Babylonian Journal of Networking
Vol.2026, **pp**. 38–42
DOI: https://doi.org/10.58496/BJN/2026/005; ISSN: 3006-5372
https://mesopotamian.press/journals/index.php/BJN

Research Article

A Hybrid Graph and Transformer-Based Framework for Relational Identity Anomaly Detection in Digital Interaction Networks

Cristina Borzan [1,*]

[1] *Technical University of Cluj-Napoca, Faculty of Industrial Engineering, Robotics and Management Production, Romania*.

ARTICLE INFO

Article History

Received 06 Jun 2026
Revised 18 Jul 2026
Accepted 05 Aug 2026
Published 31 Aug 2026

Keywords
Relational Identity Anomaly Detection,
Graph Neural Networks,
Transformer Networks,
Digital Interaction Networks,
Identity Security.

ABSTRACT

Digital interaction networks are increasingly connecting identities, devices, accounts, and services, creating complex environments in which anomalous identity behavior can emerge. This study addresses the problem of detecting relational identity anomalies that conventional feature-based methods and individual deep learning models may fail to recognize. The problem requires attention because sophisticated identity attacks often exploit interconnected relationships, coordinated interactions, and long-range behavioral dependencies rather than isolated attributes. This study develops a hybrid Graph and Transformer-based framework that combines graph neural networks for learning structural relationships with Transformer-based self-attention for modeling contextual and long-range interaction dependencies. The framework fuses these complementary representations and applies anomaly scoring to distinguish normal and suspicious identity behaviors. Experimental results show that the proposed framework achieves 96.8% accuracy, 95.9% precision, 96.2% recall, 96.0% F1-score, and 97.1% AUC. These results demonstrate that combining relational graph representations with contextual Transformer learning improves identity anomaly detection compared with conventional machine learning, standalone GNN, Transformer, and existing hybrid approaches. The findings extend previous research by showing that structural and contextual information can jointly provide more effective representations for detecting subtle and coordinated anomalies in complex digital interaction networks.

1. INTRODUCTION

Interaction networks based on digital interactions have become more complicated over time as people, devices, platforms, and digital services keep exchanging data and building dynamic interactions [1]. These interconnected networks pose challenges concerning the emergence of identity-related anomalies, such as impersonation, fraudster collaboration, synthetic identities, and unusual interactions [2]. The current identity anomaly detection approaches mostly use isolated features or machine learning techniques but fail to capture the relational and contextual properties of the digital interactions [3]. The graph learning approach can serve as an efficient method to detect anomalies in identity systems because it enables the representation of the interactions between entities as links and nodes, thus identifying the dependencies and anomalies in relationships [4]. However, graph models can have some difficulties with capturing long-term dependencies and contextual relationships in interactions [5].

For this purpose, the current research proposes an advanced framework of relational identity anomaly detection using hybrid graph-based and Transformer-based methods for digital interaction networks. The proposed framework uses a combination of graph-based representation learning along with Transformer-based contextual learning, both of which are designed to learn about the structural dependencies, interactions, and long-range relationships between different digital identities. In this way, graph learning will be used to extract topologically aware representations of interconnected entities, while at the same time the Transformer-based part of the model will learn about the contextual dependencies across sequential and relational interactions.

2. LITERATURE REVIEW

Studies of anomaly detection in the digital identity domain based on machine learning and deep learning have recently been conducted in abundance [6]. Traditional machine learning algorithms like support vector machines, decision trees, random forests, and ensemble classifiers have proven to be successful in identifying fraud cases through analysis of various transactional, behavioral, and demographic attributes [7]. Unfortunately, all of these studies usually consider identity records independently and are thus unable to capture the interactions between users, devices, identities, and different kinds of services

*Corresponding author. Email: cristinaborzan2026@outlook.com

[8]. On the other hand, deep learning algorithms have helped to enhance representation learning by extracting nonlinear and high-dimensional features, whereas autoencoders and other unsupervised techniques have been used for deviation from regular behavior in identity identification [9]. Nevertheless, most of these approaches still heavily rely on features and cannot effectively represent complex relational dependencies [10].

