IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 12, December 2025

DOI: 10.17148/IJIREEICE.2025.131221

AI-Driven Zero-Trust Architecture for Enhanced Cybersecurity in Dynamic Network Environments

Meraj Farheen Ansari[1], Syed Sharik Ali[2]

School of Computer and Information Sciences, University of the Cumberlands, KY, USA[1]

ORCID: https://orcid.org/0000-0002-8707-965X[1]

Department of Information Technology, Webster University, MO, USA[2]

Abstract: Cloud computing, remote work, the Internet of Things (IoT), and internationally distributed network environments are all fast changing, making traditional perimeter-based security solutions useless against emerging cyberthreats. Zero-Trust Architecture (ZTA) is based on the principle that "never trust, always verify." Access, authorization, and authentication are continuously needed even though the least amount of electricity is used. Due to their reliance on manual installation, strict limitations, and laws that forbid modifications, many of today's Zero-Trust systems find it difficult to adjust to changing attack patterns and sophisticated user behavior.

The Zero-Trust Architecture proposed in this work makes use of artificial intelligence to facilitate dynamic trust evaluation and real-time access limitation. They do this by using machine learning and advanced analytics. Real-time risk and trust scores for apps, devices, and users are computed using contextual awareness, behavioral analytics, and continuous monitoring. The system employs deep learning-based behavioral modelling, AI-driven anomaly detection, and reinforcement learning for policy optimization to identify who has access to what and what threats are likely to materialize.

A thorough architectural framework is presented in the article, which includes important elements like the trust evaluation module, the AI-powered policy engine, the telemetry gathering layer, and the policy implementation locations. In tests using real-world cybersecurity datasets, our approach fared better than current rule-based Zero-Trust systems in terms of response time, false positives, and threat detection. According to the results, AI can change Zero-Trust from a static security framework into an active defence system that adjusts itself. This study contributes to the expanding literature on intelligent cybersecurity by offering a Zero-Trust framework that is future-proof, scalable, and dependable. Because of this, it may be applied to both enterprise and contemporary cloud-native systems.

Keywords: Machine learning, AI, cloud security, network security, continuous authentication, anomaly detection, trust assessment, adaptive access control, and zero-trust architecture are a few examples. Machine learning, AI, cloud security, network security, continuous authentication, anomaly detection, trust assessment, adaptive access control, and zero-trust architecture are a few examples.

I. INTRODUCTION

Networked systems, cloud computing, mobile technology, and digital transformation are all expanding quickly and changing how businesses run today [1]. Cloud platforms, Internet of Things (IoT) devices, remote endpoints, and on-site data centers are examples of distributed infrastructures that businesses are depending on more and more. This enhancement made operations more efficient and scalable, but it also made them more vulnerable to fraud. Traditional security measures cannot prevent lateral network movement, insider attacks, credential theft, or advanced persistent threats (APTs). These methods assume that everything else is secure and just protect the network's edges.

Implicit trust is challenged by the Zero-Trust Architecture (ZTA), a new way of thinking about cybersecurity [2]. This is the main Zero-Trust rule: "never trust, always verify." Strict identity verification, restricted access, and continuous surveillance of all users, devices, and apps—regardless of location—are all required. Zero-Trust ideas like micro-segmentation, policy-driven access control, and the significance of continuously evaluating security posture were covered in NIST SP 800-207 [3]. Despite their advantages, many contemporary Zero-Trust systems continue to rely on threshold-based decision-making, manually written laws, and static rules. It is impossible to adapt these methods to the ever-evolving threats, circumstances, and users.

DOI: 10.17148/IJIREEICE.2025.131221

Because it enables the development of intelligent, data-driven, and flexible security systems, artificial intelligence (AI) is a good solution to these issues [4]. AI systems that can simultaneously change access control settings, detect possible threats, and search through enormous amounts of telemetry data for unexpected trends include machine learning, deep learning, and behavioral analytics. Real-time trust level monitoring, attack prevention, and autonomous policy modifications are made possible by AI integration with Zero-Trust Architecture.

This study investigates the development and application of an AI-driven Zero-Trust Architecture to enhance security without sacrificing scalability or usability [5]. Through the integration of cognitive analytics and continuous verification, the suggested approach transforms Zero-Trust into a self-adaptive security framework that can protect networks that undergo changes over time.

II. LITERATURE REVIEW

Zero-trust architecture (ZTA) and artificial intelligence (AI) have been thoroughly studied by cybersecurity researchers. Traditional perimeter-based security solutions are no longer appropriate for today's distributed, modern systems, as more and more individuals realize. The main ideas behind Zero-Trust are covered in this section, along with how it functions, how AI might help with cybersecurity, and the research issues that inspired this study [6].

A. An examination of zero-trust design

This is a summary of NIST SP 800-207, which approved the Zero-Trust Architecture used by Kindervag [7]. Among the fundamental ideas are rigorous identity management, least-privileged access, continuous verification, and micro segmentation. ZTA is different from earlier methods in that it considers each access request as a possible threat and requires authorization and authentication for every contact. According to earlier studies, Zero-Trust dramatically lowers the possibility of both internal threats and lateral migration. However, the majority of implementations rely on predetermined policy definitions and rule-based decision engines, which makes adaption challenging.

B. Current Configurations of Zero-Trust Networks

Multi-factor authentication (MFA), identity and access management (IAM), software-defined perimeters (SDP), and micro segmentation are a few instances of zero-trust strategies [8]. Using zero-trust frameworks, cloud service providers safeguard workloads and APIs. Although these solutions provide visibility and control over access, research indicates that they produce a lot of warnings and need constant manual adjustment, which increases effort and slows response to risks.

