International Journal of Science and Research Methodology (IJSRM)
Volume 29, Issue 5, May 2026 ijsrm.humanjournals.com ISSN: 2454-2008

Zero-Trust Intelligent (ZTI) Model for Mitigating and Controlling Negligent Insiders Threat in a Medium-Scale Enterprise

Ibeneme-Sabinus I. L.[1], Martins C.O.[2], Amaka E. N.[3], Ewunonu T. C [4], Nworuh G. E.[5], Okon I. A.[6], Ugbor I. C.[7]., Okonkwo T. O.[8]

[1,2,3,4,5,6,7] Department of Cybersecurity, Federal University of Technology Owerri, Nigeria.
[8] Department of Information Technology, Federal University of Technology Owerri, Nigeria.

Received: 21 March 2026 Revised: 11 April 2026 Accepted: 23 April 2026

ABSTRACT-.

Negligent Insider Threat (NIT) is a type of cyberattack originating from an individual who works for an organization or has authorized access to its networks or systems. It is a type of insider threat that could be perceived as the easiest launched threat in the internet as the perpetrator seen as formal employee or a fired employee firing back using their authorized access to an organization's data and resources to harm the company's equipment, information, networks, and systems This research paper addresses the Negligent Insiders' Threat (NIT) where employee in an organization unintentionally fall prey to scammers by leaking organization's sensitive information to the public domain. The study deploys a Zero Trust Architecture Model (ZTAM) that advocates for the principle of "Never Trust, Always Verify {NTAV}." This model requires that for every access attempt, whether from inside or outside, the network must be thoroughly verified and continuously monitored by organization's System Analyst by exhibiting different interrogative agreed layout questions within the organization, where each PC is assigned to different employees (Emp) through an Information Control Unit (ICU). The ICU monitors all entrance such as "Source and Destination of the information as well as User behaviour within the system, which will assist in directing the user to it destination if correctly answered, it will assist in restricting most redirected information and intentionally exposing organization's information to the public domain and when not trusted be quickly disconnected by the stationed analyst.

Keywords: Zero Trust Architecture, Never Trust t, Always Verify.

INTRODUCTION

Insider threat is a cybersecurity risk which originates within an organization, posed by some individuals: a current or former employee, consultant, board member, or business partner and could be intentional, unintentional, or malicious. who has authorized access into organization's data or information and deem it fit to misuse privileges given to them by stealing data and compromising sensitive information [4]. These Individuals are capable of causing data and financial losses, or operational disruptions [2]. Insider's cyber threat now accounts for roughly 60% of all data breaches in most organizations, with over half resulting from employee error in dealing with sensitive documents [5]. The threat has always been in forefront, often serving as one of the entry points for malicious activities, which leads to greater disruptions and losses [6]. These threats can be intentional, unintentional, or the result of compromised accounts. Its motivations by the perpetrators range from financial gain and system disruptions [7]. This type of Threat has created a significant challenge to modern cybersecurity activities, as they emanate from individuals within an organization who have access to critical systems and data [1]. Organization's data is identified as the most crucial intellectual property, and any compromise could cripple the entire operation, leading to long-lasting reputational damage and risks associated with the law of breaching confidential organization's data [3]. **I**nsider's threats are categorized into Malicious, Negligent, and Compromised (Figure 1).

International Journal of Science and Research Methodology (IJSRM)
Volume 29, Issue 5, May 2026 ijsrm.humanjournals.com ISSN: 2454-2008

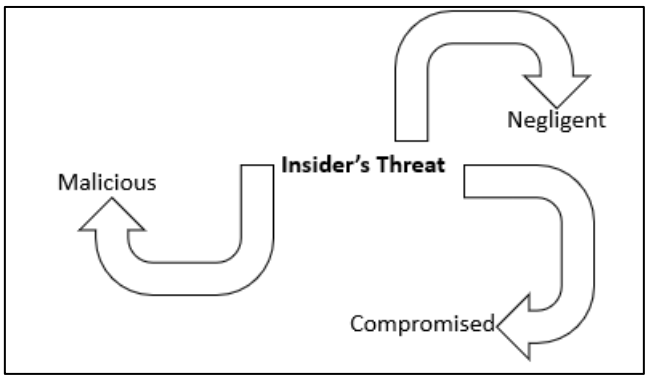

Figure 1: Illustrating Various Types of Insider's Threats

The malicious insiders' threat intentionally misuse their access for personal gain, revenge, or other harmful reasons. Negligent insiders' threat cause harm unintentionally through carelessness, errors, or ignorance of security policies, such as falling for phishing scam. Compromised insiders' threat are individuals whose accounts or access have been hijacked by an external attacker. Consequently, mitigating this type of threat requires a combination of technological solutions and human-oriented strategies, such as behavioral analytics pattern and concentrated Cybersecurity training practices. This research paper addresses the Negligent Insiders' Threat (NIT) where employee in an organization unintentionally fall prey to scammers by leaking organization's sensitive information to the public domain. The study deploys a Zero Trust Architecture Model (ZTAM) that advocates for the principle of "Never Trust, Always Verify {NTAV}." This model requires that for every access attempt, whether from inside or outside, the network must be thoroughly verified and continuously monitored by organization's System Analyst by exhibiting different interrogation agreed layout questions within the organization.

