, micro-segmentation, and the enforcement of the concept of least privilege were examined in relation to the ZT model's guiding principle of "never trust, always verify." The evaluation showed that the model successfully reduced the attack surface and mitigated unauthorized access, with notable gains in safeguarding information and network security.

4.2 Evaluation Matrix for MITRE ATT&CK

Subsequently, the MITRE ATT&CK matrix's isolated application was evaluated with an emphasis on its effectiveness in identifying, comprehending,

and preparing for recognized attack vectors. This component was instrumental in improving the capacity of threat intelligence and security teams to anticipate and respond to cyber threats by utilizing documented adversary behaviors and techniques.

4.3 Assessment of an Integrated Strategy

The combined impact of merging the Zero Trust (ZT) model with the MITRE ATT&CK matrix has been investigated after the individual assessments. The objective of this integrated approach was to incorporate the strategic insights provided by the ATT&CK matrix with the proactive defense mechanisms of ZT. The results indicate that the integration considerably enhances an organization's cyber resilience, providing a more comprehensive and dynamic defense mechanism against sophisticated cyber threats. The combination enables the continuous adaptation to new tactics and techniques employed by adversaries, in addition to defending against known threats. In order to assess the efficacy and efficiency of the proposed scheme, the aforementioned models are collectively referred to as the Cyber Threat Elimination Strategy (CTES). This strategy is cross-validated with the conventional security model, the Zero Trust Model (ZTM).

Table 1: Data Frequency Analysis Between CTES and ZTM.

S. No.	Data (kbps)	ZTM (%)	CTES (%)
1.	1000	32.45	73.54
2.	1500	35.14	72.66
3.	2000	31.56	75.66
4.	2500	44.69	79.52
5.	3000	49.70	80.43
6.	3500	53.50	81.51
7.	4000	57.21	82.52
8.	4500	62.61	85.53
9.	5000	66.42	88.66
10.	5500	69.56	88.72

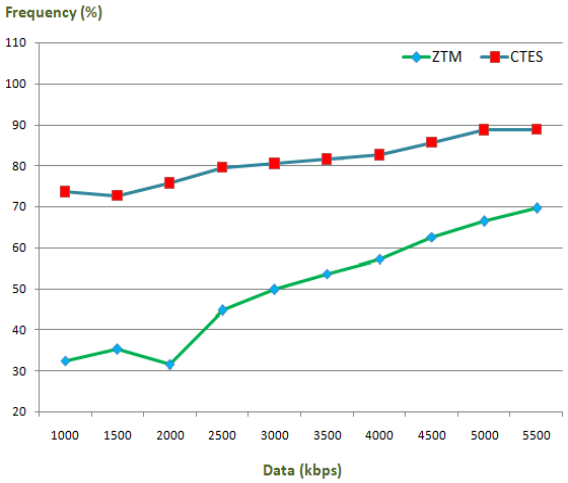

Figure 2: Data Frequency Evaluation.

The data frequency ratio of the suggested method, which is referred to as CTES, is depicted in the accompanying figure, which is referred to as Figure 2. This method is cross-validated with the traditional model known as ZTM in order to assess the data frequency ratio of the proposed scheme. A descriptive representation of the same could be found in the table that follows, which is referred to as Table 1.

4.4 Statistical Evaluation

By tracking indicators like breach detection rate and incident response durations, quantitative analysis was able to determine how long it took for responses to finish after each occurrence and what percentage of incidents were really discovered. After putting the Zero Trust paradigm into practice in government agencies, these measures were utilized to quantitatively assess the effectiveness of security.

Table 2: Data Frequency Analysis Between CTES and ZTM.

S. No.	Data (kbps)	ZTM (%)	CTES (%)
1.	1000	82.63	97.64
2.	1500	84.54	97.72
3.	2000	81.26	96.71
4.	2500	84.39	95.59
5.	3000	89.51	95.64
6.	3500	83.42	96.69
7.	4000	87.39	95.47
8.	4500	82.77	96.58
9.	5000	86.45	97.49
10.	5500	89.61	97.56

Figure 3: Security Efficiency Analysis.

Figure 3 shows the results of comparing the suggested method, CTES, with the standard model, ZTM, in order to determine the security ratio of the proposed scheme. What follows is a descriptive table of the same information, Table 2.