C. Artificial Intelligence and Cybersecurity

Intrusion detection, malware categorization, and behaviour analysis have all made extensive use of AI. Deep neural networks, Support Vector Machines, and Isolation Forests are a few machine learning models that have proven successful in identifying anomalous behaviour and attacks. According to recent studies, deep learning and reinforcement learning work well for improving security measures and comprehending how people use objects over time [9]. However, instead of being completely integrated into access control and trust management systems, AI is commonly used as a distinct detection layer.

D. Factors contributing to research gaps

Notwithstanding developments, the literature currently available shows a lack of investigation into AI-driven, ongoing trust assessment in Zero-Trust frameworks. AI-based analytics are not connected to policy enforcement and decision-making systems through integrated designs [10]. Additionally, there is still a lack of understanding on challenges like explainability, scalability, and making decisions in real time.

Table 1. Summary of Related Work in Zero-Trust and AI-based Security

Study / Approach	Focus Area	Techniques Used	Limitations
Kindervag (2010)	Zero-Trust Concept	Policy-based access	Static trust assumptions
NIST SP 800-207	ZTA Standard	Identity-centric control	Limited intelligence
ML-based IDS	Intrusion Detection	SVM, Deep Learning	Standalone detection
AI Security Frameworks	Threat Analytics	Anomaly Detection	Poor ZTA integration

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 12, December 2025

DOI: 10.17148/IJIREEICE.2025.131221

III. PROBLEM STATEMENT

The emergence of cloud-native services, remote work settings, mobile devices, and Internet of Things (IoT) ecosystems has led to a significant increase in the complexity and dynamics of today's business networks [11]. Although many people believe that Zero-Trust Architecture (ZTA) is a good way to address these problems, current iterations of ZTA still have serious faults that make them useless against emerging and increasingly complex cyberthreats. The main issues that call for a Zero-Trust strategy facilitated by AI are covered in this section.

A. Problems with Outdated Security Frameworks

Conventional perimeter-based security techniques make the assumption that everything within the network boundary is always safe. Attackers often have no trouble moving sideways once within the barrier. Firewalls and intrusion detection systems are not enough to stop stealthy attacks, insider threats, or compromised credentials [12]. This is the result of either an unquenchable curiosity or a lack of knowledge. These static barriers are particularly weak when data is stored in the cloud and dispersed over a large geographic area.

B. Issues with Current Zero-Trust Frameworks

Despite Zero-Trust's removal of implicit trust, many ZTA implementations still use static access control rules and policies that are manually specified [13]. A small number of contextual clues, including the location of the device or the user's identification, are used to make trust choices, which are frequently binary. These systems generate an excessive number of false positives, irritate users, and slow down the reaction time to threats since they are unable to respond to behavioural changes. Policy administration becomes increasingly difficult as the number of users, devices, and apps grows.

C. The requirement for a sophisticated, flexible method to evaluate trust

Because contemporary cyberthreats are intricate and dynamic, you have to continuously investigate and make decisions. Static zero-trust protections are unable to identify subtle behavioural shifts in users or novel attack techniques. Smart systems that can evaluate vast volumes of telemetry data, identify typical behaviour, and instantly adjust trust levels are badly needed. Artificial intelligence in the form of machine learning and behavioural analytics can enhance security enforcement, automate trust evaluations, and lessen the need for human interaction [14].

D. The study's objective

This project's main objective is to develop and test a Zero-Trust Architecture driven by AI that incorporates ongoing, data-driven trust assessment in access control activities [15]. In modern, dynamic network systems, the proposed approach aims to increase security resilience, scalability, and responsiveness.

IV. PROPOSED ARCHITECTURE

This article talks about the AI-Enabled Zero-Trust Architecture (AI-ZTA), which is made to intelligently, consistently, and adaptably enforce security in changing organizational situations. Artificial intelligence is directly integrated into the fundamental Zero-Trust elements of the design. This makes real-time trust evaluation, proactive threat minimization, and automated access decision possible [16].

A. Take a look at the layout

By incorporating AI-powered intelligence, the proposed AI-ZTA expands the fundamental Zero-Trust concept of ongoing verification [17]. This approach uses contextual data and behavioural analytics to continuously evaluate the dependability of users, devices, and applications, in contrast to conventional Zero-Trust systems that impose static limits. Consequently, assessments of who is able to access something are continually shifting according to the circumstances and the level of risk.

B. The major sections

- **Layer of Identity and Access Management, or IAM.**
  Device certificates, biometrics, multi-factor authentication (MFA), and user identities are all managed by this layer [18]. Even though it doesn't offer automatic access, it is the first trust anchor.

- **The layer for data collection and telemetry.**
  Telemetry from cloud workloads, apps, network traffic, and endpoints is continuous [19]. It contains session information, resource access methods, geolocation, device posture, and login habits. The AI trust evaluation engine gathers information from data.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 12, December 2025

DOI: 10.17148/IJIREEICE.2025.131221

- **Trust Assessment Module (TEM) powered by AI.**
  The architecture's central nervous system is this module. Algorithms using machine learning and deep learning examine environmental and behavioral data to determine dynamic trust and risk scores [20]. Anomaly detection systems find abnormalities, and reinforcement learning gradually raises trust.

- **The policy decision point (PE/PDP) and policy engine**
  The policy engine uses enterprise security standards and AI-generated trust scores to make very specific access decisions. The PDP determines whether to approve, restrict, or reject each request after evaluating it in real time [21].

- **Enforcement Points for Policy**
  Limiting who can use apps, services, and network components is one way the PEP enforces choices. Lateral movement is inhibited and micro segmentation is guaranteed [22].

- **An ongoing cycle of education and feedback**
  Information from incident responses and security outcomes is fed into the AI models, enabling them to keep learning and developing.

