IJSES
Volume 10, Issue 7, pp. 25-28, July 2026.
International Journal of Scientific Engineering and Science
ISSN (Online): 2456-7361

Zero-Trust Identity Controls for Banking AI Agents

Amir Ahmed Ansari
Department of Information Technology, Indiana Wesleyan University, IN, USA
Email address: amir.research.lab@gmail.com

***Abstract*— *The rapid integration of AI agents in the field of banking has created another challenge – autonomous identity governance in mission-critical systems. One cannot apply IAM policies that govern permanent machine identities and human identities for transitory and fluid AI identities. The current paper proposes a Zero Trust Identity Governance Framework (ZTIGF) in order to address the problem associated with the governance of AI agents in banking. Distinguishing between human and machine identities, continuous authentication, provision of the least privilege access, monitoring of behavior, and implementation of policies to control the actions of AI agents are among the most important aspects of the proposed approach. In order to eliminate insider attacks, identity theft, privilege escalations, and fraudulent actions performed by AI agents, ZTIGF applies behavioral analysis of AI identities, ephemeral authorization tokens, decentralized digital identities, and multi-factor authentication.*

Keywords*— *Zero Trust Architecture, Identity and Access Management, Artificial Intelligence, Banking Security, Machine Identity, Autonomous Finance.

I. INTRODUCTION

In the banking sector, AI-powered self-sovereign bots have rapidly been adopted for automating essential activities such as fraud detection, risk assessment, lending, customer service, and transaction surveillance. The AI bots are capable of interacting independently with the bank's critical systems, processing large volumes of information, and making decisions within time constraints with little human involvement. Nevertheless, the autonomy of the bots creates grave challenges of identity and access management when both the human bots and artificial intelligence bots use the same logins and passwords. Traditional Identity and Access Management (IAM) technologies fall short in AI-powered scenarios because they are designed for human users and static machine identities [1]. This is because they pose risks such as identity impersonation, privilege misuse, illicit transactions, and lack of accountability. Zero-Trust Security architecture, which operates on the principle of "never trust, always verify," provides a potential solution [2]. Continuous authentication and authorization of all human identities, devices, and machines are ensured under this model. This project will ensure zero-trust identity restrictions for autonomous banking operations that effectively demarcate human and machine identities.

II. LITERATURE REVIEW

Due to the rapid emergence of AI-based banking systems, research in the area of secure identity management for agentic actors has gained attention recently [3]. While conventional IAM frameworks tend to focus on human users and static machine identities, the recent body of research emphasizes the importance of dynamic identity constraints that will apply specifically to AI systems. Focusing on continuous validation and enforcement of policies in agentic workflows, Zero-Trust framework was developed by Cisco Systems [4]. Okta proposed the usage of context-based access control and behavioral analysis for adaptive identity management. Huang et al. have analyzed the problem of managing machine identity lifecycle with respect to the reduction of privileges and temporary credentials. For improving traceability, Xu et al. have considered the use of blockchain-based verification for decentralized identity systems applicable to autonomous systems. Identity overlaps and its consequences in the financial sector between human operator and machine agent were analyzed by Janani et al. These contributions are quite insightful but only little attention is paid to banking AI workflows that require combining machine autonomy, human validation, and compliance with regulations under one Zero-Trust framework [5].

TABLE 1: Literature Review Summary

Author / Year	Research Focus	Method Used	Key Findings	Limitation
Huang et al. (2025)	AI Agent Identity Management	Dynamic IAM Model	Improved machine identity lifecycle	Limited banking focus
Xu et al. (2026)	Decentralized AI Identity	Blockchain-based verification	Strong traceability and trust	High implementation complexity
Janani et al. (2025)	Human–Machine Identity Risk	Security risk analysis	Identified privilege overlap threats	No practical framework
Cisco Systems (2026)	Zero Trust for AI	Policy-based architecture	Continuous verification model	Enterprise generic
Okta (2025)	Adaptive Identity Security	Behavioral analytics	Real-time anomaly detection	Limited autonomous workflow support

III. PROBLEM AND MOTIVATION

Use of self-governed AI entities in banking operations poses serious risks in the areas of security and governance. Unlike conventional software bots, autonomous AI can log into a financial system, conduct transactions, and make decisions without direct human intervention. This creates security risks such as credential hijacking, privilege escalation, unauthorized fund transfer, and compliance risks due to the ambiguity surrounding AI, machine services, and employee identities [6].

IJSES
Volume 10, Issue 7, pp. 25-28, July 2026.
International Journal of Scientific Engineering and Science
ISSN (Online): 2456-7361

Existing IAM solutions suffer from excessive privileges and lack of accountability as they cannot differentiate autonomous AI identities from machine identities. Furthermore, lack of short-term credential management and runtime monitoring exposes the system to cyber-attacks and even insider risks. The objective of this project is to build an architecture where human and machine identities will remain distinct, least privilege policy is enforced, trust verification is continuous, and all AI activities are monitored in real-time. The autonomous financial process becomes more secure, efficient, and complies with regulations [7].

