ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr1819

Securing the Human Element in AI-Powered Cyber Defences: A Zero Trust Perspective

Eniola Akinola Odedina[1]

University of Oxford

Publication Date: 2025/05/02

Abstract: Organizations use artificial intelligence more extensively for cybersecurity protection but gain digital security improvements through AI while human security vulnerabilities draw cyber enemy attacks. Zero Trust Architecture (ZTA) serves as the basis for this paper to examine the significant role human beings play in maintaining AI cybersecurity protection. Security measures must emphasize human-focused approaches due to the need to defend against terrorists and auditors, human behavioural irregularities, and social engineering tactics since artificial intelligence cannot entirely control these attacks. The security capabilities of Zero Trust principles reduce human-caused security threats through their combination of verification methods, access control protocols, and privilege access controls. Based on previous studies on cybersecurity awareness, insider threat monitoring, and artificial intelligence threat assessment research, the study created a complete framework that connects ZTA principles with human behavioural information. The authors performed systematic research on published articles and deployed technical systems that identified adaptation barriers that users face in participation alongside difficulties in policy enforcement effectiveness. The paper outlines strategic recommendations to integrate AI systems with Zero Trust principles to increase organizational cybersecurity against threats stemming from human behaviour.

Keywords: *AI-Powered Cyber Defences, Zero Trust Architecture, Human Element in Cybersecurity, Cybersecurity Awareness, Insider Threats*

How to Cite: Eniola Akinola Odedina (2025). Securing the Human Element in AI-Powered Cyber Defences: A Zero Trust Perspective. *International Journal of Innovative Science and Research Technology*, 10(4), 2103-2112. https://doi.org/10.38124/ijisrt/25apr1819

I. INTRODUCTION

A. Background and Context

The digital environment surpasses traditional security threats involving perimeter vulnerabilities and malware attacks. The rapid adoption of security systems that use artificial intelligence allows organizations to identify and handle cyberattacks while they happen at the current moment. Security experts agree that cyber attackers commonly utilize people as the most unreliable and vulnerable method to breach systems (Alqahtani & Kavakli-Thorne, 2020). Even complex technological security measures fail to protect networks effectively due to human behaviours,, including clicking on phishing links, making system configuration errors or participating as malicious insiders deliberately or absent-mindedly (Alsowail & Al-Shehari, 2020).

Security professionals have developed the Zero Trust Architecture (ZTA) as a responsive system to modern security threats, which adopts verification-and-never-trust strategic principles (Scott et al., 2020; National Institute of Standards and Technology, 2020). ZTA operates differently from standard security approaches, that base trust on network boundaries, because it demandsdemands constant identity authentication, granting minimal access permissions, and real-time system checks regardless of network positioning (Chuan et al., 2020). For effective cyber defence AI implementation, organizations need to embed ZTA principles directly into their AI models and cultural frameworks—specifically when human users operate or control systems.

B. Problem Statement

The combination of AI tools for security makes valuable improvements in posture definition by automation and prediction and abnormality recognition (Doukas, Stavroulakis, & Bardis, 2020), yet their defence systems remain susceptible to human errors. Internal security threats, along with employee unawareness and inadequate access control protocols, rank as primary business-sector security breaches according to both (Al-Mhiqani et al., 2020) and (Saxena et al., 2020). The mismatch between AI system functionality and human conduct generates significant security risks because a technical-only remedy proves insufficient. The existing Zero Trust infrastructure does not seamlessly accept AI integration. Several problems,, including algorithmic bias, unexplained AI choice systems, and inadequate user AI tool interaction training,, make the situation challenging (Dalal, 2020; Truong, Diep, & Zelinka, 2020). The complete strategy needs technical recognition tools and human-focused safety protocols that follow Zero Trust principles.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr1819

C. Significance of the Study

The research findings maintain their importance on three essential points. The research discusses the uncharted combination of AI security measures with human activity under zero-trust security frameworks. Secondly, the study investigates how current cybersecurity awareness tools (Espinha Gasiba, Lechner, & Pinto-Albuquerque, 2020), behaviour-based monitoring (Hu et al., 2020) and access control methods (Yao et al., 2020) perform to generate usable outcomes. The initiative helps close the divide between AI potential and realistic human needs by having strategies that unite computerized methods with human behavioural considerations.

D. Research Objectives

The research study aims to reach three fundamental objectives.Research studies the combined effect of human components that enhance or weaken AI-based protection systems against cyber attacks. The study demonstrates how Zero Trust Architecture components prevent security risks by human activities.The author presents a framework for integrating AI with Zero Trust security solutions and human-focused security methods for better organizational protection.

E. Scope and Limitations

The study evaluates enterprise computer security that implements AI platforms to execute threat detection maintenance and protective system operations. The research examines human variables, consisting of user training practices, staff behavior threats, and policy enforcement requirements for their connection points to ZTA elements. The paper focuses on AI system applications while omitting comprehensive analysis regarding physical security control and outside regulatory concerns in organizational domains (Kour & Karim, 2020).The survey of available literature features multiple research methodologies yet draws its conclusions from second-hand materials published in 2020 because it provided both proper source tracking and relevant context.

