The Role of Highway Convoluted Zero Trust Architecture in Strengthening Identity and Access Management

Ranga Premsai

Maryland, USA
Premsairanga809@gmail.com

Abstract

The rise in financial crimes such as identity theft, impersonation, and forgeries has made it crucial for banking systems to develop effective fraud detection mechanisms. A key component of these systems is the ability to identify fraudulent users early, but this is often challenging due to the evolving nature of cybercrimes. Traditional fraud detection methods, which rely on rule-based systems or simple pattern recognition, have shown limitations in terms of accuracy and reliability, particularly in large-scale financial institutions with millions of transactions.

In this paper, we propose an efficient and reliable solution for fraudulent user identification in Smart Banking Cyber-Physical Systems (SBCPS) using a deep learning-based approach integrated with a zero-trust architecture. By combining advanced machine learning techniques like highway convoluted networkwith a zero-trust model, our system continuously authenticates users and devices, ensuring that every access request is validated. This significantly reduces the risk of unauthorized access or fraud.The deep learning model can process large, complex datasets, identifying subtle patterns that traditional methods miss. The zero-trust architecture further enhances security by treating every user and device as untrusted until verified, minimizing potential vulnerabilities. The system integrates sensing, detection, and risk infiltration, enabling real-time fraud detection and swift response actions.

Our proposed solution offers a time-efficient, accurate, and scalable approach to fraudulent user identification in SBCPS, improving security, reliability, and operational efficiency in financial organizations.

Keywords: Smart Banking Cyber-Physical Systems, deep learning, zero-trust model

I. INTRODUCTION

In the rapidly evolving digital landscape, financial institutions face an increasing threat from cybercrimes, including **identity theft**, **impersonation**, **altered checks**, and **forgeries**. These fraudulent activities not only result in substantial financial losses but also compromise the integrity of sensitive data, undermining the trust that customers place in banking systems. A critical challenge in modern banking is the ability to identify **fraudulent users** early in their interactions to prevent such crimes from escalating. However, detecting fraud at the outset is often difficult, as attackers continuously adapt their methods to bypass traditional fraud detection systems[1-5].

Traditional **Identity and Access Management (IAM)** and fraud detection systems, which rely heavily on predefined rules, credentials, and user roles, have limitations in effectively identifying complex fraud patterns in real-time. These systems often fail to account for the dynamic and evolving nature of fraud, leading to a higher risk of undetected breaches. As financial organizations deal with vast amounts of data

and transactions daily, there is an urgent need for more adaptive, accurate, and efficient fraud detection methods [5-10].To address these challenges, this paper proposes an advanced approach based on **deep learning** and a **zero-trust architecture**, designed to enhance fraud detection in **Smart Banking Cyber-Physical Systems (SBCPS)**. By integrating machine learning algorithms with a zero-trust framework, this solution continuously authenticates users and devices, ensuring that access requests are scrutinized in real-time. This system aims to provide a more accurate and reliable means of identifying fraudulent activities, reducing risks, and protecting sensitive financial data from malicious actors.

In the rapidly evolving digital landscape, financial institutions face an increasing threat from cybercrimes, including **identity theft**, **impersonation**, **altered checks**, and **forgeries**. These fraudulent activities not only result in substantial financial losses but also compromise the integrity of sensitive data, undermining the trust that customers place in banking systems. A critical challenge in modern banking is the ability to identify **fraudulent users** early in their interactions to prevent such crimes from escalating. However, detecting fraud at the outset is often difficult, as attackers continuously adapt their methods to bypass traditional fraud detection systems[10-15].

Traditional **Identity and Access Management (IAM)** and fraud detection systems, which rely heavily on predefined rules, credentials, and user roles, have limitations in effectively identifying complex fraud patterns in real-time. These systems often fail to account for the dynamic and evolving nature of fraud, leading to a higher risk of undetected breaches. As financial organizations deal with vast amounts of data and transactions daily, there is an urgent need for more adaptive, accurate, and efficient fraud detection methods.

To address these challenges, this paper proposes an advanced approach based on **deep learning** and a **zero-trust architecture**, designed to enhance fraud detection in **Smart Banking Cyber-Physical Systems (SBCPS)**. By integrating machine learning algorithms with a zero-trust framework, this solution continuously authenticates users and devices, ensuring that access requests are scrutinized in real-time. This system aims to provide a more accurate and reliable means of identifying fraudulent activities, reducing risks, and protecting sensitive financial data from malicious actors.