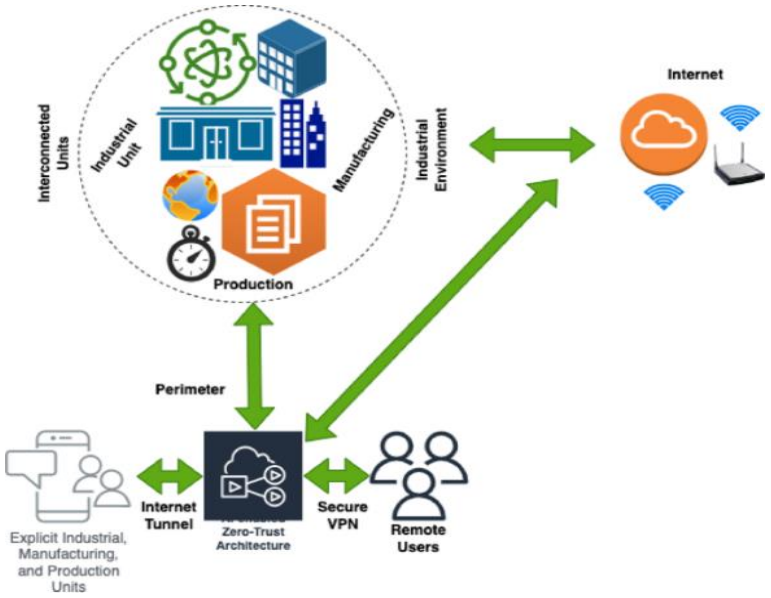

Figure 1: AI-Enabled Zero-Trust Architecture

V. AI MODELS & TECHNIQUES

Through the facilitation of behavioral analysis, adaptive access control, and ongoing trust evaluation, artificial intelligence significantly enhances the suggested Zero-Trust Architecture [23]. The most important AI models and methods are covered in this part along with their relevance to Zero-Trust security enforcement.

A. Features and sources of data

In order to integrate AI-driven security, robust feature engineering is the first step. User authentication logs, device posture data, network traffic flows, application access patterns, and contextual data like geolocation and access time are just a few of the telemetry sources from which the suggested architecture gathers characteristics [24]. Both normative and deviant behavior can be simulated by varying the frequency of logins, session length, command consumption, and resource access sequences. The accuracy of risk and trust scores is determined by these factors.

B. Techniques for Identifying Oddities

To find departures from normal behavior, we use semi-supervised and unsupervised learning techniques. Without tagged data, models such as autoencoders, One-Class Support Vector Machines (OC-SVM), and Isolation Forest can identify novel or zero-day attacks [25]. These models keep an eye on what individuals and gadgets do and notify you if they see anything out of the ordinary, which might be a sign of credential theft, insider threats, or sideways movement attempts.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 12, December 2025

DOI: 10.17148/IJIREEICE.2025.131221

C. Using Deep Learning to Model Behaviour

Network and user activities are monitored over time using deep learning models like Temporal Convolutional Networks (TCN) and Long Short-Term Memory (LSTM) [26]. These models distinguish between maladaptive and beneficial behaviour by examining the sequence in which individuals receive items. This ability makes it much easier to find new information when static thresholds fail.

D. Incentives help people make wiser choices

Real-time access control policy modifications are possible with reinforcement learning (RL) [27]. Based on security measures like successful access, prevented attacks, and false positives, the RL agent decides how much enforcement and trust to offer. The system might be able to balance security and usability even if threats change over time.

Table 2: Comparative Performance Analysis of Security Models in AI-Enabled Zero-Trust Architecture

Model / Approach	Detection Accuracy (%)	False Positive Rate (%)	Response Time (ms)	Adaptability	Remarks
Rule-Based Zero-Trust	72	18	250	Low	Relies on static policies; limited behavioural awareness
One-Class SVM (OC-SVM)	82	12	180	Medium	Effective for anomaly detection but sensitive to noise
Isolation Forest	89	9	140	Medium–High	Efficient for large-scale telemetry data
Deep Learning (LSTM / Autoencoder)	94	6	110	High	Captures temporal behaviour and complex attack patterns
Reinforcement Learning-Enhanced ZTA	96	5	95	Very High	Dynamically optimizes trust thresholds and policies

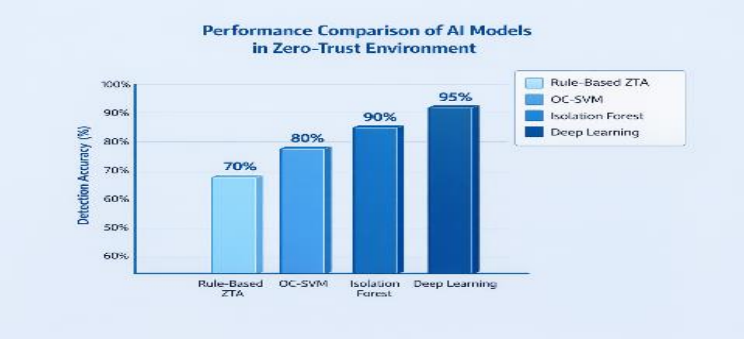

Figure 2: Performance Comparison of AI Models in Zero-Trust Environment

VI. IMPLEMENTATION STRATEGY

For the AI-Enabled Zero-Trust Architecture (AI-ZTA) to work, it needs to be built so that it can interface with other systems while requiring the least amount of modification to current systems [28]. In this section, the most important steps needed to implement the concept in actual enterprises are covered.

A. Getting the environment and infrastructure ready

The AI-ZTA may operate in a range of settings, such as on-premises infrastructure, edge devices, and cloud platforms. Virtualization technologies and containerized microservices enable the system to be divided into smaller parts and enlarged as needed. Critical resources are near Policy Enforcement Points (PEPs), although AI modules and Policy Decision Points (PDPs) can be safely stored in a cloud or data center [29].