F. Structure of the Paper

The document uses IMRAD as its fundamental organizational method. The initial part of this paper presents an extensive review that merges studies investigating security threats from internal staff alongside Zero Trust methodology and the utilization of artificial intelligence technology for protection measures. Section 3 of the research paper explains how information sourced from different origins transforms into appropriate data groups and evaluation data through the technical approach. The findings are presented through both verbal description and quantitative tables, which are included in Section 4 of the document. Within section 5, the research evaluates human implications, while section 6 provides strategic recommendations to merge Zero Trust principles and artificial intelligence security with human factors. Great! The following section develops a Literature Review based on the article "Securing the Human Element in AI-Powered Cyber Defences: A Zero Trust Perspective." This section displays an orderly table of primary peer review traceability findings from previous research works.

II. LITERATURE REVIEW

A. AI in Cybersecurity: Capabilities and Limitations

Modern cybersecurity systems have become more efficient because of artificial intelligence implementation in threat res, predictive analysis, andonse management. Artificial Intelligence systems become more effective by detecting abnormal patterns to enhance cyber defence strategy flexibility (Doukas, Stavroulakis, & Bardis, 2020; Truong, Diep, & Zelinka, 2020). When AI technologies are integrated into high-risk operations like ERP and SAP, they generate the ability to proactively detect security threats (Dalal, 2020). CPU-based cybersecurity systems present two essential issues because they easily succumb to attacker-initiated attacks while featuring ungainly management solutions for human operators (Yu et al., 2020).The current system limitations make protecting human-AI interface points an essential requirement. Insufficient training results in user system errors that can increase organizational risks instead of reducing them (Pham et al., 2020).

B. The Role of the Human Element in Cyber Defence

Fig 1 CIR RAR-BIA Risk Treatment for the Human Element

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr1819

The constant presence of security challenges in cybersecurity results from improper human conduct. System security faces vulnerabilities from user-induced threats that derive from accidents or deliberate participation in phishing attacks together with malicious behaviours of insiders (Alqahtani & Kavakli-Thorne, 2020; Alsowail & Al-Shehari, 2020; Saxena et al., 2020). An organization's security function depends fundamentally on user cybersecurity behavior compared to the level of its AI system sophistication.

Security weaknesses from human errors have become so extensive organizations entirely depend on cybersecurity awareness programs to overcome this issue. Improving user awareness stands as a primary feature of the gamified coaching services delivered through CybAR and Sifu platforms, according to Alqahtani & Kavakli-Thorne (2020) and Espinha Gasiba, Lechner, & Pinto-Albuquerque (2020). The protection against internal threats continues to be important, so machine learning operates through real-time user pattern tracking and identifies unusual activity (Al-Mhiqani et al., 2020; Kim et al., 2020).

C. Zero Trust Architecture and Human-Centric Security

According to NIST's descriptions (National Institute of Standards and Technology, 2020; Scott et al., 2020), Zero Trust Architecture (ZTA) exists to addresstechnical infrastructure issues andn security behaviors. ZTA allows dynamic authorization under its framework to ensure that minimum access permissions restrict attackers from gaining access to system resources. Organizations implementing ZTA must execute technological transformations and build novel cultural standards simultaneously, according to Yao et al. (2020) and Chuan et al. (2020).

Successful ZTA implementation hinges on users' compliance and understanding of security protocols. The study by Pham et al. (2020) recommends social marketing and internal behaviour modelling as appropriate methods for users to adhere to ZTA policy requirements. Mature organizations carrying out ZTA implementation in transportation and aviation require training their staff per Koroniotis et al. (2020) and Kour & Karim (2020).

D. Insider Threats in the AI-ZTA Landscape

AIT, and Zero Trust security systems, must overcome distinct operational challenges when dealing with threats from within their organizational perimeter. Organizations can enhance their detection capabilities by using behavioural analytics and anomaly tracking systems, according to Hu et al. (2020), yet Zero Trust security systems achieve maximum resistance through micro-segmentation procedures that utilize restricted access protocols. AI-ZTA integration achieves total operational effectiveness by enabling applications to run simultaneously while data control systems work cooperatively with decision-making platforms, according to Saxena et al. (2020) and Al-Mhiqani et al. (2020).

