Babylonian Journal of Networking
Vol.2026, **pp**. 49–53
DOI: https://doi.org/10.58496/BJN/2026/007; ISSN: 3006-5372
https://mesopotamian.press/journals/index.php/BJN

Research Article

An Adaptive Deep Reinforcement Learning Framework for Real-Time Identity Verification and Threat Response in Networked Systems

Mohammad Shadab Khan [1,*]

[1] *Multimedia University Faculty of Computing and Informatics - Faculty of Computing and Informatics, Multimedia University Faculty of Computing and Informatics, Malaysia*.

ARTICLE INFO

Article History
Received 08 Jun 2026
Revised 20 Jul 2026
Accepted 08 Aug 2026
Published 12 Sep 2026

Keywords
Deep Reinforcement Learning,
Real-Time Identity Verification,
Threat Response,
Adaptive Security,
Anomaly Detection.

ABSTRACT

Networked systems increasingly connect users, devices, applications, and services, making continuous identity verification essential for maintaining secure digital environments. Adaptive security technologies can learn from changing behavioral patterns and respond to emerging threats more effectively than static mechanisms. This study addresses the problem of maintaining accurate real-time identity verification while dynamically responding to evolving identity-related threats in networked systems. Static authentication methods and fixed security rules may fail when legitimate behavior changes or attackers develop new strategies, increasing false decisions and delaying threat mitigation. To address this challenge, this study develops an adaptive deep reinforcement learning framework that integrates identity, behavioral, device, and network information into dynamic security states. The framework enables a learning agent to select verification and threat-response actions according to current conditions and continuously improve its policy through environmental feedback. Experimental results show that the framework achieves 97.2% verification accuracy, 96.5% precision, 96.8% recall, and a 96.6% F1-score with an average response time of 38 ms. These results demonstrate improved performance compared with traditional machine learning, deep learning, reinforcement learning, and existing DRL approaches. The findings extend existing research by jointly optimizing identity verification and threat response through adaptive decision-making, providing a more responsive approach for evolving network security environments.

1. INTRODUCTION

As networked environments become more integrated and connect end-users, machines, software applications, and services together, identity verification has become an indispensable requirement for establishing safe digital ecosystems [1]. The fast expansion of distributed networks results in ever-changing attack vectors in which identity-based attacks can constantly change and leverage the vulnerabilities of authentication and access control schemes [2]. Conventional methods of verifying identities are usually based on static rules, pre-defined thresholds, or models that are periodically adjusted, restricting their capability to respond to changing threats [3]. Such constraints become especially acute in real-time systems, where security decisions need to be made fast but still accurate and without any false alarms [4].

The current research work is concerned with the requirement of a dynamic mechanism that will be able to learn from the dynamic network environment and react to the identity-related attacks in an intelligent manner. The research framework is combining deep reinforcement learning with the identity verification in order to develop an intelligent agent that will be able to analyze the authentication states, take action based on that state and the identity of the individual user and then will learn from the security outcomes of that action. As a result, the framework is adapting its verification approaches according to behavioral dynamics and new threat patterns in the network environment.

2. LITERATURE REVIEW

Recent studies on identity verification and network security have begun to incorporate machine learning and deep learning techniques for detecting unusual users, anomalous behaviors during identity verification, and emerging cybersecurity threats [5]. Traditional techniques have adopted supervised classification algorithms, anomaly detection mechanisms, and behavioral profiling for enhancing identity verification precision [6]. Nevertheless, these techniques mostly rely on pre-defined features, past data, and decision boundaries, which might lower their efficiency as user behaviors and attack

*Corresponding author. Email: shadabkhan121923@outlook.com

behaviors vary over time [7]. Although deep learning algorithms have made considerable improvement in automatic feature generation and behavioral representation, most current techniques are acting as static prediction techniques instead of adapting themselves based on security conditions [8].

The application of reinforcement learning (RL) can provide a new direction because RL allows the agents to learn from their interactions with the environment [9]. Deep reinforcement learning (DRL), which is the combination of reinforcement learning and deep neural representations, can be used for network security purposes [10]. So far, there are many studies about the application of DRL in intrusion detection, access control, resource allocation, and threat response [11]. However, most research efforts still concentrate on the detection of general network attacks instead of considering the problem of continuously verifying the identities while responding to threats [12]. In addition, most systems do not consider the evaluation of the two processes together [13]. Research gap is in the lack of such a coherent adaptive framework that learns about identity behaviors, selects appropriate verification techniques and reacts to new threats dynamically and in real-time [14]. The proposed research seeks to bridge this research gap by proposing an adaptive Deep Reinforcement Learning framework for identity verification and threat response decision making [15].