Key Security Challenges

- Human and AI agents sharing credentials
- Lack of machine identity segregation
- Excessive privilege assignment
- Weak behavioural monitoring
- Inadequate auditability and compliance tracking

Research Motivation

- Strengthen trust in autonomous banking systems
- Prevent identity misuse and fraud
- Improve transparency and accountability
- Support regulatory compliance (e.g., Reserve Bank of India, Basel Committee on Banking Supervision guidelines)
- Facilitate safe human-AI interaction

TABLE 2: Problem and Threat Analysis

Threat Category	Description	Risk Level	Banking Impact
Credential Theft	Stolen AI/API credentials	High	Unauthorized access
Privilege Escalation	AI gains excess permissions	High	Fraudulent transactions
Identity Impersonation	Fake agent acts as trusted entity	Medium	Data breach
Insider Threat	Employee misuses delegated access	Medium	Compliance failure
Audit Failure	Lack of traceability	High	Regulatory penalties

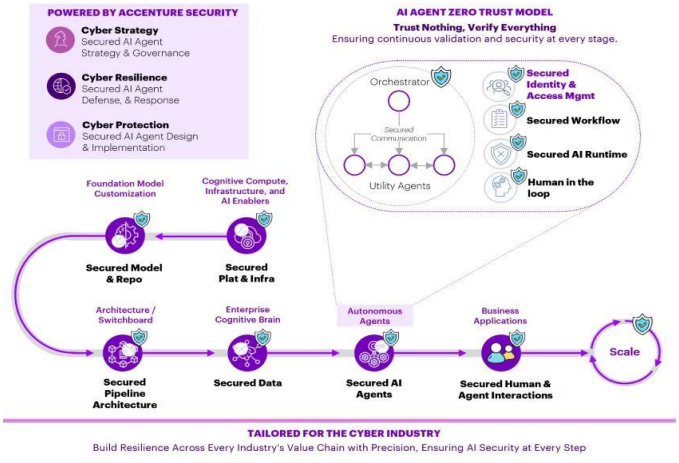

Figure 1: Tailored for The Cyber Industry

IV. Related Work

Facilitate human-AI collaboration safely Recent trends in artificial intelligence governance and Zero-Trust security have significantly influenced identity management literature for autonomous systems [8]. With an emphasis on continuous authentication, enforcement of policies, and secure interactions between machines, Cisco Systems developed a Zero-Trust architecture framework for agentic AI [9]. For scenarios utilizing artificial intelligence, Okta recommended adaptive identity management techniques incorporating behavioural analysis and privilege limitation. Ping Identity emphasized the importance of securing APIs and decentralized machine identities to improve trust among dispersed autonomous systems. Contemporary identity and access management (IAM) strategies in the banking sector generally fail to consider the autonomous AI agents operating without human intervention; rather, they are designed to safeguard human employees and conventional software solutions. While Huang et al. explored temporary credentials and least privilege access for artificial intelligence services, Xu et al. identified blockchain-enabled decentralized identity verification as their contribution. Nevertheless, there is a dearth of studies addressing the requirements of banking procedures that necessitate strict segregation between human and machine identities, continual behavioural assessment, and regulatory compliance in autonomous financial ecosystems [10].

Research Gaps

- Lack of banking-specific AI identity models
- Limited human–AI role separation
- Weak real-time trust validation
- Insufficient runtime anomaly monitoring
- Minimal regulatory alignment for autonomous finance

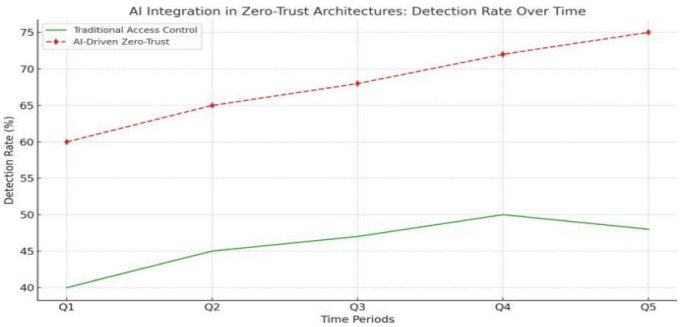

Figure 2: AI Integration in Zero-Trust Architecture Detection Rate Over Time

V. Methodology / Proposed Framework

In this research paper, a proposed architecture of an identity governance framework for autonomous AI agents in banks, the Zero-Trust Identity Governance Framework (ZTIGF), is provided [11]. With the help of designated trust domains, this framework ensures strict isolation among the identities of humans, machines, and AI agents. Every AI agent is granted a unique, ephemeral identifier, which is continuously authenticated using behavioral verification, token rotation, and multi-factor authentication. In order to prevent unnecessary exposure to financial assets, a policy engine applies the least