4.5 Acquire Expertise on Qualitative Analysis

Gaining insights from IT managers and security officials about the technical and operational obstacles encountered during the deployment of the Zero Trust model, the feedback acquired through qualitative analysis highlighted the ease of implementation and operational efficiency. We also looked at user and administrative comments on how normal processes become more efficient following the improvement. Such qualitative analytical input was critical in elucidating the difficulties and successes encountered in putting the Zero Trust paradigm into practice. Separate or combined evaluations of the Zero Trust model's and the MITRE ATT&CK matrix's contributions were conducted using time-based and efficiency-based resilience assessment metrics, incident response time and breach detection rate quantitative analysis metrics, and operational efficiency and ease of implementation qualitative feedback metrics. The comprehensive methodology used in this research to improve operational continuity and boost security posture makes it especially useful for public organizations that are confronted with several security concerns. The significance of each module and the enhanced advantages of integration in bolstering cyber defense postures are highlighted by this. It lays forth a transparent plan for public institutions to strengthen their cyber defenses. In addition, this study shows that cyber threat environment is always changing and that adaptive security solutions are necessary. It also points out places where additional research is needed and where improvements might be made. Public institutions may implement a more robust cyber security framework with the help of the clear tactics and recommendations provided by this study. Also, by helping us comprehend cyber risks better, they greatly aid in the creation of strategic reaction measures.

Figure 4 shows the results of comparing the proposed CTES strategy to the standard ZTM model for threat prediction accuracy. The goal of this cross-validation is to see how well the CTES approach performs. Table 3 presents the same information in a descriptive format.

Table 3: Analysis of Threat Prediction Accuracy Between CTES and ZTM.

S. No.	Epochs	ZTM (%)	CTES (%)
1.	1000	85.43	98.72
2.	1500	86.82	98.63
3.	2000	85.71	97.47
4.	2500	84.69	96.38
5.	3000	83.43	96.49
6.	3500	82.55	97.57
7.	4000	85.34	96.56
8.	4500	84.42	97.49
9.	5000	85.56	98.71
10.	5500	84.71	98.66

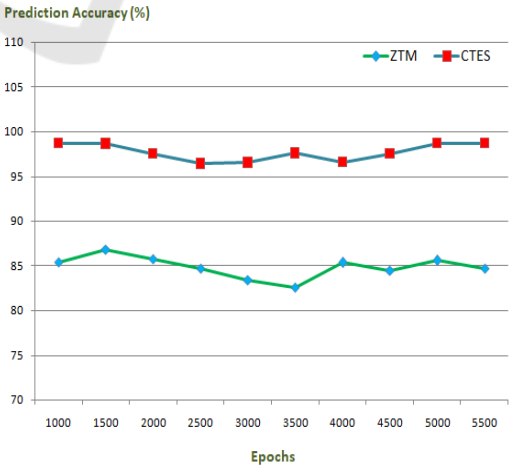

Figure 4: Threat Prediction Accuracy.

Figure 5 shows the total time needed to process the data with the aforementioned clear security

measures using the CTES approach. To evaluate the time ratio of the proposed scheme, it is cross-validated with the ZTM conventional model. Table-4 presents the same information in a descriptive format.

Table 4: Time Requirement Analysis Between CTES and ZTM.

S. No.	Data (kbps)	ZTM (ms)	CTES (ms)
1.	1000	2689	527
2.	1500	3554	638
3.	2000	3789	749
4.	2500	3963	824
5.	3000	4586	963
6.	3500	4977	1058
7.	4000	5397	1163
8.	4500	5818	1269
9.	5000	6238	1375
10.	5500	6658	1481

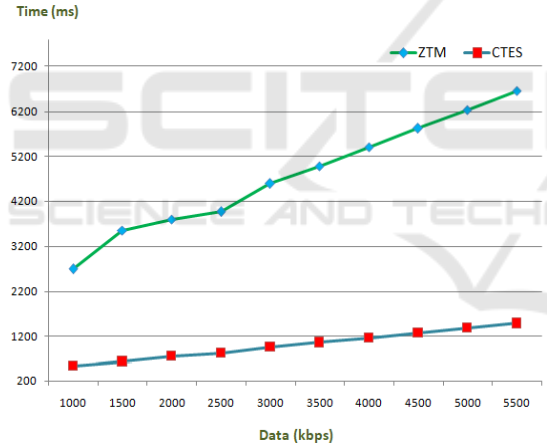

Figure 5: Time Requirements Evaluation.