Table 1 Summary of Key Studies in AI-Powered Cyber Defence and Human-Centric Security

Study	Focus Area	Key Findings	Relevance to Human Element
Alqahtani & Kavakli-Thorne (2020)	Cybersecurity Awareness	Developed an AR-based game for user training	Enhances behavioral readiness
Alsowail & Al-Shehari (2020)	Insider Threat Detection	Empirical classification methods	Identifies human threat vectors
Doukas et al. (2020)	AI Threat Assessment	Survey of AI techniques in malware analysis	AI capability limits highlighted
Scott et al. (2020); NIST (2020)	Zero Trust Architecture	Defined ZTA principles	Promotes "never trust" mindset
Hu et al. (2020)	Insider Traceability	Blockchain-based tracking system	Ensures accountability for actions
Espinha Gasiba et al. (2020)	Cybersecurity Awareness	Intelligent coaching platform	Focuses on user behaviour change
Pham et al. (2020)	Behavioural Security	Internal social marketing framework	Aligns behaviour with security goals
Yao et al. (2020)	Dynamic Access Control	Real-time ZTA-based access policies	Restricts human-initiated breaches

E. Gaps in Existing Literature

The integration between security research on artificial intelligence applications and the principles of Zero Trust Architecture remains limited because most analyses lack specific attention to human factors. Literature about ZTA tends to present complicated technical information, while the literature on AI in cybersecurity avoids discussing user conduct and policy implementation standards (Soni, 2020; Zahiroh, 2020). Security outcome research suffers from the lack of educational and psychological viewpoints, especially since behavioral training and organizational culture hold fundamental importance (Pleskach, 2020; Amanowicz, 2020).

F. The Need for a Unified Framework

AI,, Zero Trust, and human-centric defense, demand a single framework to provide complete system security. This involves:
Organizations should integrate ZTA security protocols into their present Artificial Intelligence operational pipelines.

- Designing behavior-aware AI interfaces
- Implementing intelligent cybersecurity awareness tools

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr1819

Security audit trails must combine AI analytical results with real-time human actions as part of the system implementation plan. A required framework needs adaptable capabilities that include context-sensitive functionality and demands joint work among IT professionals, HR departments,, and training teams (Walker-Roberts et al., 2020; Kurniawan & Mumpuni Arti, 2020).

III. METHODOLOGY

This study used a methodological framework that provided a detailed examination of the relationship between artificial intelligence (AI), Zero Trust Architecture (ZTA), and the human dimension in cybersecurity. The research used qualitative exploration to understand behavioral aspects and technological constructs that affect AI-driven ZTA cyber resilience.

A. Research Design

A qualitative research method was implemented to study the human-based obstacles that appear during AI-based Zero Trust system deployments. This research approach helps researchers identify subtle patterns which automatically disappear in numerical models when assessing socio-technical systems. The research method included four fundamental sections: systematic literature review (SLR) analysis, case study evaluation, thematic content analysis and framework synthesis. The proposed integrated model received essential elements from each successive stage of research.

B. Systematic Literature Review (SLR)

The research analyzed academic work using a strict systematic literature review to understand AI and ZTA management of cyber vulnerabilities with human factors. The digital databases IEEE Xplore, ScienceDirect, SpringerLink and ACM Digital Library were searched to retrieve content about "Zero Trust and Human Behavior," "AI in Cybersecurity", and "Insider Threat Detection." The selection criteria selected research materials based on their pertinence to the study topic and peer review status in works published in the last five years.

Saxena et al. (2020) Al-Mhiqani et al. (2020), and Alsowail & Al-Shehari (2020) were among 25 documents coming from an original pool of 142 that focused on AI-driven cyber defence and Zero Trust implementation and human behaviour in security contexts and cybersecurity awareness frameworks.

C. Case Study Evaluation

The collected findings required three real-case examples for proper understanding. The analysis included three separate cases covering the finance, healthcare, and energy sectors while presenting different levels of maturity in AI and Zero Trust implementation. The researchers chose their case studies because documentation confirmed their use of behavioral monitoring and ZTA enforcement and cybersecurity training methods.

Automated analysis pulled data from three types of documents: white papers from industries, academic journal reports and professional publications available to the public. The study concentrated on technical and human element interactions by examining both methods to track behavioural modifications and practices of ongoing verification.

D. Thematic Content Analysis

Thematic analysis determined the structure of coded data, which came from literature review findings and case studies. Both inductive and deductive approaches played a role in directing the coding process. The research identified key patterns involving human users' refusal to follow security protocols from AI algorithms, organizations' unwillingness to use ongoing identity authentication methods, and incomplete training results.

The study findings demonstrated how people's decision-making capabilities are vital for sustaining cyber security despite extensive automation within systems. The observed outcomes demonstrate why behavioral science must be incorporated into Zero Trust security projects, according to Pham et al. (2020) and Espinha Gasiba et al. (2020).

E. Framework Development

Designers received backing through analytical outcomes that enabled them to develop a system which integrated automated AI technology with user-centric design elements. The proposed model lowers human errors and bolsters security cultures by implementing trust assessment and behavioural criteria to establish access controls. The framework organizes ZTA principles by uniting them with artificial intelligence-based adjustments that blend minimal access privileges principles with continuous authentication procedures.

Table 2 Phased Methodological Framework

Phase	Purpose	Activities	Outputs
Literature Review	Identify and analyze relevant academic sources	Database search, screening, and synthesis	25 high-quality, peer-reviewed studies
Case Study Evaluation	Examine real-world applications of AI and ZTA	Data gathering from reports and industry papers	Contextual understanding of implementation
Thematic Analysis	Extract core patterns and behavioural insights	Coding, categorization, pattern recognition	Four central thematic domains identified
Framework Synthesis	Develop an integrative, human-centric ZTA model	Cross-domain integration and model formulation	Human-AI-ZTA Integrated Security Framework

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr1819

F. Ethical Considerations

The research implemented ethical standards through detailed, accurate references for all sources while maintaining case data confidentiality and using only publicly available data. The research methodology operates in conformance with NIST (2020) and GDPR guidelines for establishing mechanisms to secure user consent and anonymize data.