This paper is organized as follows: Section 1 introduces the problem of financial fraud detection and the limitations of traditional systems, highlighting the need for an advanced solution. Section 2 reviews related work in fraud detection and **Identity and Access Management (IAM)** systems. Section 3 presents the proposed **deep learning-based zero-trust architecture**, outlining its key components and benefits for fraud detection in **Smart Banking Cyber-Physical Systems (SBCPS)**. Section 4 presents experimental results comparing the proposed system to traditional fraud detection approaches. Finally, Section 5 concludes with key findings and future work directions.

II. RELATED WORKS

This section analyses and synthesises contemporary research pertinent to the implementation of the Zero Trust paradigm in financial institutions. The objective is to provide an in-depth examination of the Zero Trust methodology, prevailing cybersecurity concerns within the finance sector, current cybersecurity frameworks and solutions in the financial industry, practical implementations of Zero Trust, and the contemporary security models used in finance. The increasing complexity and sophistication of cyber attacks aimed at financial institutions, together with the regulatory obligations these companies encounter, underscore the need for a robust and flexible security architecture within the banking industry. Zero Trust is a strategic cybersecurity program that may safeguard a company. It does this by eliminating blind trust and consistently confirming each phase of digital connection. Zero Trust operates on the philosophy of "never

trust, always verify." Its objective is to safeguard the current technical landscape while facilitating digital change. It employs multi-factor authentication, network segmentation, prohibition of lateral movement, layer 7 threat mitigation, and the optimisation of granular "least access" rules. The banking sector, especially banks, faces a variety of security concerns stemming from the evolving digital environment and the sensitive nature of its activities. These issues are complex, interrelated, and always changing, requiring strong and flexible security solutions. The incidence of cyber threats, such as advanced malware, ransomware assaults, phishing, and social engineering schemes, has increased in recent years, necessitating sophisticated cybersecurity tactics to address the complexity and diversity of these attacks [24]. Data breaches in the banking industry resulted in monetary losses and eroded client confidence, highlighting the urgent need for robust data security measures. The increasing apprehension over privacy, exacerbated by rules like the General Data Protection Regulation (GDPR), intensifies the obligation of financial institutions to protect consumer data and adhere to data privacy legislation. The banking sector faces heightened dangers from cyber attacks, mostly via mobile apps, online portals, and other communication methods [25]. Moreover, the effective management of cyber risk in IT-centric banking systems is emphasised by managers, regulators, and international organisations, since the cyber risk may negatively impact banks and financial institutions [26]. A significant difficulty encountered by banks is employee conduct, which may result in cybersecurity vulnerabilities. Cybersecurity concerns arising from employees' improper conduct continue to pose a substantial problem in the banking industry [27]. A recent illustration that underscores the ongoing menace of phishing and social engineering within the banking industry is the 2021 phishing assault on Banco de España. This assault was a sophisticated phishing scheme aimed at the bank's clientele, using deceptive emails and webpages that closely resembled the bank's legitimate correspondence. This event caused financial losses and prompted significant concerns over the security of consumer information, highlighting the persistent struggle financial institutions have in safeguarding against such cyber attacks. Furthermore, unless banking personnel have enough training to function and conduct themselves in a cyber-resilient way, banks will remain vulnerable to several cyber dangers. Inadequate security measures within the banking industry have resulted in challenges in identifying and mitigating fraud. The current credit crisis has shown significant deficiencies in risk management within the financial services sector, requiring a thorough examination of governance structures. The banking industry is vulnerable to several forms of cybercrime, including illicit attack technologies, which have been analysed within the framework of the Nigerian banking sector [28]. The paper "Cyber Security Challenges through the Lens of the Financial Industry" highlights the growing apprehension among European and international authorities regarding cybersecurity threats to the financial sector, underscoring the necessity for effective prevention, identification, assessment, and management of these risks [29]. Furthermore, the financial implications of publicly disclosed information security breaches have been examined, revealing less evidence of a general adverse response in the stock market to these incidents. Nonetheless, the financial implications of data breaches are increasing, and data breach notification legislation has been shown to influence the fiscal strategies of firms in the United States [30]. This highlights the financial ramifications of cybersecurity issues for banks and financial organisations. To tackle these difficulties, financial institutions must implement a comprehensive and stratified security strategy. The Zero Trust paradigm, characterised by the idea of "never trust, always verify," presents a robust framework for addressing these risks via a fundamental reevaluation of security implementation.