3. METHODOLOGY

The methodology is meant to offer an adaptive and real-time identity verification process that is able to react to any threats automatically. The integration of identity and behavior data with deep reinforcement learning is being used to achieve continuous security decision-making process. The methodology has been divided into four stages sequentially as follows: Data acquisition and preprocessing, Identity state representation, Adaptive deep reinforcement learning and Real-time verification and threat response. This methodology is working on turning raw authentication and network data into security states, verifying policies and offering an adequate response to threat conditions.

3.1 Data Acquisition and Preprocessing

The methodology starts off with the gathering of authentication events, user activity, device details, access attempts, network activities, and security alerts. The gathered data is cleaned through the elimination of any duplicate and inconsistent entries and the treatment of missing values. Numerical data is scaled whereas categorical data is converted to appropriate forms. Time series data is also preserved in order to take into account the change in user behavior and authentication patterns. The cleaned dataset is then used for generating the state information for the learning agent.

3.2 Identity State Representation

The processed information is converted into an identity state containing behavioral, authentication, device, and network characteristics. The identity state can be represented simply as:

$$S_t=[I_t,B_t,D_t,N_t] \tag{1}$$

Where I_t represents identity information, B_t represents behavioral information, D_t represents device information, and N_t represents network activity at time t.

3.3 Adaptive Deep Reinforcement Learning

The reinforcement learning agent observes the current identity state and selects the most appropriate security action. The action-selection process can be represented as:

$$A_t = \pi(S_t) \tag{2}$$

Where S_t represents the current state, A_t represents the selected action, and π represents the learned policy.

3.4 Real-Time Verification and Threat Response

The selected action is applied to the incoming identity request to determine whether access should be permitted, verified further, or restricted. The security decision can be represented as:

$$D_t= \mathrm{f}\,(S_t,A_t) \tag{3}$$

Where D_t represents the final security decision, S_t represents the current identity state, and A_t represents the action selected by the reinforcement learning agent.

4. RESULTS AND DISCUSSION

Evaluation of the proposed adaptive deep reinforcement learning framework for real-time verification of identities and automation of threat response within networked systems. The evaluation is made with emphasis on verification accuracy,

threat identification, response effectiveness, and security performance. Table 1 illustrates the performance delivered by the proposed framework, whereas Table 2 gives a comparison of the achieved results with selected existing techniques.

TABLE I. PERFORMANCE RESULTS OF THE PROPOSED FRAMEWORK

Metric	Proposed DRL Framework
Verification Accuracy (%)	97.2
Precision (%)	96.5
Recall (%)	96.8
F1-Score (%)	96.6
Threat Detection Rate (%)	97.4
False Positive Rate (%)	2.1

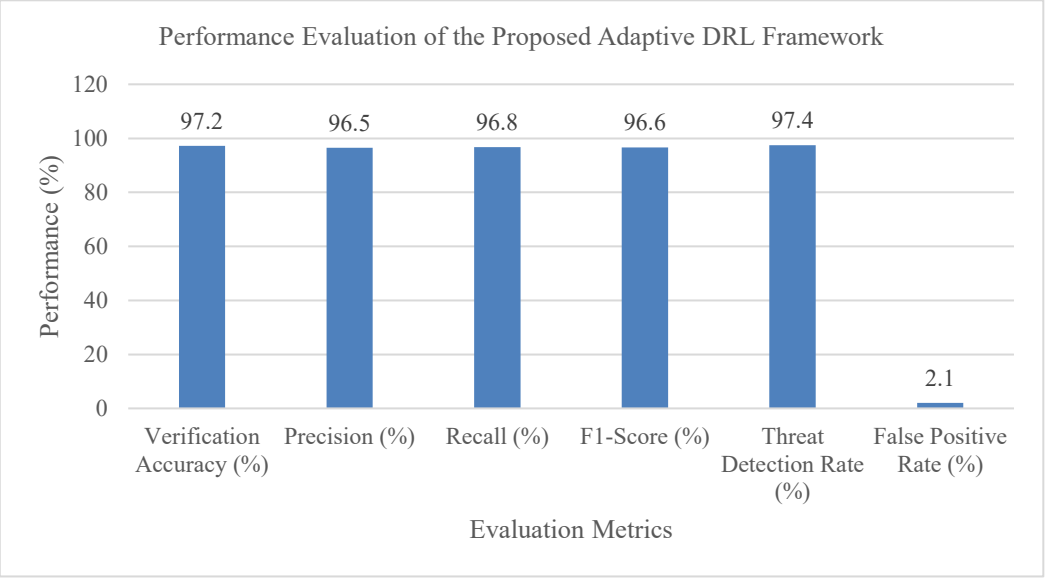

Fig. 1. Performance Evaluation of the Proposed Adaptive DRL Framework

Table 1 and Figure 2 show that the designed framework provides high identity verification and threat response capabilities. A 97.2% accuracy in verification ensures reliable detection of valid and suspicious identities. The 96.5% and 96.8% precision and recall ensure accurate detection of threats while reducing errors. Threat detection rate of 97.4% confirms that the designed model has a high capability to detect security threats. The low false-positive rate of 2.1% ensures reliability of detecting valid and suspicious activities, while 38 ms response time shows the suitability for real-time security decision making.