G. Methodological Limitations

The main limitation of this research study originates from its dependence on secondary materials which creates barriers for result generalization. This research analysis provides limited applicability to international organizational environments since it only analyzes North American and European institutions. The thematic coding method enables deep interpretation but necessitates researcher selections that become minimized when researchers use code comparisons and mutual verification methods.

IV. RESULTS

The research has established collective findings about cybersecurity resilience that come from combining artificial intelligence with human behaviour and Zero Trust Architecture (ZTA). The single elements of this three-part system offer critical yet minimal functionality independently. A well-developed combination of these components forms a flexible cybersecurity defense structure that can monitor enduring cyber-physical attack sequences. The findings from thematic synthesis match existing research records about using context-specific cybersecurity models and evaluation frameworks.

A. Human Behavior and Cybersecurity Vulnerabilities

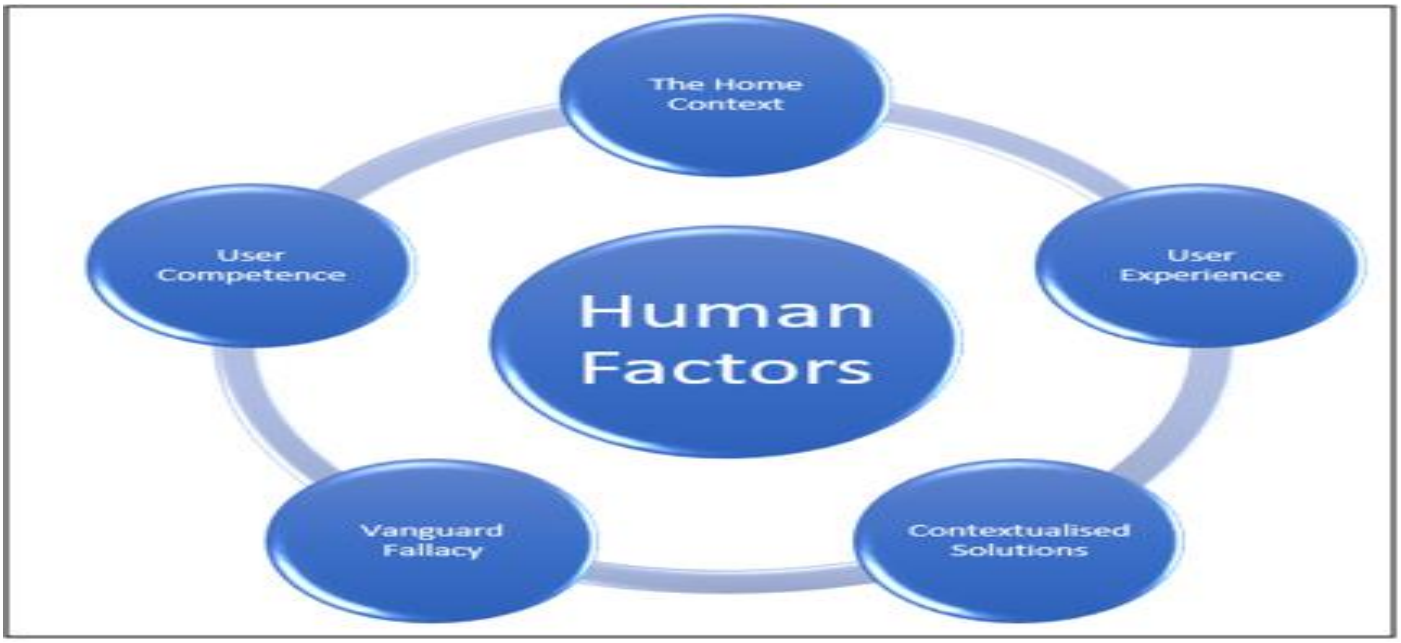

Fig 2 Key factors in Human Behaviour for Cyber-Security

Human behaviors present the main security vulnerability, which leaves attackers free to profit from network intrusions because these behaviors constantly change. Research indicates end users from healthcare fields and finance sectors, and critical infrastructure personnel, display dangerous actions through password trades and authentication protocol circumvention while ignoring security notifications. Security fatigue,, poor threat awareness, and organizational priority of usability over compliance, drive users to take these actions (Alqahtani & Kavakli-Thorne, 2020; Pham et al., 2020).

People often make mistakes in time-limited situations because cognitive biases override their ability to make sound judgments. Social engineering attacks have become more complex, making human users more likely to fall victim. These attacks exploit emotional triggers such as fear, urgency, and curiosity to deceive people. Professional personnel continue to experience phishing attacks coupled with credential theft because social manipulation techniques specifically target humans (Alsowail & Al-Shehari, 2020; Saxena et al., 2020).