privilege principle according to their designated tasks. Any suspicious activity by AI agents leads to the activation of real-time monitoring modules, which identify any irregularity and trigger automatic containment of the identified agents. Compliance and accountability are ensured through unalterable audit logs. In all identity verification processes, the system adheres to the principles of Zero Trust, which include "never trust, always verify." The approach minimizes the threat of insiders, credential exploitation, and autonomy by facilitating collaboration between humans and AIs in bank activities [12].

Identity Separation Layer

Divides the three areas of identity:

- Human Identity: employees, analysts, managers
- Machine Identity: APIs, servers, applications
- AI Agent Identity: autonomous bots and decision agents

Preventing identity overlap and privilege confusion is the goal [13].

Continuous Authentication Layer

Implements:

- Multi-Factor Authentication (MFA)
- Mutual TLS (mTLS)
- Token expiration and rotation
- Session trust re-validation

Goal: Ensure dynamic verification of each request [14].

Least Privilege Access *Engine*

Uses:

- Role-Based Access Control (RBAC)
- Attribute-Based Access Control (ABAC)
- Task-bound permissions

Goal: Restrict AI agents to doing only necessary tasks [15].

Behavioural Monitoring Engine

Functions:

- Detect anomalous AI decisions
- Monitor API usage patterns
- Trigger automated alerts

Goal: Find rogue or compromised agents early on [16].

Audit and Compliance Layer

Supports:

- Immutable logging
- Regulatory reporting
- Explainable AI decisions

Purpose: Improve transparency and accountability [17].

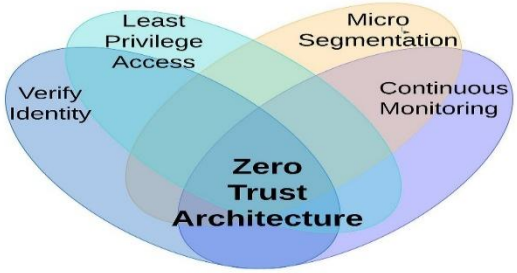

Figure 3: Zero Trust Architecture

VI. Experiment / Case Study / Simulation

An autonomous banking workflow simulation has been designed by employing a loan approval system based on an AI agent for evaluation purposes regarding the proposed Zero-Trust Identity Governance Framework (ZTIGF). Specifically, an AI agent employs banking APIs, credit databases, and client data to autonomously manage loan application processes [18]. The framework continuously validates the identity of an AI agent, monitors its activities, and restricts access using the principle of least privilege. Some of the examples of cybersecurity threats used in testing included credential theft, privilege escalation, and agent impersonation. Numerous performance measures, including operational effectiveness, compliance score, anomaly detection time, and illegal access attempts, have been documented. According to the results, compared to traditional IAM systems, ZTIGF significantly reduces security breaches and promotes audit transparency. Thus, the simulation proves that workflow efficiency is ensured, regulation compliance is achieved in an autonomous environment, and banking security is enhanced due to a distinction between human and machine identities and their constant validation [19].

Case Study Scenario: AI Loan Approval System

Workflow:

- Client makes application for digital lending.
- Financial background of the client is obtained using AI agent.
- Risk model determines eligibility.
- Each activity of AI is authenticated by identity engine.
- Any exception is checked by human supervisor.
- Audit trail includes final approval.

Attack Simulation Scenarios

Tested threats:

- Credential theft attack
- Privilege escalation attempt
- Rogue AI agent behavior
- Unauthorized API access
- Insider misuse simulation

TABLE 3: Simulation Results Comparison

Metric	Traditional IAM	Proposed ZTIGF	Improvement
Unauthorized API Calls	17	2	88%
Privilege Abuse Events	11	1	91%
Detection Time (minutes)	42	6	86%
Compliance Score	72%	96%	24%
Workflow Efficiency	81%	93%	12%

Performance Metrics

Measured:

- Unauthorized access attempts
- Threat detection time
- Compliance score

- Operational delay
- System trust score

Outcome Analysis

Key findings:

- Strong reduction in security incidents
- Faster anomaly detection
- Better regulatory compliance
- Improved trust in autonomous banking workflows