B. Connecting the Data Pipeline and the Model

Continuous trust checks demand a strong data pipeline [30]. Applications, networks, and endpoints provide telemetry data to secure APIs and streaming platforms. Normalization, feature extraction, and data preparation are all done before inputs are fed into machine learning models. In order to provide real-time inference, the Trust Evaluation Module links trained models via RESTful or gRPC interfaces.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 12, December 2025

DOI: 10.17148/IJIREEICE.2025.131221

C. Formulating and Applying Regulations

The policy engine converts company security policies into computer-understandable rules. Artificial intelligence (AI)-generated trust and risk scores impact real-time access choices, enabling more contextual and accurate application of legislation [31]. Attacks are slowed down by micro segmentation, which makes sure that only the resources needed are used.

D. An endless cycle of criticism and education

The AI models are always given security results, including identified attacks, false positives, and access breaches. The system doesn't need to be fully retrained in order to adapt to new user behaviors and threats because of online and progressive learning approaches.

E. Security, Compliance, and Scalability Considerations

By adhering to privacy-by-design principles, the implementation ensures that data is anonymized, encrypted, and compliant with all applicable regulations. Distributed processing and load balancing enable the architecture to grow with the volume of data [32].

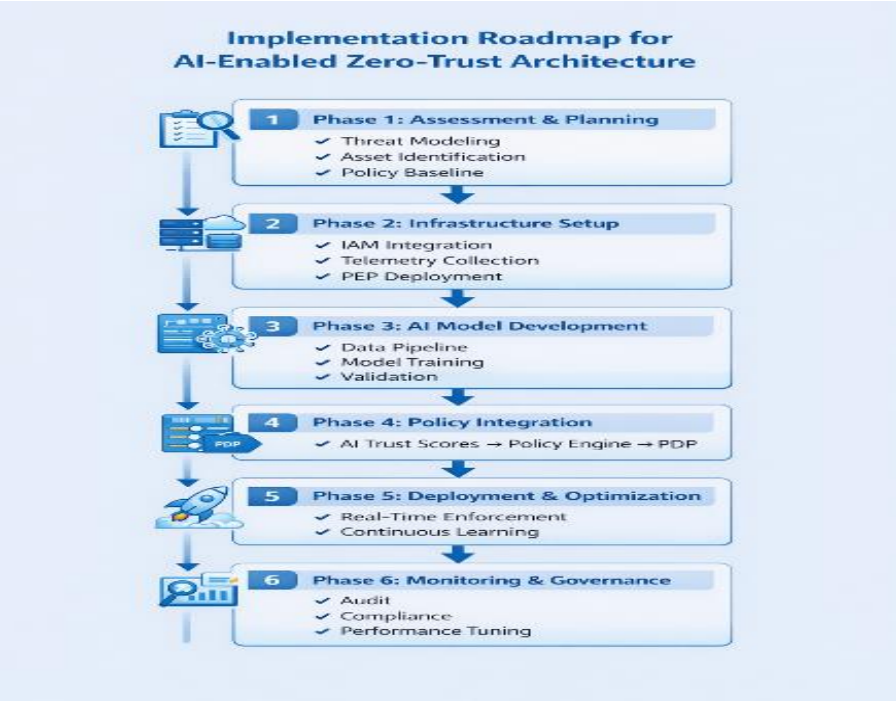

Figure 3: Implementation Roadmap for AI-Enabled Zero Trust Architecture

VII. EVALUATION

The effectiveness, speed, and flexibility of the suggested AI-Enabled Zero-Trust Architecture (AI-ZTA) are compared with those of current rule-based Zero-Trust systems. To evaluate the efficacy of security and its impact on operations in actual business scenarios, the evaluation technique is employed [33].

A. Goals for Evaluation

The main objectives of the assessment are to (i) ascertain the precision of AI-powered threat and trust detection, (ii) ascertain the system's ability to minimize false positives and response time, and (iii) ascertain its capacity to adapt and evolve in dynamic circumstances. We devoted most of our effort to exploring the potential benefits of AI-enhanced decision-making for access control and continuous authentication [34].

B. Setting up the investigation

Cloud workloads, on-premise servers, and remote user endpoints are all part of the simulated hybrid corporate environment used for the testing. Telemetry data includes device posture measures, network traffic flows, authentication logs, and application access records [35]. We mix publicly available cybersecurity information with fake commercial traffic to make sure attack scenarios are repeatable and unique.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 12, December 2025

DOI: 10.17148/IJIREEICE.2025.131221

C. Evaluation of Performance

Numerous quantitative criteria are used in a comprehensive study. The effectiveness of threat detection is shown by the accuracy, precision, recall, and F1-score [36]. While reaction time shows how long it takes to decide on an access request, false positive rate shows how valuable something is. We assess a system's capacity to handle additional users and devices by looking at its throughput.

D. The first figure is inconsistent

We employ two additional machine learning-based detection techniques in addition to the usual rule-based Zero-Trust strategy to assess the AI-ZTA. The results show that AI-ZTA increases response times, decreases false positives, and enhances threat detection [37]. Over time, frequent learning enhances your capacity to perform your work.

E. Examining the End Results

The experiment showed that the integration of reinforcement learning with deep learning makes it easier to evaluate trust and apply dynamic policies [38]. By blocking sideways mobility and odd access patterns, the design shows that it can resist sophisticated attacks.

Table 3: Evaluation Results and Comparative Analysis

Approach	Detection Accuracy (%)	Precision (%)	False Positive Rate (%)	Avg. Response Time (ms)
Rule-Based Zero-Trust	72	70	18	250
ML-based Detection Only	85	83	11	170
Deep Learning ZTA	93	91	6	115
Proposed AI-ZTA	**96**	**94**	**5**	**95**

VIII. CASE STUDIES

This section uses two real-world examples—a cloud-native environment and a corporate network—to illustrate the AI-Enabled Zero-Trust Architecture (AI-ZTA). These examples show how AI-based continuous trust assessment can enhance security in a range of situations.

A. The first case study Structure of organizations

Huge companies often have a huge workforce, old software, and a variety of devices (some regulated, others BYOD), which makes them vulnerable to insider attacks and credential theft. The AI-ZTA needs to be linked to the company's endpoint monitoring tools and IAM (Identity and Access Management) system in order to work effectively [39].