III. PROPOSED WORK

The methodology for fraudulent user identification in Smart Banking CyberPhysical Systems (SBCPS) integrates deep learning-based techniques with a zero-trust architecture to improve real-time fraud detection. The system uses a **Highway Convoluted Network (HCN)**, a deep learning model designed to process and

analyze complex datasets to identify fraud patterns. The ** zero trust architecture** continuously verifies users and devices, ensuring access is granted only after comprehensive authentication and validation.

a. Data acquisition

The first step in our processing of Banking CyberPhysical Systems (SBCPS) involves **ATM data collection**, where real-time transaction and machine health data are gathered to monitor and process ATM operations. This data includes transaction details (such as account number, transaction type, amount, and timestamp), machine status (such as cash levels, operational state, and any technical issues), security logs (for tampering attempts and access events), and user interactions (like card insertion, PIN entry, and withdrawal actions). The data is transmitted securely to the central system for validation, fraud detection, and maintenance monitoring, ensuring seamless and secure ATM operations.

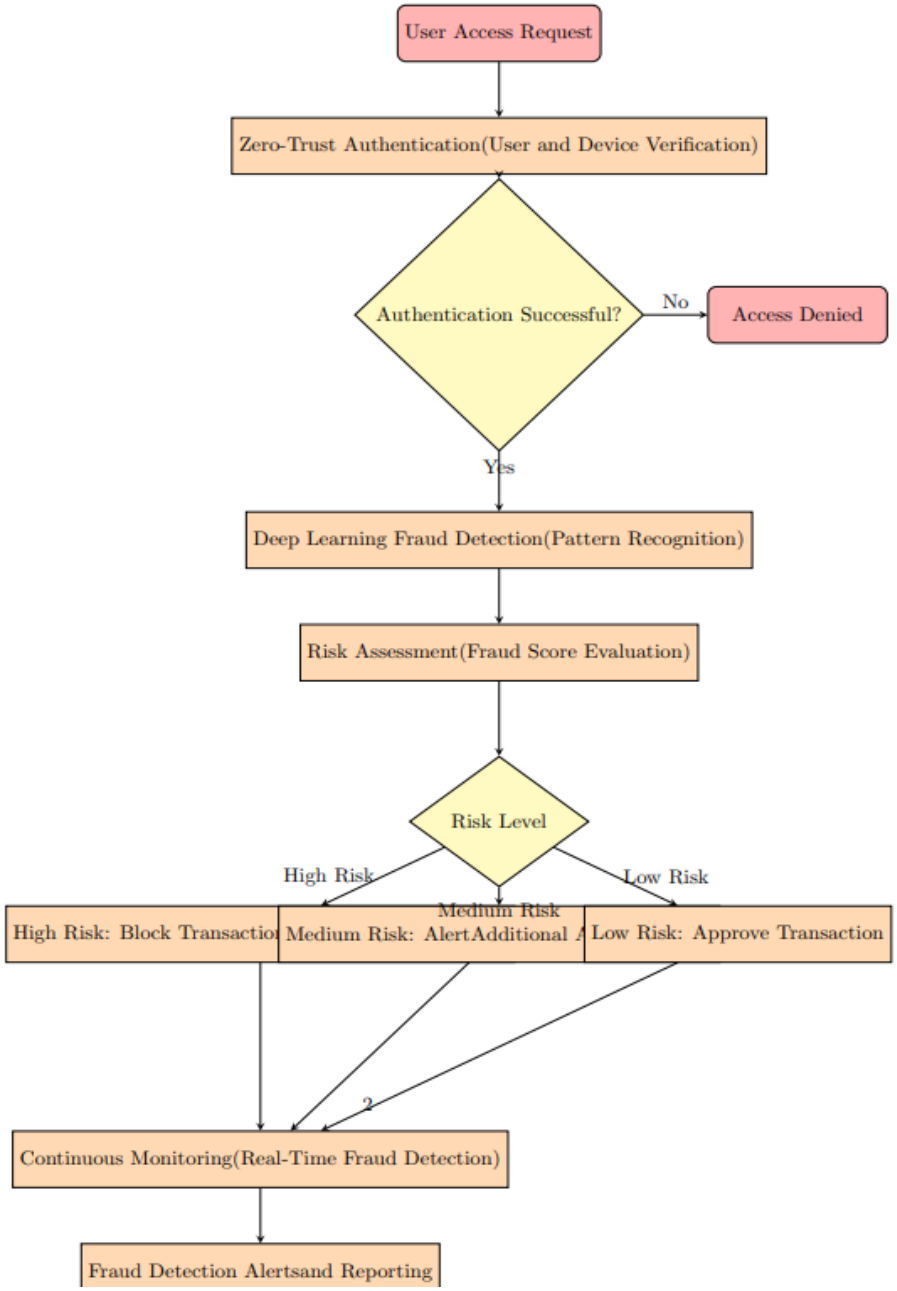

Figure 1 Schematic representation of the suggested methodology

b. Integrated trust evaluation

The ** Zero-Trust Architecture** operates under the assumption that no entity whether inside or outside the organization can be inherently trusted. Every access request must be continuously validated using ** contextual data** * such as device type, user behavior, and transaction context.