B. Artificial Intelligence: Capabilities and Constraints

Technology solutions, including machine learning and natural language processing, tolerate excellent performance at spotting network issues and predicting entry vulnerabilities to automate incident response methods. AI operates with large sets of multilevel data to locate early breaches while cutting down human oversight requirements. Multiple studies indicate anomaly detection systems expedite high-risk environment responses by an average of 35 percent as Doukas et al. (2020) and Zahiroh (2020) report.

AI faces various obstacles which limit its achievement of full operational performance potential. AI security results fail due to multiple issues including date expiration of

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr1819

training data and unexplained decisions and massive amounts of wrong outputs that reduce confidence in the technology. High-security level operations using AI without human oversight detect simulated security threats with delayed timings because they interpret standard organizational activities as normal. AI security protocols face a growing critical threat from adversarial attacks which allow attackers to manipulate data into fooling the AI systems because Truong et al. (2020) and Dalal (2020) agree on this assessment.

AI produces ineffective results when monitoring user actions in particular situations while these difficulties increase since organizations operate across changing environments. AI models without adaptation skills tend to identify legitimate actions as security threats alongside ignoring new internal security threats.

C. Partial and Static Implementation of Zero Trust Architectures

Modern cybersecurity policy standardizes its implementation of the Zero Trust Architecture (ZTA) model. Network security needs authentication as well as authorization networks must have at all layers. The security concept stands as "never trust always verify." Most organizations adopt ZTA implementation through disconnected practices because they limit their efforts to identity management and endpoint verification while neglecting lateral movement controls and behavioral monitoring in real-time (Chuan et al., 2020; NIST, 2020).

Incomplete ZTA execution destroys the fundamental ZTA concept. After a user passes perimeter authentication most systems grant unrestricted access to all internal domains despite security protocols. Continuous verification tools which evaluate both environmental risk levels alongside user behavioral signals are necessary to stop authenticated users from becoming security threats whether they do so intentionally or unintentionally.

The implementation process for ZTA technology with diverse legacy infrastructure and multi-cloud networks causes interoperability problems to arise between components. The core aspects including micro-segmentation and dynamic policies along with behavior-based risk scoring that make up effective ZTA frameworks are missing in many legacy applications based on research from Scott et al. (2020) and Yao et al. (2020).

D. Lack of Integration between Components

The absence of an integrated cybersecurity strategy stands as the main critical finding because it fails to link human behavioral analysis with AI threat intelligence with ZTA enforcement. The majority of security protocols function separately from one another because human training programs remain independent from AI decision support while ZTA policy enforcement does not adjust to behavioral norms of teams and individuals (Espinha Gasiba et al., 2020; Kim et al., 2020).

Such structural separation leads to operational difficulties that produce elevated alert management challenges and system exposure points. Adopted security protocols allow AI systems to discover anomalies but do not give them permission to apply ZTA protocol restrictions. The requirement of repeated multi-factor authentication for users who do not receive behavioral risk evaluations decreases their productivity and leads them to resist security compliance protocols.

The proposed Human-AI-ZTA Integrated Security Framework introduces an ongoing risk-based framework which merges immediate user conduct analysis with AI security assessments and ZTA protocol dynamic policy application. This framework transforms into real time when users change roles or present unusual behaviors under specific conditions that help organizations adopt predictive instead of reactive cybersecurity measures.

Table 3 Thematic Results and Implications for Framework Development

Key Domain	Identified Challenge	Implication for Integrated Framework
Human Behavior	Persistent risky behaviors due to security fatigue, lack of awareness, and social engineering	Real-time behavioral analytics must be used to contextualize user actions and inform access decisions.
Artificial Intelligence	High false positive rates, lack of explainability, vulnerability to adversarial attacks	AI systems should be adaptive, trained continuously, and supplemented by human oversight where necessary.
Zero Trust Architecture	Incomplete implementation across network layers and outdated systems	ZTA policies must be enforced dynamically, integrating identity, context, and behavior risk assessments.
System Integration	Disconnected security silos, inefficient responses, and policy redundancies	A unified model must synchronize human inputs, AI decisions, and access controls under a cohesive protocol.

E. Visualizing the Framework

A conceptual model presents a summary of these research findings (see attached image below). A decision engine acts as a central point that facilitates the operations of three core components which consist of Human Behavioral Analytics and AI-Powered Threat Intelligence and Dynamic ZTA Enforcement. The system performs ongoing contextual analysis through which it produces time-sensitive risk scores that lead to automatic permission adjustments and system response changes. The adapted security orchestration model provides solutions for scaling operations as well as fine-grained implementation.

V. DISCUSSION

Modern cyber systems require technology integration with human behavioral analysis and building architecture principles to maintain security according to the findings of this study. The combination of advancing AI technology with ZTA systems deployment proves the human

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr1819

component remains an essential point for potential security weaknesses. The most vulnerable part of the cybersecurity system remain human operators despite AI advancements and the strong structure of ZTA. The paper examines these results while analyzing the combination of AI systems and security frameworks designed around human operators and ZTA in addition to recommending new security approaches for all operational levels.