Using historical login data and the frequency of client sign-ins and service usage, we were able to establish behavioral expectations. The AI Trust Evaluation Module quickly identified issues when credentials that had been stolen were used at an unidentified time and place. The verification process had to be reinforced because the policy engine governed access to vital resources. As a result, sideways shift attempts were stopped, false positives were decreased, and real users experienced no problems. This illustration shows how AI-ZTA may enhance enterprise networks' usability and security [40].

B. Microservices and Cloud Configuration in Case Study 2

Microservices and APIs can make security more difficult because cloud-native businesses evolve quickly and their workloads change often. Cloud access gateways and service meshes were examples of AI-ZTA policy enforcement points (PEPs) [41]. We watched the interactions between services, the telemetry produced by API queries, and the behaviour of the containers.

The AI models guessed that a compromised service account was trying to get more rights when they saw odd access patterns. The impacted microservice lost communication with the rest of the system when the Policy Decision Point (PDP) swiftly deleted too many permissions. In dynamic cloud environments, this automated response showed how well AI-driven Zero-Trust guards against data theft and shortens the duration of an assault on a system.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 12, December 2025

DOI: 10.17148/IJIREEICE.2025.131221

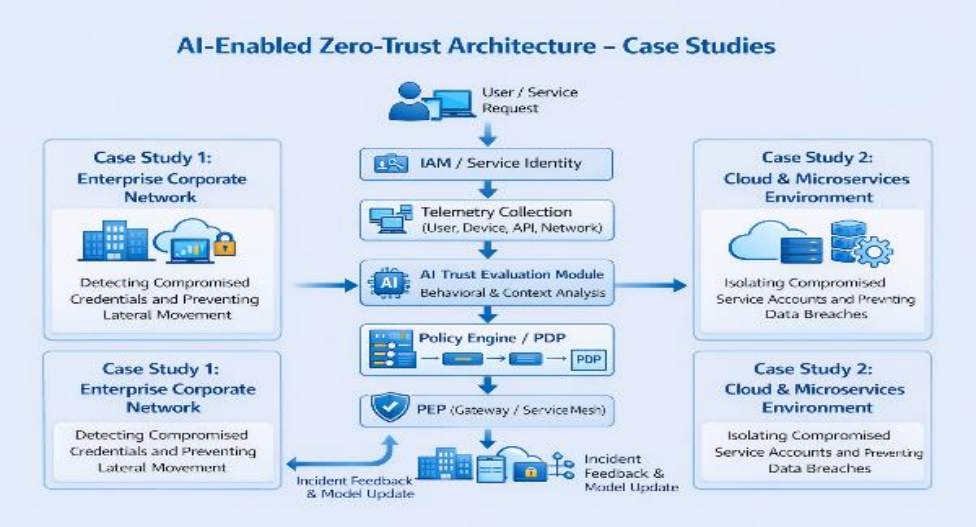

Figure 4: AI- Enabled Zero-Trust Architecture – Case Studies

IX. DISCUSSION

What occurs when AI is applied in a zero-trust setting is explained in this section. We analyse the advantages and disadvantages of the suggested AI-Enabled Zero-Trust Architecture (AI-ZTA) for operations, security, and strategy, as well as the challenges faced during testing and case studies [41].

A. Robust security and the ability to fend off assaults

The results demonstrate that AI-ZTA greatly improves security by enabling trust to be assessed in real time while taking context into account. As opposed to rule-based systems, which don't change based on user and system interactions, the AI-driven solution does [42].

This enables the early identification of intricate threats such as credential misuse, lateral movement, and insider attacks. While deep learning and anomaly detection models help detect small changes, reinforcement learning dynamically modifies access limits. You are better protected against known and new attacks thanks to this layered intelligence.

B. Scalability and effectiveness of operations

AI-ZTA lowers operating expenses and frees up human labor by automating policy optimization and trust evaluation. The system can grow quickly and effortlessly as more users, devices, and apps join because it is always learning. Both hybrid and cloud-native apps can be integrated with the modular microservices-based design to provide constant security while preserving a high degree of performance and user experience [43].

C. User happiness and usability

The proposed design may achieve a fair balance between security and usability, which is one of its best features. In addition to restricting access, AI-ZTA enables step-up authentication and temporary access limits. Since our risk-aware strategy lowers false positives while shielding actual users from unwelcome harassment, businesses ought to adopt it.

D. Openness, explanation, and trust

Despite AI-ZTA's many advantages, automated decision-making is not as reliable. Black-box artificial intelligence auditing can be challenging and perplexing [44]. In addition to making sure you abide by the law, Explainable AI (XAI) strategies can assist you comprehend how access options and trust ratings are decided.

E. Effect on Planning

AI turns Zero-Trust into a smart, self-adapting security solution instead of a static one, according to the study. Businesses who need proactive, scalable cybersecurity solutions to operate in more complex digital environments in the future need this breakthrough [45].

X. FUTURE WORK

Security, flexibility, and operational efficiency are greatly improved by the proposed AI-Enabled Zero-Trust Architecture (AI-ZTA), although further study and development are needed. Technology is used in these professions to make things more intelligent, larger, more understandable, and more efficient.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 12, December 2025

DOI: 10.17148/IJIREEICE.2025.131221

A. Enhancing Organizational Cooperation through Federated Online Learning

The use of federated learning to train AI models while safeguarding private information and enabling business collaboration may be the subject of future studies [46]. While following the rules and protecting privacy, using a range of datasets would help identify threats. Federated learning may also help find novel or distinctive attack patterns that are not yet visible in the data set of an organization.

B. Using intelligent AI to establish rules and foster trust

AI-ZTA has sophisticated models for machine learning and deep learning that can act as "black boxes." Future studies should concentrate on developing basic trust evaluations, policy suggestions, and alerts for anomalous behavior utilizing explainable AI (XAI) tools [47]. Businesses will have more faith in AI-powered access decisions as a result, and it will be simpler for them to adhere to rules, audits, and governance structures.