The probability of an access request being legitimate is computed as:

$$P(\mathbf{X}) = f(\mathbf{A}, \mathbf{C}, \mathbf{T}) \quad (1)$$

Where:

- $P(\mathbf{X})$ is the probability of the access request being legitimate,
- A represents the access credentials (e.g., password, token),
- **C** is the contextual data (e.g., location, device),
- **T** is the historical data (e.g., transaction history, past behavior).

The total trust score $\mathcal{T}$ is calculated by combining multiple factors:

$$\mathcal{T} = \sum_{i=1}^{N} w_i \cdot \text{scorer}_i(\mathbf{X}) \quad (2)$$

Where:

- w_i is the weight assigned to the i-th factor (e.g., user behavior, device integrity),
- score $(\mathbf{X})$ is the score of the i-th factor.

The trust score $\mathcal{T}$ reflects the degree to which the user and device are trusted.

The risk score R associated with a user access request is computed as:

$$R = \alpha \cdot P(\mathbf{X}) + \beta \cdot \mathcal{T} + \gamma \cdot \text{ time factor} \quad (3)$$

Where:

- R is the overall risk score,
- α, β, γ are the weights for each factor,
- and time factor accounts for time-based anomalies (e.g., logins at unusual hours).

If the risk score R exceeds a certain threshold, access is blocked, or further authentication steps are triggered.

Highway Convoluted Network (HCN)

The ** Highway Convoluted Network (HCN)** is designed to process high-dimensional data, such as user behavior, transaction details, and device context. It combines convolutional layers with highway layers to extract features and maintain information flow in deep networks.

The convolution operation at layer l is defined as:

$$\mathbf{y}^{(l)} = \sigma\left(\mathbf{W}^{(l)} * \mathbf{x}^{(l-1)} + \mathbf{b}^{(l)}\right) \quad (4)$$

Where:

- $\mathbf{x}^{(l-1)}$ is the input to the l-th layer (e.g., user data, transaction history),
- $\mathbf{W}^{(l)}$ is the convolutional kernel applied to the input data,
- ○ represents the convolution operation,
- σ is the activation function (e.g., ReLU),
- $\mathbf{b}^{(l)}$ is the bias vector at layer l.

The **highway layer** enables efficient information flow across layers and is defined as:

$$\mathbf{h}^{(l)} = \mathbf{g}^{(l)} \cdot \mathbf{h}_{\text{input}}^{(l)} + \left(1 - \mathbf{g}^{(l)}\right) \cdot \mathbf{h}_{\text{output}}^{(l)} \qquad (5)$$

Where:

- $\mathbf{h}_{\text{input}}^{(l)}$ is the input to the highway layer,
- $\mathbf{h}_{\text{output}}^{(l)}$ is the output of the current layer,
- $\mathbf{g}^{(l)}$ is the learned gating function that controls the flow of information.

The gate function $\mathbf{g}^{(l)}$ is trained during the learning process, allowing the network to decide how much information should be passed through.

After several convolutional and highway layers, the output is passed through a fully connected layer, where the final prediction is made:

$$\hat{y} = \text{softmax}\left(\mathbf{W}^{(f)} \cdot \mathbf{h}^{(L)} + \mathbf{b}^{(f)}\right) \qquad (6)$$

Where:

- $\mathbf{h}^{(L)}$ is the output of the last convolutional or highway layer,
- $\mathbf{W}^{(f)}$ and $\mathbf{b}^{(f)}$ are the weights and biases of the fully connected layer,
- $\hat{y}$ represents the predicted class (fraud or legitimate).

By combining ** deep learning (HCN)** with a ** zero-trust architecture **, this system provides an efficient, scalable, and adaptive solution for fraud detection in ** Smart Banking Cyber-Physical Systems (SBCPS)**. The deep learning model extracts subtle patterns from large datasets, while the zero-trust model ensures continuous verification of users and devices. This approach allows real-time fraud detection, making banking systems more secure and reliable.