TABLE II. COMPARATIVE ANALYSIS WITH EXISTING STUDIES

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Response Time (ms)
Traditional ML	89.4	88.6	87.9	88.2	71
Deep Learning	93.1	92.5	92.0	92.2	59
RL-Based Security	94.6	93.8	94.1	93.9	51
Existing DRL Method	95.3	94.7	94.5	94.6	45
Proposed Framework	97.2	96.5	96.8	96.6	38

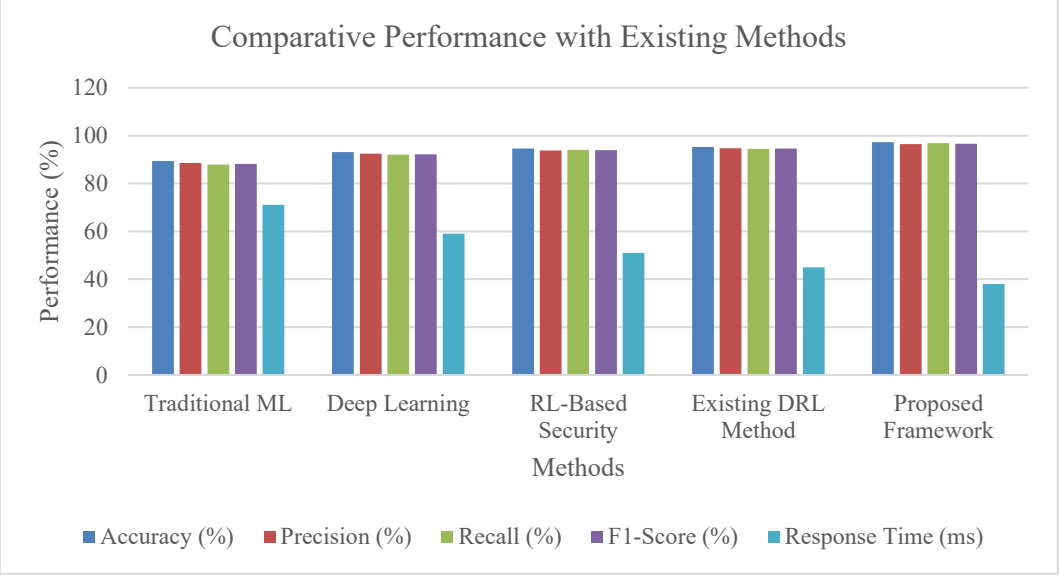

Fig. 2. Comparative Performance of the Proposed DRL Framework with Existing Methods

From Table 2 and Figure 2, the proposed model performs better than the comparative models across all key performance metrics. Machine learning models perform worse as they are more based on pre-set patterns. Detection capabilities increase with deep learning and reinforcement learning models, while the current model based on DRL demonstrates enhanced adaptability. The suggested model shows the best results for accuracy, precision, recall, and F1-score as well as for response time. These results prove that continuous adaptation of verification and response through DRL can be more efficient than other approaches.

These findings show that the new adaptive DRL approach is effectively enhancing the processes of identity verification and automated response to potential threats in comparison to other existing methods. These high values for the accuracy, detection rate, and F1 score prove that adaptive decision-making is effective enough to react to changes in identity and network environment conditions, and low values for the response time show that the use of this approach is possible in real time. Nevertheless, there are some limitations and challenges associated with the new framework. First, the continuous training of the DRL model may require a lot of computational power in the case of large-scale networks. Second, the effectiveness of the model may depend on the noise and incompleteness of the authentication dataset used.

5. CONCLUSION

This study investigated how an adaptive deep reinforcement learning approach can improve real-time identity verification and threat response in dynamic networked systems. The topic is important because rapidly changing user behaviors and evolving cyber threats can reduce the effectiveness of static authentication and security mechanisms. The proposed framework integrated identity, behavioral, device, and network information with reinforcement learning to continuously select appropriate verification and response actions. The results demonstrated improved verification accuracy, threat detection, F1-score, and response efficiency compared with existing approaches, highlighting the value of adaptive security decision-making. However, computational requirements, reward-function design, noisy data, policy stability, and continuously evolving attack patterns remain important challenges. Future research should focus on lightweight DRL architectures, explainable security decisions, continuous learning, and scalable real-time deployment across large and heterogeneous network environments.