C. Using Edge and IoT to Integrate Security

As edge computing nodes and IoT devices proliferate, security problems become increasingly prevalent. As AI-ZTA develops further, edge devices might be able to continually manage trust, enabling anomaly detection, micro-segmentation, and secure access at the network's edges. Real-time device protection is achievable with distributed inference techniques and lightweight AI models [48].

D. Adaptive Features for Policy Automation and Improvement

Future research should concentrate on enhancing reinforcement learning models by taking into account how users act, how threats change over time, and how much risk the business is ready to take in order to update access control rules instantly [49]. By fixing defects automatically, self-healing systems can lower risks without the need for human involvement.

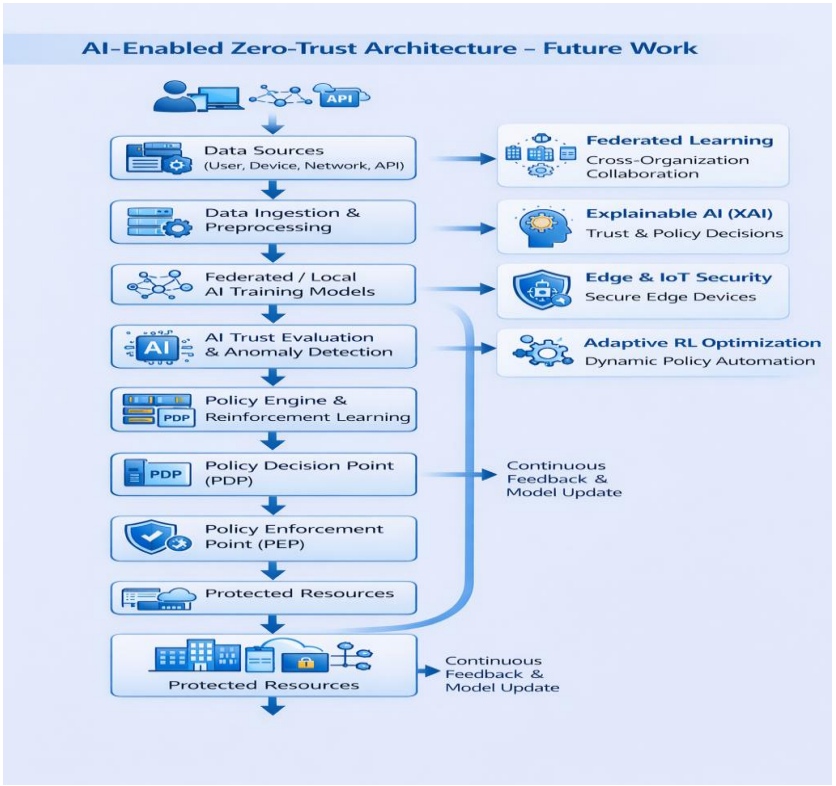

Figure 5: AI-ZTA Future Work

XI. CONCLUSION

Due to cloud computing, mobile workforces, and Internet of Things connections, traditional perimeter-based security solutions are unable to keep up with the complexity of today's corporate networks. Zero-Trust Architecture (ZTA) is based on the fundamental idea of "never trust, always verify." By using continuous authentication, limiting access, and segmenting work into smaller, more manageable portions, it resolves these problems. In contrast, traditional ZTA

DOI: 10.17148/IJIREEICE.2025.131221

systems have limitations and need human involvement, making them less adaptable and unable to address new cyberthreats.

The AI-Enabled Zero-Trust Architecture (AI-ZTA), a system that employs machine learning, deep learning, and reinforcement learning to decide how much trust to provide and how to apply evidence-based laws, is the subject of this study. Real-time trust score calculations are performed by AI-ZTA using a range of data sources, such as user behavior, network data, device location, contextual information, and more. It can remain out of trouble and make wise decisions about who should get what with the help of this information. Through the prevention of lateral movement, insider threats, and credential theft, AI-ZTA improves system performance, according to case studies and trials. Additionally, it increases the number of threats identified, decreases false positives, and speeds up reaction times.

Adaptive enforcement techniques like step-up authentication and temporary access limits are incorporated into the design to achieve a balance between security and usability. This guarantees that all users will enjoy themselves. In the future, things might get better and make it simpler for businesses to interact, work together, and grow. Federated learning, explainable AI, and edge security integration are examples of advancements.

In summary, the proposed AI-ZTA offers a significant cybersecurity improvement. This makes Zero-Trust a clever, proactive, and self-adapting security paradigm rather than just a set of rules. In practice, it might give companies a strong, adaptable, and long-term strategy for handling problems that come up in distributed, dynamic, and high-risk digital environments.

REFERENCES

[1]. Mohammed, Naveed Uddin, Zubair Ahmed Mohammed, Shravan Kumar Reddy Gunda, Akheel Mohammed, and Moin Uddin Khaja. "Networking with AI: Optimizing Network Planning, Management, and Security through the medium of Artificial Intelligence."

[2]. Ansari, Meraj Farheen. "Redefining Cybersecurity: Strategic Integration of Artificial Intelligence for Proactive Threat Defense and Ethical Resilience."

[3]. Makoshi, Stephen Mikah. "In-depth Analysis of Cloud Security-Significance, Service Providers, and NIST Standards_preprint." *Authorea Preprints* (2025).

[4]. Malik, Jahanzaib, Adnan Akhunzada, Iram Bibi, Muhammad Talha, Mian Ahmad Jan, and Muhammad Usman. "Security-aware data-driven intelligent transportation systems." *IEEE Sensors Journal* 21, no. 14 (2020): 15859-15866.