Learning on graphs has become a significant avenue toward overcoming these challenges since digital interactive systems lend themselves naturally to graphs [11]. Through Graph Neural Networks (GNNs), it is now possible to represent entities and their relationships via neighborhood aggregation, and thus detect anomalous nodes and edges using structural and contextual knowledge [12]. Graph attention mechanisms are making representation even better by weighing neighbors and their interactions differently [13]. Nevertheless, there might be problems when relationships span more than one hop or when interaction sequences have long-range dependencies [14]. The use of Transformer models has opened up a new solution avenue by making use of the self-attention mechanisms to model dependencies across long-distance sequences and heterogeneous behavior patterns [15]. The application of these models to identity and anomaly detection allows for the representation of rich contexts, but the use of Transformer-based models alone could fail to recognize the network topology and structural relationships explicitly. Recent research works have tried to overcome this limitation through hybrid models, which make use of graph-based learning along with attention-based models to make use of the benefits of both approaches. However, even today's literature faces limitations when it comes to scalability, dynamic interaction networks, heterogeneous identity relations, and coordinated anomalies.

3. METHODOLOGY

This research suggests a methodological approach that aims at the detection of relational identity anomalies using both graph-structured relations and long-distance contextual dependencies in complex networks of interactions in the digital space. Digital identities, devices, accounts, and interactions can be represented within this framework as interrelated entities that provide the means for studying both the structural and behavioral aspects of identities.

3.1 Data Collection and Graph Construction

Methodology: The methodology begins with the data collection for digital interactions, including identity features, authentication actions, transactions, device linkage, and interaction information. Data preprocessing involves handling of missing values, duplicates, categorical data, and normalization of numeric data. The processed data is then modeled into a heterogeneous interaction graph, wherein the nodes refer to identities, devices, accounts, or digital objects, whereas the edges refer to interactions and relationships.

3.2 Graph-Based Relational Representation Learning

Graph-based learning gradually learns the interrelationships between the connected digital entities. A Graph Neural Network (GNN) consolidates data from neighboring nodes to form relationship embeddings. Several graph layers help the network model learn both local and multi-hop dependencies in the digital interaction graph. The relationship embedding for each entity is generated through the consolidation of existing features of that entity along with the data from neighboring entities. The relationship embedding may be defined as:

$$h^{(l+1)}{}_u = \sigma\left(W^{(l)}\, h^{(l)}{}_u + \sum_{u \in N(u)} \alpha_{vu}\; W^{(l)}\, h^{(l)}{}_u \right) \quad (1)$$

Where, $h^{(l)}{}_u$ is the representation of node u at layer l, $N(u)$ represents its neighboring nodes α_{vu} denotes the attention weight between nodes v and u, $W^{(l)}$ represents the trainable transformation matrix, and σ is the nonlinear activation function . The graph attention technique places more emphasis on key connections, enabling the model to differentiate between normal connections and abnormal connections. This means that the embeddings generated by this technique capture the structural features of the digital identities and their associated interaction environment.

3.3 Transformer-Based Contextual Modeling

The graph-based representations are then fed into the Transformer encoder for modeling contextual dependencies. The multi-head self-attention mechanism learns the relationships between identity interactions in different positions and interaction sequences. Position-aware mechanisms are introduced in order to retain the sequence of events. This allows the system to capture long-term dependencies and behavioral patterns, which can be hidden from other graph neighborhoods.

3.4 Hybrid Fusion and Anomaly Detection

Finally, the fusion of graph representations and Transformer representations takes place via the feature-fusion module in order to obtain the enhanced identity representations. The latter are fed to the anomaly detection module, which determines an anomaly score for each identity or identity behavior. The decision threshold is dividing normal cases from abnormal

ones. The performance of the proposed framework is evaluated by means of accuracy, precision, recall, F1-score, AUC, false-positive rate, and computational efficiency.