5 CONCLUSIONS

Jun-Hyung Park, et al., 2025, With an emphasis on measures that systems engineers and program managers may utilize to guide alternative analysis, this study expands upon previous work on cyber resilience metrics. Cyber resilience metrics and efficacy measurements may be established from four separate perspectives: programmatic, engineering, mission assurance, and risk management. It also offers a score system for these indicators. It identifies a vast number of potential metrics, traceable to cyber resilience objectives. It includes a measure template and instructions on how to choose, modify, and define metrics. For anyone looking for a generic resource on how to create and apply cyber resilience measures in a repeatable manner, this paper offers a good place to start. The topic of cyber resilience metrics still has many unanswered questions. Some of these features, as seen below, include the ability to compare, the definition of computationally combinable metrics, and the creation of a score system that systems engineers may utilize to assess different solutions. Consistency in assessment methodologies and assumptions about the metric's relevant context is essential for comparing metric values across companies, projects, or systems. While model-based systems engineering has the potential to capture certain assumptions and calculate model-based metric values, further research is required to identify its limits and provide practical recommendations. Having a standard way to describe enemies is one potential foundational element. Cyber resilience considerations at the level of a critical infrastructure sector, a region, or a collection of businesses executing a mission or business function is attractive when expressed in terms of a single figure-of-merit that allows comparison, such as a FICO-like score. On the other hand, there are certain recognized hazards associated with these types of ratings. For example, they don't take organizational size or mission into account, they rely on outdated threat models or standards of practice, and they promote a compliance mentality instead of a risk management one. As the research progresses, it will become clear that this reasoning needs improvement. To make sure security measures are effective and easy to maintain, more study might look at improved user experience design. To conclude, strengthening cyber resilience in the long run may be achieved by extending the framework to include increasingly advanced persistent threats.

REFERENCES

Brady D. Lund, et al., "Zero Trust Cybersecurity: Procedures and Considerations in Context", Encyclopedia, 2024.

Chunwen Liu, et al., "Dissecting zero trust: research landscape and its implementation in IoT", Cybersecurity, 2024.

FNU Jimmy, "Zero Trust Security: Reimagining Cyber Defense for Modern Organizations", International Journal of Scientific Research and Management, 2024.

Hongzhaoning Kang, et al., "Theory and Application of Zero Trust Security: A Brief Survey", Entropy, https://doi.org/10.3390/e25121595, 2023.

Jun-Hyung Park, et al., "A Proposal for a Zero-Trust-Based Multi-Level Security Model and Its Security Controls", Appl. Sci., 2025.

Kehe Wu, et al., "Design and Implementation of the Zero Trust Model in the Power Internet of Things", International Transactions on Electrical Energy Systems, 2023.

Naeem Firdous Syed, et al., "Zero Trust Architecture (ZTA): A Comprehensive Survey", IEEE Access, 2022.

Naga Vinod Duggirala, "Zero Trust Security: Redefining Data Protection in the Digital", International Research Journal of Engineering and Technology, 2024.

Nisha T N, et al., "Zero trust security model: Defining new boundaries to organizational network", Proceedings of the 2023 Fifteenth International Conference on Contemporary Computing, 2023.

Onome Edo, et al., "Zero Trust Architecture: Trend and Impact on Information Security", International Journal of Emerging Technology and Advanced Engineering, 2022.

Sandeep Reddy Gudimetla, "Zero Trust Security Model: Implementation Strategies and Effectiveness Analysis", International Research Journal of Innovations in Engineering and Technology, 2024.

Shaikh Ashfaq, et al., "Zero Trust Security Paradigm: A Comprehensive Survey and Research Analysis", Journal of Electrical Systems, 2023.

William Yeoh, et al., "Zero trust cybersecurity: Critical success factors and A maturity assessment framework", Computers & Security, 2023.

Yiliang Liu, et al., "Zero Trust-Based Mobile Network Security Architecture", IEEE Wireless Communicatio n, 2024.

Zillah Adahman, et al., "An analysis of zero-trust architecture and its cost-effectiveness for organizational security", Computers & Security, 2022.