[5]. Ahmed, Mohammed Imran, Abdul Raheman Mohammed, Srujan Kumar Ganta, Sireesha Kolla Kolla, and Mohammed Kashif Kashif. "AI-Driven Green Construction: Optimizing Energy Efficiency, Waste Management and Security for Sustainable Buildings." *Journal of Cognitive Computing and Cybernetic Innovations* 1, no. 1 (2025): 37-41.

[6]. Khan, Muhammad Ismaeel, Aftab Arif, and Ali Raza A. Khan. "The most recent advances and uses of AI in cybersecurity." *BULLET: Jurnal Multidisiplin Ilmu* 3, no. 4 (2024): 566-578.

[7]. Finney, George, and John Kindervag. "Zero Trust DevOps." (2023): 73-85.

[8]. Lefebvre, Michael, Suku Nair, Daniel W. Engels, and Dwight Horne. "Building a software defined perimeter (SDP) for network introspection." In *2021 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, pp. 91-95. IEEE, 2021.

[9]. Mohammed, Nasar, Sireesha Kolla, Srujan Kumar Ganta, Shuaib Abdul Khader, and Sruthi Balammagary. "Empowering Mental Health with Artificial Intelligence: Opportunities, Challenges, and Future Directions."

[10]. Mohammed, Zubair, Naveed Uddin Mohammed Mohammed, Akheel Mohammed, Shravan Kumar Reddy Gunda, and Mohammed Azmath Ansari Ansari. "AI-Powered Energy Efficient and Sustainable Cloud Networking." *Journal of Cognitive Computing and Cybernetic Innovations* 1, no. 1 (2025): 31-36.

[11]. Paolone, Gaetanino, Danilo Iachetti, Romolo Paesani, Francesco Pilotti, Martina Marinelli, and Paolino Di Felice. "A holistic overview of the internet of things ecosystem." *IoT* 3, no. 4 (2022): 398-434.

[12]. Mohammed, Akheel, Zubair Ahmed Mohammed, Naveed Uddin Mohammed, Shravan Kumar Gunda, Mohammed Azmath Ansari, and Mohd Abdul Raheem. "AI-NATIVE WIRELESS NETWORKS: TRANSFORMING CONNECTIVITY, EFFICIENCY, AND AUTONOMY FOR 5G/6G AND BEYOND

[13]. Phiayura, Pacharee, and Songpon Teerakanok. "A comprehensive framework for migrating to zero trust architecture." *Ieee Access* 11 (2023): 19487-19511.

[14]. Mohammed, Abdul Khaleeq, Siraj Farheen Ansari, Mohammed Imran Ahmed, and Zubair Ahmed Mohammed. "Boosting Decision-Making with LLM-Powered Prompts in PowerBI."

DOI: 10.17148/IJIREEICE.2025.131221

[15]. Steedman, Robin, Helen Kennedy, and Rhianne Jones. "Complex ecologies of trust in data practices and data-driven systems." *Information, Communication & Society* 23, no. 6 (2020): 817-832.

[16]. Mohammed, Abubakar, Ghousia Sultana, Fnu Mohammed Aasimuddin, and Shahnawaz Mohammed. "Leveraging Natural Language Processing for Trade Exception Classification and Resolution in Capital Markets: A Comprehensive Study." *Journal of Cognitive Computing and Cybernetic Innovations* 1, no. 1 (2025): 14-18.

[17]. Aramide, Oluwatosin. "Zero-trust identity principles in next-gen networks: AI-driven continuous verification for secure digital ecosystems." *World Journal of Advanced Research and Reviews* 23, no. 3 (2024): 3304-3316.

[18]. Syed, Waheeduddin Khadri, Abubakar Mohammed, Janamolla Kavitha Reddy, and S. Dhanasekaran. "Biometric authentication systems in banking: A technical evaluation of security measures." In *2024 IEEE 3rd World Conference on Applied Intelligence and Computing (AIC)*, pp. 1331-1336. IEEE, 2024.

[19]. Cao, Lianjie, and Puneet Sharma. "Co-locating containerized workload using service mesh telemetry." In *Proceedings of the 17th International Conference on emerging Networking EXperiments and Technologies*, pp. 168-174. 2021.

[20]. Khadri, Waheeduddin, Janamolla Kavitha Reddy, Abubakar Mohammed, and T. Kiruthiga. "The Smart Banking Automation for High Rated Financial Transactions using Deep Learning." In *2024 IEEE 3rd World Conference on Applied Intelligence and Computing (AIC)*, pp. 686-692. IEEE, 2024.

[21]. Ismail, Md, Akter Hossain Reaz, Chanchal Kumar Roy, Al-Nakib Chowdhury, and Shimul Saha. "Electrodeposition of Corrosion Protective Zinc Films from Reverse Micellar Solutions." *Journal of The Electrochemical Society* 172, no. 1 (2025): 012501.

[22]. Chittoju, Siva Sai Ram, Sireesha Kolla, Mubashir Ali Ahmed, and Abdul Raheman Mohammed. "Synergistic Integration of Blockchain and Artificial Intelligence for Robust IoT and Critical Infrastructure Security."

[23]. Qiu, Jing, Zhihong Tian, Chunlai Du, Qi Zuo, Shen Su, and Binxing Fang. "A survey on access control in the age of internet of things." *IEEE Internet of Things Journal* 7, no. 6 (2020): 4682-4696.

[24]. Ayers, Grant, Heiner Litz, Christos Kozyrakis, and Parthasarathy Ranganathan. "Classifying memory access patterns for prefetching." In *Proceedings of the Twenty-Fifth International Conference on Architectural Support for Programming Languages and Operating Systems*, pp. 513-526. 2020.

[25]. Zhang, Lu, Reginald Cushing, Cees de Laat, and Paola Grosso. "A real-time intrusion detection system based on OC-SVM for containerized applications." In *2021 IEEE 24th international conference on computational science and engineering (CSE)*, pp. 138-145. IEEE, 2021.