4. RESULTS AND DISCUSSION

This hybrid framework using Graph and Transformer is examined to measure how effective this method is at detecting relational identity anomalies in digital interaction networks. This examination includes classification efficiency, anomaly detection ability, and model effectiveness in general. These results are shown in Table 1 below, whereas Table 2 is for comparative analysis.

TABLE I. PERFORMANCE RESULTS OF THE PROPOSED FRAMEWORK

Metric	Proposed Hybrid Graph-Transformer Framework
Accuracy (%)	96.8
Precision (%)	95.9
Recall (%)	96.2
F1-Score (%)	96.0
AUC (%)	97.1

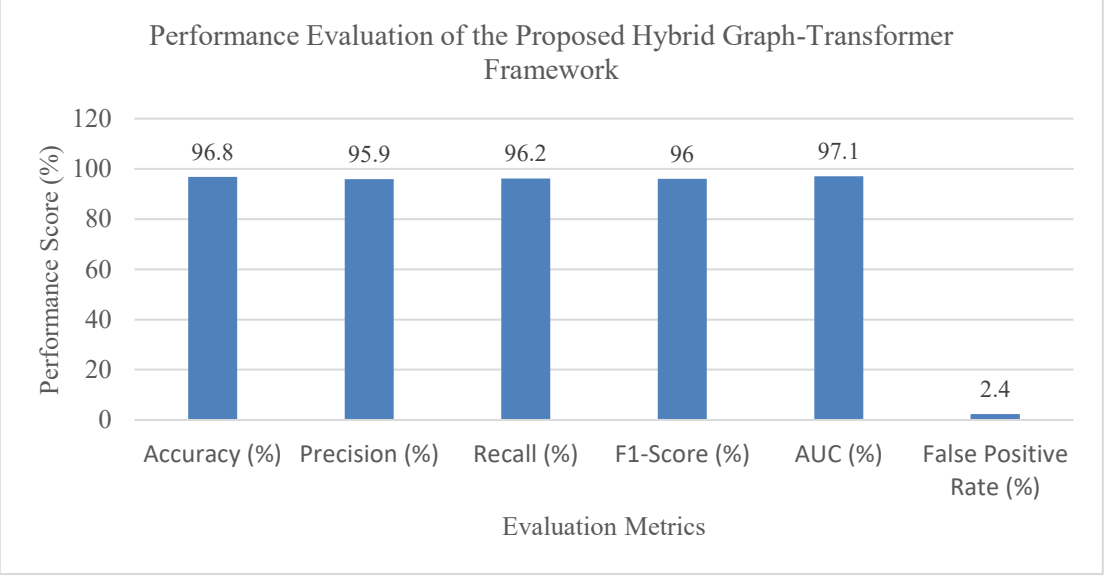

Fig. 1. Performance Evaluation of the Proposed Hybrid Graph-Transformer Framework

As shown in Table 1 and Figure 2, the suggested framework is demonstrating a very good level of anomaly detection capabilities for all measures considered during the evaluation process. The value of accuracy equal to 96.8% shows a high reliability of identity classification, whereas the precision and recall values of 95.9% and 96.2% respectively show a good ability to detect abnormal interaction patterns with a relatively small number of false detections. Additionally, the value of F1-score is 96.0% and shows a balance in detecting abnormal activity, and an AUC value of 97.1% also confirms this.

TABLE II. COMPARATIVE ANALYSIS WITH EXISTING STUDIES

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Traditional Machine Learning	88.7	87.9	86.8	87.3
GNN-Based Method	92.5	91.8	91.2	91.5
Transformer-Based Method	94.1	93.2	92.8	93.0
Existing Hybrid Method	95.2	94.3	94.0	94.1
Proposed Framework	96.8	95.9	96.2	96.0