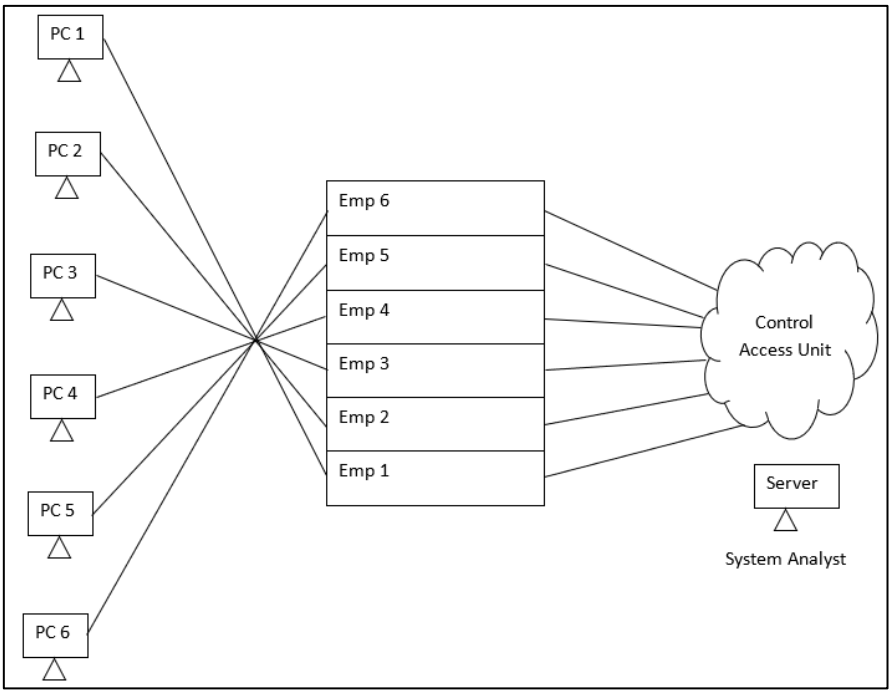

Figure 2: Information Control Unit (ICU)

The diagram in figure 2 demonstrates how each PC is assigned to different employees (Emp). It exhibits that every access and communication linked to the organization will be solely managed by a System Analyst. The ICU monitors all communications as well as User behaviour within the system. The model suggested that by close monitoring practices in the organization by the system analyst through a structured interrogative section with a particular PC, before access is granted to such PC (Emp), will go a long

way in addressing some kind of negligence put up by most employee of any reputable organization and maintain direction to every entrance into system.

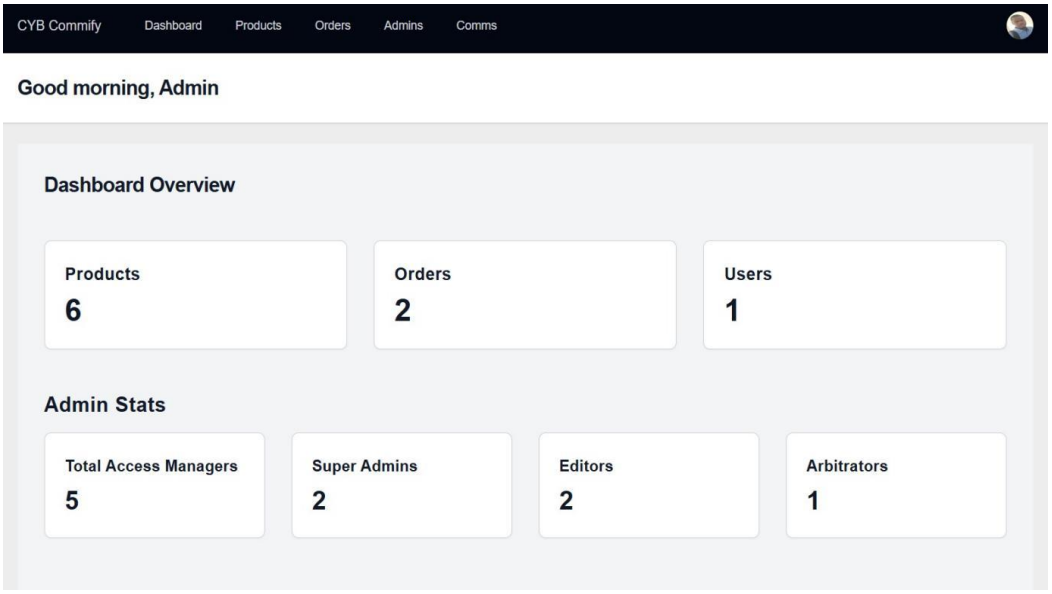

Figure 3: User Interface of the Developed System

Figure 3 shows the interactive section between organization's System Analyst and each employee (Emp) of a system This illustrates that before any transaction is made within the organization, access must be granted to monitor all entrance such as "Source and Destination of the information" by simple interrogation section between the system analyst and the concern PC which will assist in directing the user to it destination if correctly answered.