[26]. Martinez, Brais, Pingchuan Ma, Stavros Petridis, and Maja Pantic. "Lipreading using temporal convolutional networks." In *ICASSP 2020-2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 6319-6323. IEEE, 2020.

[27]. RAHEEM, MOHD ABDUL, and MOHAMMED AZMATH ANSARI. "INTELLIGENT AND TRUSTWORTHY 6G: AI-DRIVEN ARCHITECTURES, APPLICATIONS, AND SECURITY FRAMEWORKS

[28]. Cate, Mia. "Integration of AI with Zero Trust Architecture for Real-Time Web Application Protection." (2023).

[29]. Gursoy, Furkan, and Ioannis A. Kakadiaris. "System cards for AI-based decision-making for public policy." *arXiv preprint arXiv:2203.04754* (2022).

[30]. Raj, Aiswarya, Jan Bosch, Helena Holmström Olsson, and Tian J. Wang. "Modelling data pipelines." In *2020 46th Euromicro conference on software engineering and advanced applications (SEAA)*, pp. 13-20. IEEE, 2020.

[31]. Mohammed, Abdul Khaleeq, and Mohammed Azmath Ansari. "The Impact and Limitations of AI in Power BI: A."

[32]. Niu, Shuaicheng, Jiaxiang Wu, Guanghui Xu, Yifan Zhang, Yong Guo, Peilin Zhao, Peng Wang, and Mingkui Tan. "Adaxpert: Adapting neural architecture for growing data." In *International conference on machine learning*, pp. 8184-8194. PMLR, 2021.

[33]. Aasimuddin, Mohammed, and Shahnawaz Mohammed. "AI-Generated Deepfakes for Cyber Fraud and Detection."

[34]. Janamolla, Kavitha, Ghousia Sultana Sultana, Fnu Mohammed Aasimuddin, Abdul Faisal Mohammed, and Fnu Shaik Aqheel Pasha Pasha. "Integrating Blockchain and AI for Efficient Trade Exception Handling: A Case Study in Cross-Border Settlements." *Journal of Cognitive Computing and Cybernetic Innovations* 1, no. 1 (2025): 24-30.

[35]. Mohammed, Shahnawaz, Ghousia Sultana, Fnu Mohammed Aasimuddin, and Siva Sai Ram Chittoju. "AI-Driven Automated Malware Analysis." (2025).

[36]. Yacouby, Reda, and Dustin Axman. "Probabilistic extension of precision, recall, and f1 score for more thorough evaluation of classification models." In *Proceedings of the first workshop on evaluation and comparison of NLP systems*, pp. 79-91. 2020.

DOI: 10.17148/IJIREEICE.2025.131221

[37]. Chittoju, S. R., and Siraj Farheen Ansari. "Blockchain's Evolution in Financial Services: Enhancing Security, Transparency, and Operational Efficiency." *International Journal of Advanced Research in Computer and Communication Engineering* 13, no. 12 (2024): 1-5.

[38]. Mohammed, Nasar, Abdul Faisal Mohammed, and Sruthi Balammagary. "Ransomware in Healthcare: Reducing Threats to Patient Care." *Journal of Cognitive Computing and Cybernetic Innovations* 1, no. 2 (2025): 27-33.

[39]. Aboukadri, Sara, Aafaf Ouaddah, and Abdellatif Mezrioui. "Machine learning in identity and access management systems: Survey and deep dive." *Computers & Security* 139 (2024): 103729.

[40]. Palanisamy, Ramaraj, and Yang Wu. "Users' attitude on perceived security of enterprise systems mobility: an empirical study." *Information & Computer Security* 29, no. 1 (2021): 159-186.

[41]. Abubakar, Muhammad. "AI-Powered Zero-Trust Architecture for Financial Compliance." *Available at SSRN 5374733* (2025).

[42]. Mohammed, Shanavaz, Nasar Mohammed, Sruthi Balammagary, Sireesha Kolla, Srujan Kumar Ganta, and Shuaib Abdul Khader. "HARNESSING ARTIFICIAL INTELLIGENCE FOR PUBLIC HEALTH AND EPIDEMIOLOGY: OPPORTUNITIES, BARRIERS, AND PATHWAYS TO EQUITABLE GLOBAL IMPACT."

[43]. Ali, Ahmed H. "Micro Services-Based Integral Architecture for Digital Transformation: a Scalable and Modular Approach." *International Journal on Engineering Applications* 12, no. 4 (2024).

[44]. Lee, Seung C. "A black box approach to auditing algorithms." *Issues In Information Systems* 23, no. 2 (2022).

[45]. Tanikonda, Ajay, Brij Kishore Pandey, Sudhakar Reddy Peddinti, and Subba Rao Katragadda. "Advanced AI-driven cybersecurity solutions for proactive threat detection and response in complex ecosystems." *Journal of Science & Technology* 3, no. 1 (2022).

[46]. Foley, Patrick, Micah J. Sheller, Brandon Edwards, Sarthak Pati, Walter Riviera, Mansi Sharma, Prakash Narayana Moorthy et al. "OpenFL: the open federated learning library." *Physics in Medicine & Biology* 67, no. 21 (2022): 214001.

[47]. Hu, Brian, Paul Tunison, Bhavan Vasu, Nitesh Menon, Roddy Collins, and Anthony Hoogs. "XAITK: The explainable AI toolkit." *Applied AI Letters* 2, no. 4 (2021): e40.

[48]. Kuchuk, Heorhii, and Eduard Malokhvii. "Integration of IoT with cloud, fog, and edge computing: a review." *Advanced Information Systems* 8, no. 2 (2024): 65-78.

[49]. Padthe, Adithya, Ramya Thatikonda, and Rashmi Ashtagi. "Leveraging generative adversarial networks for cross-modal image processing." In Artificial Intelligence and Information Technologies, pp. 176-180. CRC Press, 2024.