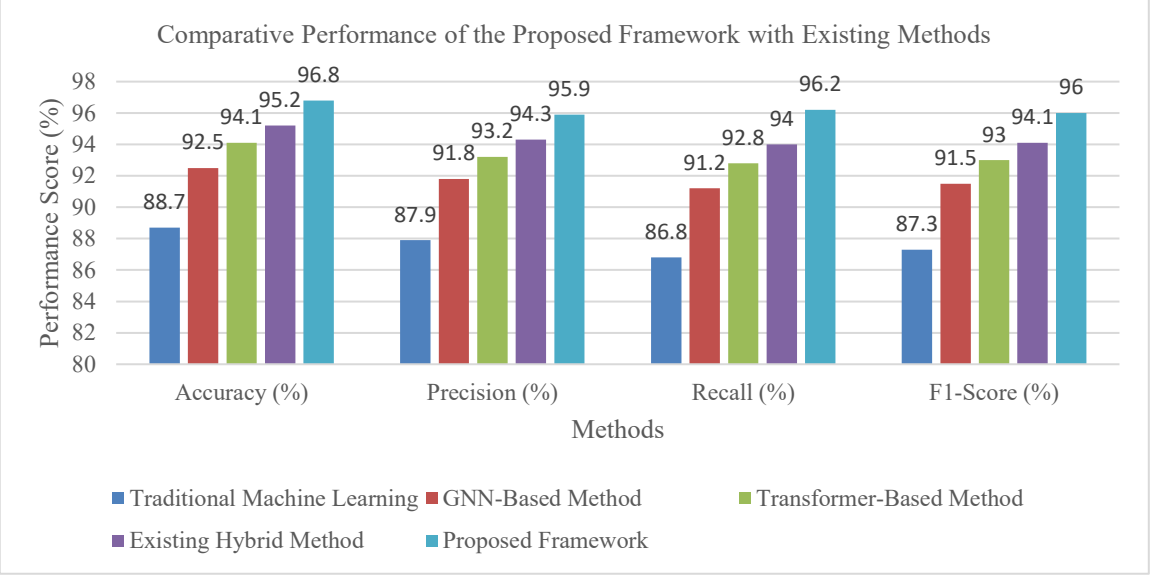

Fig. 2. Comparative Performance of the Proposed Framework with Existing Methods

Table 2 and Figure 3 illustrate the comparison between the proposed framework and some representative existing methodologies. The accuracy, precision, recall, and F1-score results show that the proposed framework achieves the best performance among all the compared methodologies. The improvement from traditional machine learning shows the advantage of deep relational representation learning. The proposed framework also performs better than both the GNN model and Transformer due to its use of structural and contextual information. Moreover, the improvement from the existing hybrid model indicates the effectiveness of joint modeling of graph relations and long-range interaction dependencies.

These results confirm that the suggested hybrid Graph-Transformer architecture is able to model structural dependencies as well as long-distance context dependencies in terms of detecting relational identity anomalies. The enhanced performance relative to other methods reveals the effectiveness of integrating two approaches with their complementary abilities of representing data. Nevertheless, there are numerous limitations and problems with the suggested approach. First, the use of this architecture may require significant computing power in terms of processing huge and constantly growing interaction networks. Second, the performance of this architecture can be impacted by incomplete or imbalanced identity data. Finally, setting up thresholds and maintaining consistent model performance can be difficult with changing behavioral patterns.

5. CONCLUSION

This study is investigating how relational and contextual information can be jointly exploited to improve identity anomaly detection in complex digital interaction networks. The topic is important because increasingly interconnected digital environments are creating sophisticated identity threats that cannot be reliably detected by analyzing isolated identity attributes alone. The proposed hybrid Graph and Transformer-based framework combines graph-based relational representation learning with Transformer-based contextual modeling to capture structural dependencies, interaction patterns, and long-range relationships. The experimental results demonstrate strong detection performance and improved effectiveness compared with existing approaches, highlighting the value of integrating complementary deep learning techniques. Nevertheless, scalability, noisy and incomplete data, dynamic network structures, and computational requirements remain important challenges. Future research should therefore focus on real-time detection, adaptive graph learning, explainable anomaly identification, and efficient deployment across large-scale evolving digital identity networks.