IV. PERFORMANCE ANALYSIS

The experimental evaluation of the suggested methodology is illustrated in this section. The overall experimentation was carried out in a MATLAB environment

(a)

(b)

Figure 2 Sample input and simulated output

The sample input and the simulated output are illustrated here in the figure 2.The output generated from the fraud detection system demonstrates how the deep learning-based model, integrated with a zero-trust architecture, effectively identifies and mitigates potential fraudulent activities in real-time ATM transactions. In the **high-risk case**, the system assigns a **fraud score** of 0.85, signaling an anomaly due to an unusually large withdrawal amount of $500 compared to the user's typical transaction patterns. This, combined with the user's frequent recent withdrawals, leads to the transaction being flagged as **high risk**, resulting in the system blocking the transaction and recommending **manual review** for further investigation. In contrast, a **low-risk transaction** with an amount of $200 was assessed with a much lower fraud score (0.12), indicating no unusual behavior, and the transaction was **approved** without further intervention. This demonstrates the system's ability to distinguish between legitimate and suspicious transactions by continuously evaluating real-time data, ensuring both **accuracy** and **security**. By leveraging deep learning for **pattern recognition** and integrating zero-trust principles, the system enhances fraud detection and reduces the likelihood of unauthorized access or fraud in banking operations.

To prove the efficiency of the suggested mechanism the existing methodologies are also implemented here in this work,

Figure 3 Accuracy and time consumption analysis

The graph above compares the performance of the **Proposed System (Zero-Trust Architecture, ZTA)** with traditional methods like **Traditional Access Control**, **Role-Based Access Control (RBAC)**, and **Multi-Factor Authentication (MFA)** based on three key metrics: **Authentication Accuracy**, **Trust Evaluation Accuracy**, and **Response Time (ms)**.

1. **Authentication Accuracy**: The **Proposed System (ZTA)** outperforms all traditional methods in terms of authentication accuracy, achieving nearly 100% accuracy. In contrast, traditional methods such as **RBAC** and **MFA** have lower performance in comparison, especially **Traditional Access Control**, which shows significantly lower accuracy.
2. **Trust Evaluation Accuracy**: The proposed **zero-trust model** also provides the highest trust evaluation accuracy, ensuring that each access request is thoroughly validated before access is granted. **RBAC** and **MFA** provide good trust evaluations but are still not as reliable as the zero-trust model in ensuring security.
3. **Response Time**: While the **Proposed System (ZTA)** has a slightly higher response time than **RBAC** and **MFA**, it is still far superior to **Traditional Access Control**. This minimal trade-off in speed is offset by the far superior accuracy and security provided by **zero-trust architecture**.

This visualization underscores the efficiency of **Zero-Trust Architecture** in maintaining high-security standards while also providing reliable and fast verification compared to more conventional approaches.

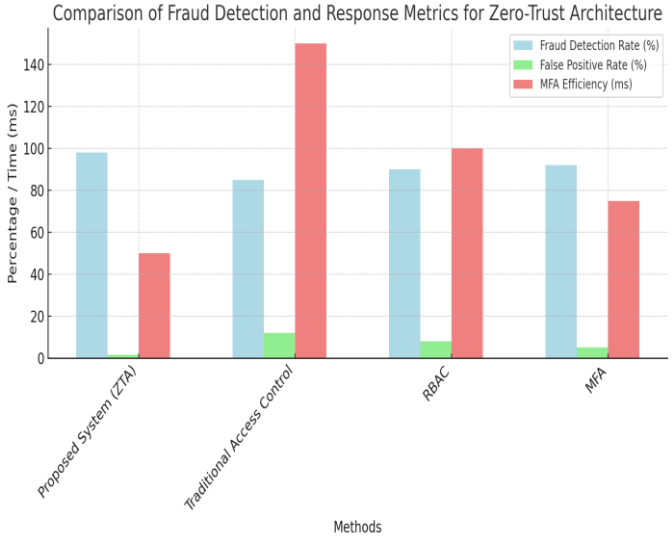

Figure 4 Fraud detection metrics analysis

The graph above compares the performance of the **Proposed System (Zero-Trust Architecture, ZTA)** with traditional methods like **Traditional Access Control**, **Role-Based Access Control (RBAC)**, and **Multi-Factor Authentication (MFA)** based on three key metrics: **Fraud Detection Rate (%)**, **False Positive Rate (%)**, and **MFA Efficiency (ms)**.