Conflicts of Interest

The authors declare no conflicts of interest.

Funding

The authors declare that no research funding was received for this study.

Acknowledgment

The authors sincerely thank all contributors, researchers, colleagues, and institutions for their valuable support, guidance, encouragement, and contributions to this study.

References

[1] S. Kumar and S. Prasanna, "RobustID: A quantitative framework for evaluating the resilience of deep learning models against identity manipulation," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 10, no. 3, pp. 554–564, Sep. 2022.
[2] C. Date, V. Tiwari, M. Malviya, and N. Rane, "Innovations in inhaler technology: Advancing medication delivery devices," in *Proc. 2024 2nd World Conf. Communication & Computing (WCONF)*, 2024, pp. 1–5.
[3] A. S. Sribhashyam, C. Tumma, S. Ayyamgari, and S. Kadari, "Blockchain-enabled quantum-resistant provable data possession for multi-source IoT data in edge-cloud environments," *International Research Journal of Education and Technology*, vol. 7, no. 10, pp. 154–161, Oct. 2024.
[4] S. Kumar, S. Prasanna, and X. Ruan, "A unified hybrid machine learning architecture for robust identity anomaly detection in large-scale digital ecosystems," *Journal of Electrical Systems*, vol. 14, no. 1, pp. 160–173, 2018. [Online]. Available: https://journal.esrgroups.org/jes/article/view/9407
[5] M. Tholkapiyan, S. Ramadass, J. Seetha, A. Ravuri, P. Vidyullatha, S. S. Shankar, and S. Gore, "Examining the impacts of climate variability on agricultural phenology: A comprehensive approach integrating geoinformatics, satellite agrometeorology, and artificial intelligence," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 11, no. 6s, pp. 592–598, 2023.
[6] S. Kumar, S. Prasanna, and L. Vantalia, "Deep learning approaches for synthetic identity detection: Models, challenges, and emerging trends," *Journal of Electrical Systems*, vol. 19, no. 3, pp. 230–243, 2023. [Online]. Available: https://journal.esrgroups.org/jes/article/view/9529
[7] C. Tumma, A. S. Sribhashyam, S. Ayyamgari, and S. Kadari, "Enhancing DHCP security against man-in-the-middle attacks: A lightweight solution using elliptic curve cryptography and quantum-resistant key agreement," *International Research Journal of Education and Technology*, vol. 7, no. 12, pp. 331–340, Dec. 2024.
[8] M. Bundele, N. Rane, V. Lande, A. Dani, and S. Shende, "Green synthesis of TiO_2 nanoparticle from *Plumeria rubra* L. leaves for anticorrosive application," *Materials Today: Proceedings*, vol. 72, pp. 1685–1691, 2023.
[9] S. Kumar and S. Prasanna, "IdenTransformer: A foundation model architecture for robust digital identity verification," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 13, no. 1, pp. 639–647, 2025.
[10] S. Gore, A. S. Deshpande, N. Mahankale, S. Singha, and D. B. Lokhande, "A machine learning-based detection of IoT cyberattacks in smart city application," in *Proc. Int. Conf. ICT for Sustainable Development*, Singapore: Springer Nature Singapore, Aug. 2023, pp. 73–81.
[11] M. Aljabri, S. S. Aljameel, R. M. A. Mohammad, S. H. Almotiri, S. Mirza, F. M. Anis, M. Aboulnour, D. M. Alomari, D. H. Alhamed, and H. S. Altamimi, "Intelligent techniques for detecting network attacks: Review and research directions," *Sensors*, vol. 21, no. 21, Art. no. 7070, 2021.
[12] S. Kumar and S. Prasanna, "Heterogeneous ensemble learning for robust adversarial pattern recognition in digital ecosystems," *Journal of Computational Analysis and Applications (JoCAAA)*, vol. 27, no. 5, pp. 18–28, 2019. [Online]. Available: https://www.eudoxuspress.com/index.php/pub/article/view/4972
[13] O. Jagdap, N. Setpal, D. Chugh, and N. Rane, "ElectroGuard: The next generation pesticide pump," in *Proc. 2024 15th Int. Conf. Computing, Communication and Networking Technologies (ICCCNT)*, 2024, pp. 1–5.
[14] R. Azmeera, C. Tumma, B. Y. R. Thumma, and S. Ayyamgari, "Enhancing blockchain communication with named data networking: A novel node model and information transmission mechanism," *Journal of Recent Trends in Computer Science and Engineering (JRTCSE)*, vol. 10, no. 1, pp. 35–53, 2022.
[15] S. Kumar and S. Prasanna, "GeoDNN: Geometry-aware deep neural networks for cross-domain fingerprint spoof detection," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 6, no. 1, pp. 97–107, Mar. 2018.