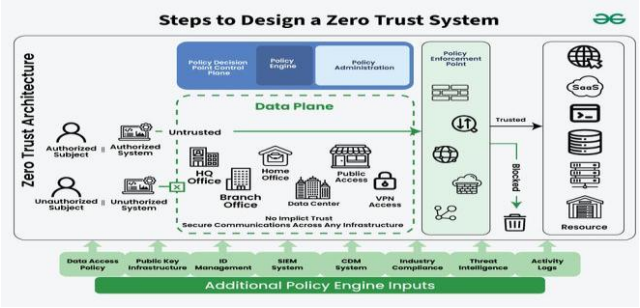

Figure 4: Steps to Design a Zero Trust System

VII. CONCLUSION

While the rise of AI agents in banking has boosted operational efficiency through automation, it has also opened up new risks that revolve around identity management. As such, conventional identity management approaches are not capable enough to distinguish between machine-based services, independently-operating autonomous AI agents, and humans. Therefore, this study proposed Zero-Trust Identity Governance Framework (ZTIGF) using the methods of identity isolation, continuous authentication, principle of least privilege, behavioural monitoring, and immutable audit trails to handle those challenges. Results obtained from the study included reduced threat detection latency, abuse of privilege, and unauthorized access, along with improved compliance and trustworthiness. The proposed architecture provides an opportunity for both human employees and AI robots to work together without compromising personal data and assets of the bank customers. Zero-Trust approach can be used by companies to build an effective, open, and lawful autonomous environment for financial transactions. Additional research should be conducted to develop concepts of explainable AI governance, decentralized identity, and institutionalized trust, which are vital for deploying smart agents worldwide.

REFERENCE

[1] M. F. Ansari, A. Mohammed, K. R. Janamolla, S. W. Khadri, S. A. Khader and M. A. Raheem, "The Double-Edged Sword: Navigating AI's Role in Banking Cybersecurity," 2025 International Conference on Transformative Computing Technologies (ICTCT), Bangalore, India, 2025, pp. 294-300, doi: 10.1109/ICTCT69201.2025.00062

[2] Akinyemi, Adeyemi. "Zero Trust Security Architecture: Principles and Early Adoption." *International Journal of Technology, Management and Humanities* 8, no. 02 (2022): 11-22.

[3] Khader, Shuaib Abdul, Amir Ahmed Ansari, and Syed Sharik Ali. "Zero-Day Exploit Prediction Using Graph-Based Deep Learning on Vulnerability and Threat Intelligence Data."

[4] Reddy, B. (2021). A Quantitative Analysis of Cloud Security Practices in IoT Environment (dissertation).

[5] Ansari, Meraj Farheen, and Syed Sharik Ali. "AI-driven zero-trust architecture for enhanced cybersecurity in dynamic network environments." International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering 13 (2025): 12.

[6] Ansari, Mohammed Azmath, Shaik Aqheel Pasha, and Narendar Kandula. "Reinforcement Learning for Adaptive Network Defense in Financial Institutions."

[7] Reddy, Balavardhan, and Amir Ahmed Ansari. "Ai-Enhanced Network Traffic Analysis For Preventing Fraud Payment In Banks."

[8] 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.

[9] 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

[10] Bajoria, Ashwin Vijaykumar. "Decentralized Autonomous Financial Ecosystems: A Technical Framework for Market Evolution." *Journal Of Engineering And Computer Sciences* 4, no. 8 (2025): 736-742.

[11] Khaja, Moin Uddin, and Balavardhan Reddy. "Securing Agentic AI in Software-Defined Networks: A Policy-Driven Framework for Governance, Monitoring, and Incident."

[12] Samarghandi, Hamed, Davood Askarany, and Bahareh Banitalebi Dehkordi. "A hybrid method to predict human action actors in accounting information system." *Journal of Risk and Financial Management* 16, no. 1 (2023): 37.

[13] Raheem, Mohd Abdul, And Mohammed Azmath Ansari. "Intelligent And Trustworthy 6g: Ai-Driven Architectures, Applications, And Security Frameworks

[14] Gouni, Praveen Kumar Reddy, and Eraj Farheen Ansari. "The Impact of Cyber-Physical Attacks on AI-Enabled Business Systems

[15] 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.

[16] Rimal, Bipin. "From Rogue Employees to Rogue Agents: Repurposing Insider Threat Detection for AI Agent Governance." *Available at SSRN 6355658* (2026).

[17] Kashif, M., & Ansari, A. A. (2026). Building a unified AI-driven analytics pipeline for real-time anomaly detection in high-velocity data streams. IJIREEICE, 14(1), 66–75. https://doi.org/10.17148/ijireeice.2026.14111

[18] 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.

[19] Khader, Shuaib Abdul Khader, and Praveen Kumar Reddy Gouni Gouni. "Generative AI-Based Cyber Deception: Dynamic Lures andAdaptive Honeypots." Journal of Cognitive Computing and Cybernetic Innovations 1, no. 3 (2025): 44-52.