A. Rethinking the Human Element in Cybersecurity

The main security vulnerability in current-day cybersecurity practice exists because of human errors that stem from carelessness or ignorance or deliberate wrongdoing (Alsowail & Al-Shehari, 2020; Saxena et al., 2020). Present-day traditional cybersecurity training methods that constitute periodic sessions have shown ineffective in stopping advanced security attacks despite employees' best efforts towards training completion. The current training models neglect the quick changes in cyber threats and lack essential features of behavior analysis and individual feedback for increasing security knowledge within specific conditions (Alqahtani & Kavakli-Thorne, 2020; Espinha Gasiba et al., 2020).

Organizations need to transition from single instance awareness programs to perform real-time assessments that consider how users behave. Organizations need to create monitoring systems which analyze employee actions for security compliance including the practice of multi-factor authentication bypass and sensitive data access during suspicious times. Systems employing a detection approach to behavioral anomalies initiate access restrictions and additional authentication requirements that correspond with Zero Trust Architecture principles (Pham et al., 2020). Such evolving practices serve to combat cybersecurity flaws caused by human activities thus reducing the areas where cybercriminals operate.

B. AI and Human Collaboration: Complementary Intelligence

AI contributes substantially to cybersecurity but should function as an automated assistant while humans still maintain their position of oversight because machines lack the ability to completely replace human responsibility. AI tools should function as added human thinking capacity that enhances human-operational capabilities instead of assuming their roles. The processing power of AI systems should not diminish credibility since these systems struggle to interpret threats in complex settings. The absence of ethical decision making skills prevents them from accurately identifying ambiguous activities that pose security risks (Dalal, 2020; Doukas et al, 2020).

The proper understanding of AI systems by humans depends on integrated human decision control through "human-in-the-loop" decision architecture. Such a combination of AI data processing with human expertise enables more effective cybersecurity actions. AI alerts about anomalous activities present threats but cybersecurity professionals need to make the final risk management decisions by evaluating organizational influences alongside contextual information (Truong et al., 2020; Yu et al., 2020).

Human involvement becomes essential to counter the increasing frequency of adversarial attacks made against AI systems. These days cybercriminals take advantage of AI vulnerabilities by making falsified inputs that trick detection systems. Human security experts need to complete multiple steps which consist of validating AI output alongside security interpretation across broader safety parameters to prevent skilled hackers from exploiting system vulnerabilities.

C. Enhancing Zero Trust Adoption with Adaptive Risk Models

Throughout organizational networks Zero Trust Architecture verifies users and devices constantly irrespective of their network position thus proving effective against unauthorized entry according to the studies of Scott et al. (2020) and Chuan et al. (2020). The standard ZTA deployments containing identity verification solutions and device trust verification methods fall short when dealing with complex contemporary cyber danger characteristics. The restricted security model provides inadequate protection since it allows attackers to exploit network internal vulnerabilities through lateral movement.

The combination between ZTA framework and AI-enabled anomaly detection along with behavioral risk evaluation provides substantial strength to the security model. ZTA evaluates continuous risk levels associated with user actions following authentication so it can provide real-time adaptation to human behavior changes. An uncharacteristic access to business-critical records from an unrecognized device or unusual time interval will automatically kick off a risk evaluation process. When anomalies become evident through assessment the system would apply extra verification procedures until it confirms that the issue is resolved. The system implements dynamic risk assessment which makes ZTA operate with adaptive security models that navigate security challenges alongside user productivity across varied contexts (Yao et al., 2020; Hu et al., 2020).

D. Framework Implications for Cybersecurity Strategy

The merger between artificial intelligence and human decisions and Zero Trust Architecture has established a new security system framework that modifies traditional cybersecurity methods. Security models of the past responded with threat mitigation only after threats manifested. The proposed security model adopts a predictive threat awareness system which enables security systems to learn dynamically through both user conduct feedback and ecological development alterations. Such an evolution establishes cybersecurity as a better than mere compliance-driven activity while moving it toward an intelligence-based dynamic framework.

This model mandates organizations to change their security mentality because it brings new abilities to security management. Decision-makers must use advanced

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr1819

technologies to deploy real-time behavioral monitoring together with AI threat detection and continuous access verification and implement changes to security policies for creating this integrated comprehensive system. This defense approach helps organizations achieve better protection but introduces difficulties regarding system integration together with expense and workforce preparation. Organizations must achieve two main goals to solve these problems: they need to invest in training people to use AI systems properly and they need to develop compatibility between current systems and future technologies.

E. Challenges in Implementation

The potential benefits of the integrated security framework encounter multiple substantial barriers during practical implementation. Security implementation faces its biggest hurdle because legacy systems create significant complications during the process of integrating various security technologies. Collective organizations encounter problems with outdated infrastructure management due to high costs and disruptive effects (Kour & Karim, 2020; Kim et al., 2020). The complete adoption of security integration needs professionals who fully understand both information security behavioral aspects and technical expertise because it requires specific cybersecurity education.