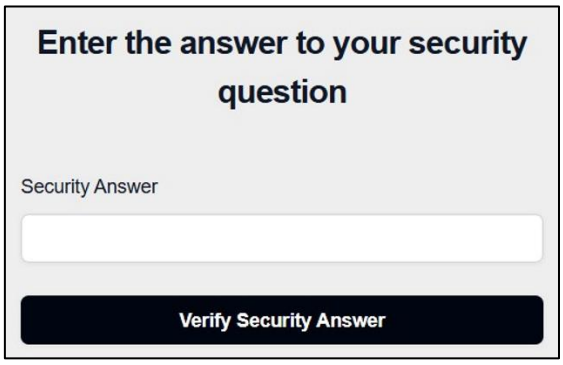

Figure 4: Security Question Verification

This section handles the question verification section where a correct answer to a question is inputted as the System Analyst monitors the technicality of every answer given for onward accessing and processing among concerned PCs (Figure 4). These will go a long way in restricting most redirected information and intentionally exposing organization's information to the public domain. By the verification of each entrance from Emp of each PC from a user, a highlight of the Source/Destination of such information will definitely be made and when not trusted be quickly disconnected by the stationed analyst.

Conclusion

This model was designed to improve security in medium scale enterprise. It provided an insight into the different types of insider's threat, understanding the various types of insider's threat and the unique features, attributes and importance of building a secured model architecture capable of defending and protecting users' systems and networks from insider's threat invasion. However, it is worth mentioning that this paper is not in itself exhaustive, rather it is meant to provide valuable background information on this type of threat. However, the study was limited by the testing scope, which occurred in controlled environments, and the time

constraints that restricted broader refinement. Despite these challenges, the research has laid a solid foundation for future advancements, showcasing the feasibility and importance of integrating innovative technologies to tackle evolving threats.

REFERENCES

1. Nonso Okika, Onum Friday Okoh, Ekom Emmanuel Etuk (2025) Mitigating Insider Threats and Social Engineering Tactics in Advanced Persistent Threat Operations through Behavioral Analytics and Cybersecurity Training. International Journal of Advance Research Publication and Reviews Vol 2, Issue 3, pp 11-27, March 2025.
2. Waiganjo, I.N. and Nandjenda, L.S. (2025) Unveiling Insider Threats: Examining Vulnerabilities in an Organizational Structure: A Case Study of NamPost. *Open Access Library Journal*, **12**, 1-1. doi: 10.4236/oalib.1112797.
3. Temitope Oyinkansola Asade, Olutoye Ransome-Kuti, Ojonoka Erika Atawodi, Oyindamola Omolayo, Nonye Fortune Lesinwa &Tolulope Awe (2025). Mitigating Insider Threats with Advanced Cyber-Security Measures in Nursing Staffing Agencies. Journal of Information Engineering and Applications www.iiste.org,ISSN 2224-5782 (print) ISSN 2225-0506,Vol.15, No.2, 2025.
4. Akinde Michael Ogunmolu (2025) Insider Threats in Energy Facilities Using Biomechanical Access Control and Al-Based Cybersecurity. Journal of Engineering Research and ReportsVolume 27, Issue 6, Page 65-82, 2025;Article no.JERR.136833ISSN: 2582-2926.
5. Sharon L. Burton (2025) Unmasking Insider Cybersecurity Threats in Aviation and Aerospace. Published by IDEAS SPREAD. Law, Economics and Society; Vol. 1, No. 2; 2025 ISSN 3066-9340 E-ISSN 3066-9359 https://doi.org/10.30560/les.v1n2p1.
6. Raman biju, Burhanuddin Moeez, Sushant Sonkusare & Pushpalata Aher (2025) Defense Sphere: A Comprehensive Solution to Insider Threats. International Journal of Research Publication and Reviews, Vol (6), Issue (4), April (2025), Page – 13823-13829. Journal homepage: www.ijrpr.com ISSN 2582-7421.
7. Ofori, H.K.; Bell-Dzide, K.; Brown-Acquaye, W.L.; Lempogo, F.; Frimpong, S.O.; Agbehadji, I.E.; Millham, R.C. (2025) Application of Machine Learning and Deep Learning Techniques for Enhanced Insider Threat Detection in Cybersecurity: Bibliometric Review. Symmetry 2025, 17, 1704. https://doi.org/10.3390/ sym17101704.

How to cite this article:
Ibeneme-Sabinus I. L et al. Ijsrm.Human, 2026; Vol. 29 (5): 12-15

Conflict of Interest Statement: All authors have nothing else to disclose.