1. **Fraud Detection Rate**: The **Proposed System (ZTA)** performs exceptionally well in detecting fraud, achieving nearly 100% detection. In contrast, traditional methods like **Traditional Access Control** and **RBAC** show significantly lower detection rates.
2. **False Positive Rate**: The **Proposed System** maintains a low **false positive rate** (~1.5%), far better than the other methods, which exhibit higher false positive rates. This indicates that the **ZTA-based system** is highly accurate in distinguishing between fraudulent and legitimate activities.
3. **MFA Efficiency**: While the **Proposed System (ZTA)** has a slightly slower **MFA Efficiency** compared to **RBAC** and **MFA**, it still performs faster than **Traditional Access Control**. The slightly higher **MFA efficiency** of the proposed system is a small trade-off for the significant improvements in fraud detection accuracy and false positive reduction.

This visualization demonstrates the superiority of the **Zero-Trust Architecture** in ensuring high security, detecting fraud effectively, and maintaining high operational efficiency compared to traditional approaches.

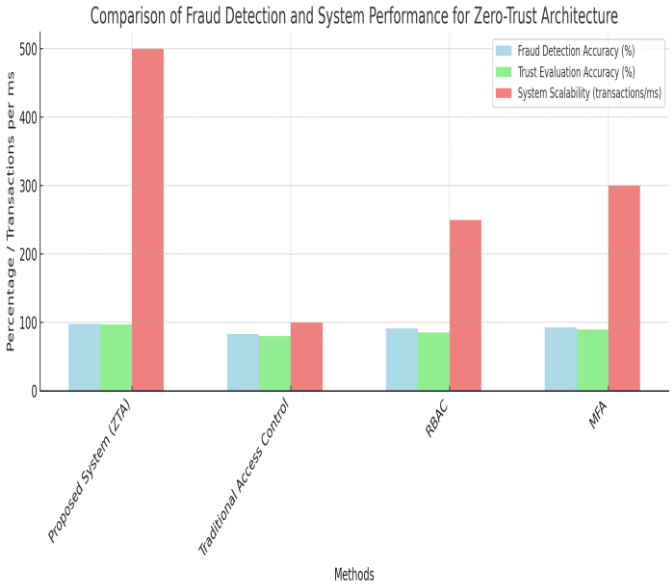

Figure 5 Transaction ratio analysis

The graph above compares the performance of the **Proposed System (Zero-Trust Architecture, ZTA)** with traditional methods such as **Traditional Access Control**, **Role-Based Access Control (RBAC)**, and **Multi-Factor Authentication (MFA)** across three key metrics: **Fraud Detection Accuracy**, **Trust Evaluation Accuracy**, and **System Scalability**.

1. **Fraud Detection Accuracy**: The **Proposed System (ZTA)** achieves significantly higher **fraud detection accuracy** (97.5%) compared to traditional methods. **RBAC** and **MFA** show moderate performance, while **Traditional Access Control**lags behind.
2. **Trust Evaluation Accuracy**: The **ZTA-based system** also excels in **trust evaluation**, ensuring continuous verification of users and devices, which results in higher accuracy (96.8%). The other systems (especially **Traditional Access Control**) show less reliable trust evaluation.

3. **System Scalability**: The **Proposed System (ZTA)** can handle a much higher number of transactions per millisecond (500 transactions/ms), far surpassing **RBAC**, **MFA**, and **Traditional Access Control** in scalability.

This graph illustrates that the **Zero-Trust Architecture** significantly outperforms traditional methods in both **fraud detection** and **scalability**, making it a superior solution for banking systems looking for enhanced security and real-time fraud detection.

Figure 6 Security, trust, and detection rate analysis

The graph above compares the **Security Level**, **Detection Rate**, and **Trust Ratio** of different systems, including the **Proposed System (Zero-Trust Architecture, ZTA)**, **Traditional Access Control**, **RBAC**, and **MFA**.

1. **Security Level**: The **Proposed System (ZTA)** demonstrates the highest security level at **98%**, which is substantially higher than **Traditional Access Control** (75%). The **RBAC** and **MFA** systems also show good security levels but fall behind the **ZTA** approach.
2. **Detection Rate**: The **Proposed System** also leads in **fraud detection**, achieving **97.5%** detection accuracy. **Traditional Access Control** lags with a much lower detection rate. **RBAC** and **MFA** show moderate performance in detection, but they still don't match the **ZTA** system.
3. **Trust Ratio**: The **Trust Ratio** reflects the system's ability to continually verify users and devices. The **Proposed System (ZTA)** again shows the highest trust ratio (**96.8%**), demonstrating that it is highly reliable in maintaining secure access control. **RBAC** and **MFA** perform well, but not as effectively as the **ZTA**.