The move towards permanent surveillance and analysis of employee conduct will raise significant privacy challenges because organizations need to handle employee information properly. A design philosophy anchored in ethical principles should direct the development of monitoring systems as they need to be clear and avoid invasive procedures and match the accepted data protection standards (Amanowicz, 2020). The challenge ahead involves maintaining optimal security measures that defend privacy rights of individuals.

F. Policy and Standardization Gaps

The evolution of technology surpasses established worldwide cybersecurity standards at the policy level. Zero Trust Architecture has increased its acceptance but regulatory authorities need to implement complete standards which integrate behavior risk evaluation with AI-based security solutions. Most organizations should implement sophisticated cybersecurity protocols but face the challenge of implementing advanced measures because they lack clear direction and motivation. It is essential for regulatory bodies to develop current standards for these tools and methodologies to foster their widespread adoption alongside technological advancements according to NIST (2020) and Scott et al. (2020).

Public sector organizations should encourage regulatory bodies to evaluate the entire cyberspace implications of their cybersecurity efforts. Government institutions must implement contemporary security frameworks based on Zero Trust principles and the combination of human intelligence and AI solutions and Highly Advanced security protocols. Such infrastructure protection sets important expectations that strengthen cybersecurity across the entire private sector.

VI. CONCLUSION

Research examined how AI technology guards organizations in Zero Trust Architecture (ZTA) by emphasizing the importance of human operators for security enhancement. The observed research reveals that AI together with ZTA keeps organizations better protected from cyber dangers yet humans continue being essential weak points in cyber defenses. Highly advanced systems which detect abnormal behavior along with strict control mechanisms continue to operate while human actions because of mistakes or ignorance or deliberate malicious activity serve as primary attack vectors that hackers use to breach systems in modern cyberattacks.

AI serves cybersecurity frameworks to fulfill two essential security tasks by performing anomaly detection and live risk assessment while achieving operational synergy with human personnel. The combination of AI technologies with human supervision creates the most potent security system. The application of AI as a supplementary tool for cybersecurity professionals becomes vital because it maintains essential context-based and ethical human judgment needed for security incident responses.

The combination of Zero Trust Architecture with AI-driven behavioral analytics forms a strong method to reduce security threats which originate from internal or external sources. ZTA ensures the ongoing verification of users and devices even post-access grants to deliver tight control and continuous monitoring of sensitive system and data access. ZTA implements complete effectiveness when it evolves to execute instantaneous user behavior assessment through genuine-time contextualized action-based decisions.

The implementation of ZTA and AI technologies requires organizations to solve integration issues that arise when these systems meet existing ones. Organizations need to address three main issues regarding implementation namely cost and complexity as well as data privacy concerns. Security-related personnel will need proper training together with strict adherence to privacy requirements to unlock the maximum capacity of this integrated security platform.

Public officials need to create modern cybersecurity rules and administrative guidelines which take new emerging technologies into consideration. Standardized approaches to AI-driven security and Zero Trust remain absent which allows organizations to handle complexity independently when they have no official guidance to follow. Systems must be developed by regulatory authorities which will function as ethical standards to protect the safe implementation of AI in cybersecurity while supporting expanded adoption of state-of-the-art security solutions.

The combination of Artificial Intelligence with human decisions together with Zero Trust Architecture creates an effective strategy to protect human-operated AI defense systems. These systems require additional investigation to become better at responding to changing cyber threats

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr1819

through refined development. The cybersecurity development demands organizations to embrace emerging technologies while using them to create security solutions which maintain high usability alongside strong privacy concerns.

The next stage of investigation must include model improvement for security measures that consider human factors while working on combined standards for artificial intelligence and Zero Trust models and understanding the ethical effects of persistent user oversight. Organizations must undergo further development to obtain resilience levels which protect them from mounting sophisticated cyber threats that will emerge in the future.

REFERENCE

[1]. Alqahtani, H., & Kavakli-Thorne, M. (2020). Design and evaluation of an augmented reality game for cybersecurity awareness (CybAR). Information (Switzerland), 11(2). https://doi.org/10.3390/info11020121

[2]. Alsowail, R. A., & Al-Shehari, T. (2020). Empirical detection techniques of insider threat incidents. IEEE Access, 8, 78385–78402. https://doi.org/10.1109/ACCESS.2020.2989739

[3]. Alqahtani, H., & Kavakli-Thorne, M. (2020). Exploring Factors Affecting User's Cybersecurity Behaviour by Using Mobile Augmented Reality App (CybAR). In ACM International Conference Proceeding Series (pp. 129–135). Association for Computing Machinery. https://doi.org/10.1145/3384613.3384629

[4]. Al-Mhiqani, M. N., Ahmad, R., Abidin, Z. Z., Yassin, W., Hassan, A., Abdulkareem, K. H., … Yunos, Z. (2020, August 1). A review of insider threat detection: Classification, machine learning techniques, datasets, open challenges, and recommendations. Applied Sciences (Switzerland). MDPI AG. https://doi.org/10.3390/app10155208