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 Sanjeev Prasanna, "DeepSynth: A robust multi-layer neural detection of coordinated latent anomalies in high-dimensional identity systems," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 7, no. 1, pp. 66–77, 2019. [Online]. Available: https://ijisae.org/index.php/IJISAE/article/view/8101

[2] S. P. Shewale, S. R. Samdani, N. M. Rane, and M. D. Deshpande, "An overview on carbon nanotubes."

[3] S. Kumar, S. Prasanna, and X. Ruan, "A unified hybrid machine learning architecture for robust identity anomaly detection in large-scale digital ecosystems," *J. Electr. Syst.*, vol. 14, no. 1, pp. 160–173, 2018. [Online]. Available: https://journal.esrgroups.org/jes/article/view/9407

[4] 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.

[5] H. E. Khodke, M. Bhalerao, S. N. Gunjal, S. Nirmal, S. Gore, and B. J. Dange, "An intelligent approach to empowering the research of biomedical machine learning in medical data analysis using PALM," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 11, no. 10s, pp. 429–436, 2023.

[6] S. Kumar, S. Prasanna, and X. Ruan, "A unified hybrid machine learning architecture for robust identity anomaly detection in large-scale digital ecosystems," *J. Electr. Syst.*, vol. 14, no. 1, pp. 160–173, 2018. [Online]. Available: https://journal.esrgroups.org/jes/article/view/9407

[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] S. Gore, D. D. Jadhav, M. E. Ingale, S. Gore, and U. Nanavare, "Leveraging BERT for next-generation spoken language understanding with joint intent classification and slot filling," in *Proc. 2023 Int. Conf. Advanced Computing Technologies and Applications (ICACTA)*, Mumbai, India, 2023, pp. 1–5, doi: 10.1109/ICACTA58201.2023.10393437.

[9] D. Kumar, P. P. Pawar, M. K. Meesala, P. K. Pareek, S. R. Addula, and S. KS, "Trustworthy IoT infrastructures: Privacy-preserving federated learning with efficient secure aggregation for cybersecurity," in *Proc. 2024 Int. Conf. Integrated Intelligence and Communication Systems (ICIICS)*, 2024, pp. 1–8.

[10] S. Kumar Sanjeev Prasanna and S. Pandya, "EvoAnom: Longitudinal temporal deep learning for evolutionary anomaly detection in digital identities," *Journal of Computational Analysis and Applications (JoCAAA)*, vol. 30, no. 2, pp. 1142–1153, Feb. 2022.

[11] N. M. Rane, S. V. Admane, S. P. Shewale, and R. S. Sapkal, "Parametric optimization and comparative study for removal of Cr (VI) from aqueous solution using lemon, sweetlime and orange peel powder by batch adsorption," in *Proc. Ninth DAE-BRNS Biennial Symp. Emerging Trends in Separation Science and Technology*, 2021, p. 56.

[12] S. Kumar, S. Prasanna, and L. Vantalia, "Deep learning approaches for synthetic identity detection: Models, challenges, and emerging trends," *J. Electr. Syst.*, vol. 19, no. 3, pp. 230–243, 2023. [Online]. Available: https://journal.esrgroups.org/jes/article/view/9529

[13] N. M. Rane, S. P. Shewale, S. V. Admane, and R. S. Sapkal, "Adsorption of hexavalent chromium by using sweet lime and orange peel powder," in *Novel Water Treatment and Separation Methods: Simulation of Chemical Processes*, Taylor & Francis Group, 2017, p. 14.

[14] S. Kumar Sanjeev 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

[15] P. P. Pawar, D. Kumar, M. K. Meesala, P. K. Pareek, S. R. Addula, and S. K. S, "Securing digital governance: A deep learning and blockchain framework for malware detection in IoT networks," in *Proc. 2024 Int. Conf. Integrated Intelligence and Communication Systems (ICIICS)*, Kalaburagi, India, 2024, pp. 1–8, doi: 10.1109/ICIICS63763.2024.10860155.