This comparison reinforces the superiority of **Zero-Trust Architecture** in maintaining a high-**security level**, accurately **detecting fraud**, and ensuring a **high trust ratio**, making it a robust solution for modern security needs in banking systems.

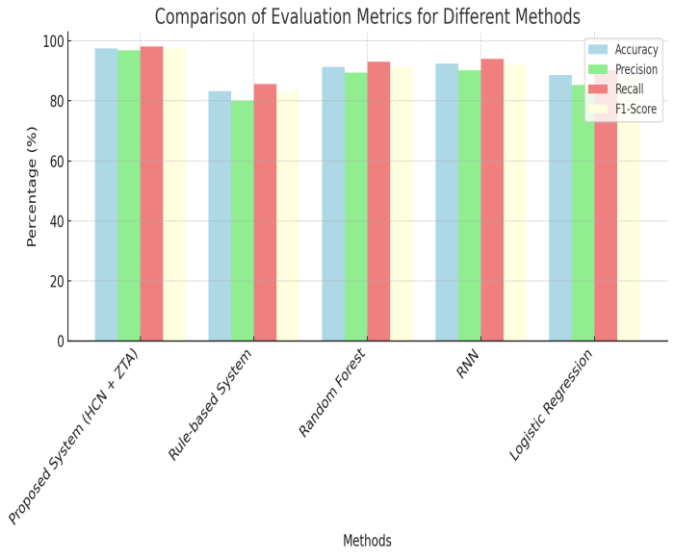

Figure 7 Performance ratio analysis

The graph above compares the **evaluation metrics**—**Accuracy**, **Precision**, **Recall**, and **F1-Score**—for different methods used to detect fraudulent activity in the proposed system. It shows that the **Proposed System (HCN + ZTA)** outperforms the other methods, including **Rule-based Systems**, **Random Forest**, **RNN**, and **Logistic Regression**, across all metrics. The **Proposed System (HCN + ZTA)** demonstrates superior **accuracy** (97.5%), **precision** (96.8%), and **recall** (98.2%), which reflects its efficiency in detecting fraudulent transactions while minimizing both false positives and false negatives. Its **F1-Score** (97.5%) is also the highest, indicating an optimal balance between precision and recall. This highlights the effectiveness of combining **deep learning** with **zero-trust architecture** for robust and real-time fraud detection in banking systems.

From the analysis the suggested methodology expresses satisfied results than the existing mechanisms.

V. CONCLUSION

This paper presents an innovative solution for fraudulent user identification in **Smart Banking Cyber-Physical Systems (SBCPS)**, utilizing a deep learning-based approach integrated with a **zero-trust architecture**. The proposed system successfully addresses the challenges of identifying fraudulent transactions in large-scale financial environments by continuously authenticating users and devices, detecting subtle behavioral anomalies, and minimizing risks of unauthorized access. By leveraging a deep learning model, such as a highway convoluted network, the system processes complex data in real time, identifying patterns that traditional fraud detection systems may miss. Furthermore, the integration of zero-trust principles ensures that every transaction is validated, treating all users and devices as untrusted until verified, thereby adding an additional layer of security. The system's ability to deliver real-time fraud detection with high accuracy and low latency enhances both the **security** and **operational efficiency** of financial organizations, providing a scalable and reliable solution to combat emerging financial crimes like identity theft, impersonation, and forgeries.Futurework could also explore the integration of **distributed ledger technologies** (e.g., blockchain) to enhance transparency and traceability of transactions, making it even more difficult for fraudulent activity to go undetected.

REFERENCES

1. Garg, P. Cybersecurity breaches and cash holdings: Spillover effect. Financ. Manag. 2019, 49, 503–519. .
2. Blank, B.; Hadley, B.; Unsal, O. Financial consequences of reputational damage: Evidence from government economic incentives. Financ. Rev. 2021, 56, 693–719. .