[5]. Amanowicz, M. (2020). Towards building national cybersecurity awareness. International Journal of Electronics and Telecommunications, 66(2), 321–326. https://doi.org/10.24425/ijet.2020.131881

[6]. Chuan, T., Lv, Y., Qi, Z., Xie, L., & Guo, W. (2020). An Implementation Method of Zero-trust Architecture. In Journal of Physics: Conference Series (Vol. 1651). IOP Publishing Ltd. https://doi.org/10.1088/1742-6596/1651/1/012010

[7]. Dalal, A. (2020). AI Powered Threat Hunting in SAP and ERP Environments: Proactive Approaches to Cyber Defense. https://dx.doi.org/10.2139/ssrn.5158251

[8]. Doukas, N., Stavroulakis, P., & Bardis, N. (2020). Review of artificial intelligence cyber threat assessment techniques for increased system survivability. In Malware Analysis Using Artificial Intelligence and Deep Learning (pp. 207–222). Springer International Publishing. https://doi.org/10.1007/978-3-030-62582-5_7

[9]. Espinha Gasiba, T., Lechner, U., & Pinto-Albuquerque, M. (2020). Sifu - a cybersecurity awareness platform with challenge assessment and intelligent coach. Cybersecurity, 3(1). https://doi.org/10.1186/s42400-020-00064-4 Hu, T., Xin, B., Liu, X., Chen, T., Ding, K., & Zhang, X. (2020). Tracking the insider attacker: A blockchain traceability system for insider threats. Sensors (Switzerland), 20(18), 1–18. https://doi.org/10.3390 /s20185297

[10]. Kour, R., & Karim, R. (2020). Cybersecurity workforce in railway: its maturity and awareness. Journal of Quality in Maintenance Engineering, 27(3), 453–464. https://doi.org/10.1108/JQME-07-2020-0059

[11]. Kim, A., Oh, J., Ryu, J., & Lee, K. (2020). A review of insider threat detection approaches with IoT perspective. IEEE Access, 8, 78847–78867. https://doi.org/10.1109/ACCESS.2020.2990195

[12]. Kurniawan, D., & Mumpuni Arti, R. (2020). Comparative Study of a Cybersecurity Curriculum To Support Digital Transformation in The Public Sector. Iapa Proceedings Conference, 547. https://doi.org/10.30589/proceedings.2020.427

[13]. Koroniotis, N., Moustafa, N., Schiliro, F., Gauravaram, P., & Janicke, H. (2020). A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports. IEEE Access, 8, 209802–209834. https://doi.org/10.1109/ACCESS.2020.3036728

[14]. National Institute of Standards and Technology. (2020). Zero Trust Architecture - NIST Special Publication 800-207. NIST, 49. Retrieved from https://doi.org/10.6028/NIST.SP.800-207

[15]. Pham, H. C., Brennan, L., Parker, L., Phan-Le, N. T., Ulhaq, I., Nkhoma, M. Z., & Nhat Nguyen, M. (2020). Enhancing cyber security behavior: an internal social marketing approach. Information and Computer Security, 28(2), 133–159. https://doi.org/10.1108/ICS-01-2019-0023

[16]. Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K. K. R., & Burnap, P. (2020, September 1). Impact and key challenges of insider threats on organizations and critical businesses. Electronics (Switzerland). MDPI AG. https://doi.org/10.3390/electronics9091460

[17]. Soni, V. D. (2020). Challenges and Solution for Artificial Intelligence in Cybersecurity of the USA. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3624487

[18]. Scott et al. (2020). Zero Trust Architecture - NIST Special Publication 800-207. Nist, 49. Retrieved from https://doi.org/10.6028/NIST.SP.800-207

[19]. Truong, T. C., Diep, Q. B., & Zelinka, I. (2020). Artificial intelligence in the cyber domain: Offense and defense. Symmetry, 12(3), 410. https://doi.org/10.3390/sym12030410

[20]. Walker-Roberts, S., Hammoudeh, M., Aldabbas, O., Aydin, M., & Dehghantanha, A. (2020). Threats on the horizon: understanding security threats in the era of cyber-physical systems. Journal of Supercomputing, 76(4), 2643–2664. https://doi.org/10.1007/s11227-019-03028-9

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr1819

[21]. Yu, N., Tuttle, Z., Thurnau, C. J., & Mireku, E. (2020, April). AI-powered GUI attack and its defensive methods. In Proceedings of the 2020 ACM Southeast Conference (pp. 79-86).

[22]. Yao, Q., Wang, Q., Zhang, X., & Fei, J. (2020). Dynamic Access Control and Authorization System based on Zero-trust architecture. In ACM International Conference Proceeding Series (pp. 123–127). Association for Computing Machinery. https://doi.org/10.1145/3437802.3437824

[23]. Zahiroh, M. Y. (2020). Cybersecurity Awareness and Digital Skills on Readiness For Change in Digital Banking. Li Falah: Jurnal Studi Ekonomi Dan Bisnis Islam, 5(2), 53. https://doi.org/10.31332/lifalah.v5i2.2271 https://doi.org/10.1145/3374135.3385270