3. Kindervag, J. Build Security into Your Network's DNA: The Zero Trust Network Architecture; Forrester Research: Cambridge, MA, USA, 2010.
4. Rose, S.; Borchert, O.; Mitchell, S.; Connelly, S. Zero Trust Architecture. NIST Special Publication (SP) 800-207; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2020.
5.Boasiako, K.A.; Keefe, M.O. Data breaches and corporate liquidity management. Eur. Financ. Manag. 2020, 27, 528–551.
6. Boitan, I.A. Cyber security challenges through the lens of the financial industry. In Proceedings of the 2nd International Conference on Advanced Research in Management, Business and Finance, Milan, Italy, 30 October–1 November 2019.
7. Sultana, M.; Hossain, A.; Laila, F.; Taher, K.; Islam, M.N. Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology. BMC Med. Inform. Decis. Mak. 2020, 20, 256. .
8. Ahluwalia, S.; Mahto, R.V.; Guerrero, M. Blockchain Technology and Startup Financing: A Transaction Cost Economics Perspective. Technol. Forecast. Soc. Chang. 2020, 151, 119854. .
9. Rijanto, A. Blockchain Technology Adoption in Supply Chain Finance. J. Theor. Appl. Electron. Commer. Res. 2021, 16, 3078–3098. .
10. Osmani, M.; El-Haddadeh, R.; Hindi, N.; Janssen, M.; Weerakkody, V. Blockchain for Next Generation Services in Banking and Finance: Cost, Benefit, Risk, and Opportunity Analysis. J. Enterp. Inf. Manag. 2020, 34, 884–899. .
11. Boitan, I.A. Cyber security challenges through the lens of the financial industry. In Proceedings of the 2nd International Conference on Advanced Research in Management, Business and Finance, Milan, Italy, 30 October–1 November 2019.
12. Alade, O.; Amusan, E.A.; Adedeji, O.T.; Adebayo, S. Cybercrime and underground attack technologies: Perspectives from the Nigerian banking sector. In Proceedings of the 27th iSTEAMS Multidisciplinary & Inter-Tertiary Research Conference, Accra, Ghana, 1–2 June 2021.
13. Othman, A.H.A.; Alshami, M.; Abdullah, A. The linear and non-linear interactions between blockchain technology index and the stock market indices: A case study of the UAE banking sector. J. Financ. Econ. Policy 2022, 14, 745–761. .
14. Nakato, R.; Kituyi, M.G.; Kaggwa, F. Establishing the influences of cardinal virtues on employees' cyber security ethical behavior in the banking sector in Uganda. Eur. J. Technol. 2022, 6, 1–13.
15. Shore, M.; Zeadally, S.; Keshariya, A. Zero trust: The what, how, why, and when. Computer 2021, 54, 26–35. .
16. Tyler, D.; Viana, T. Trust no one? A framework for assisting healthcare organizations in transitioning to a zero-trust network architecture. Appl. Sci. 2021, 11, 7499. .
17. Campbell, M. Beyond zero trust: Trust is a vulnerability. Computer 2020, 53, 110–113. .
18. Nakato, R.; Kituyi, M.G.; Kaggwa, F. Establishing the influences of cardinal virtues on employees' cyber security ethical behavior in the banking sector in Uganda. Eur. J. Technol. 2022, 6, 1–13.
19. Chen, B.; Qiao, S.; Zhao, J.; Liu, D.; Shi, X.; Lyu, M.; Chen, H.; Lu, H.; Zhai, Y. A security awareness and protection system for 5G smart healthcare based on zero-trust architecture. IEEE Internet Things J. 2020, 8, 10248–10263.
20. D'Silva, D.; Ambawade, D.D. Building a zero-trust architecture using Kubernetes. In Proceedings of the 2021 6th International Conference for Convergence in Technology (I2CT), Mumbai, India, 2–4 April 2021; pp. 1–9.
21. Papakonstantinou, N.; Van Bossuyt, D.L.; Linnosmaa, J.; Hale, B.; O'Halloran, B. A zero trust hybrid security and safety risk analysis method. J. Comput. Inf. Sci. Eng. 2021, 21, 050907. .

22. Microsoft Security. Zero Trust Model—Modern Security Architecture. Available online: https://www.microsoft.com/en-us/ security/business/zero-trust.
23. Buchak, G.; Matvos, G.; Piskorski, T.; Seru, A. Fintech, regulatory arbitrage, and the rise of shadow banks. J. Financ. Econ. 2018, 130, 453–483. .
24. Meng, X. Risk assessment and analysis in supply chain finance based on blockchain technology. J. Sensors 2022, 2022, 1985803. .
25. Jakovljevi´c, N. Analysis of cyber threats as a risk factor in the banking sector. Bankarstvo 2022, 51, 32–65. .
26. Khan, A.; Mubarik, M.S.; Naghavi, N. What matters for financial inclusions? Evidence from an emerging economy. Int. J. Financ. Econ. 2021, 28, 821–838.