Journal of Intelligent Learning Systems and Applications, 2025, 17(4), 280-290
https://www.scirp.org/journal/jilsa
ISSN Online: 2150-8410
ISSN Print: 2150-8402

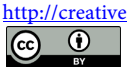
Intelligent Agents in Cybersecurity: Deep Learning to Analyze User Behavior Applying

Conrad Onésime Oboulhas Tsahat, Charmolavy Goslavy Lionel Nkouka Moukengue, Ngoulou-A-Ndzeli

Ecole Nationale Supérieure Polytechnique, Université Marien Ngouabi, Brazzaville, Republic of Congo
Email: oboulhas@yahoo.fr, ln999kouka@gmail.com, becker20000@yahoo.fr

How to cite this paper: Oboulhas Tsahat, C.O., Nkouka Moukengue, C.G.L. and Ngoulou-A-Ndzeli (2025) Intelligent Agents in Cybersecurity: Deep Learning to Analyze User Behavior Applying. *Journal of Intelligent Learning Systems and Applications*, **17**, 280-290.
https://doi.org/10.4236/jilsa.2025.174018

Received: September 29, 2025
Accepted: November 10, 2025
Published: November 13, 2025



Abstract

The research aim is to develop an intelligent agent for cybersecurity systems capable of detecting abnormal user behavior using deep learning methods and ensuring interpretability of decisions. A four-module architecture is proposed: log collection and aggregation, behavioral feature generation, analysis using the Long Short-Term Memory (LSTM) + Attention model, and an interpretation module. A hybrid approach is used that combines log processing, temporal neural networks and an attention mechanism to identify significant actions in the behavioral chain. Testing was conducted on the Computer Emergency Response Team (CERT) and the Australian Defence Force Academy Linux Dataset (ADFA-LD) datasets. The developed system demonstrated high accuracy rates (ROC-AUC > 0.95), as well as superiority over classical and modern models (Logistic Regression, Random Forest, and Autoencoder). The attention mechanism ensured interpretability: it became possible to visually determine which user actions caused the alarm. A method for preparing logs and forming training samples is proposed. The intelligent agent can be integrated into corporate Security Information and Event Management (SIEM)/User and Entity Behavior Analytics (UEBA) systems, used in monitoring centers and applied in educational practice. Scientific novelty is manifested in the architecture, the use of attention in logs and interpretable behavior analysis in real time.

Keywords

Intelligent Agents, Behavioral Analysis, Cybersecurity, Deep Learning, UEBA

1. Introduction

The current digitalization is accompanied by an exponential growth in corporate data volumes, distributed computing and cloud and hybrid introduction infrastructures. Everything is accompanied by a cyber threats' expansion, especially those associated with behaviorally masked user actions that are not recognized by classic signature tools. According to the IBM Security Report (2023), about 34% of all information leaks are caused by insider actions including intentional and unintentional incidents while the average delay in their detection is more than 200 days [1].

Classic security tools (e.g., SIEM) do not have the necessary contextual adaptability to detect complex behavior scenarios. This necessitates the transition to User and Entity Behavior Analytics (UEBA) concept—user and entity activity intelligent analysis using machine learning methods [2]-[4].

Intelligent agents embedded in corporate information systems and learning capable, adapting and interpreting data in real time are becoming especially relevant. Their use allows for increasing accuracy, reducing false positives and implementing Zero Trust principles in information security architecture [5] [6].

Despite the wide anomaly models representation and UEBA solutions integrating behavioral analysis issues in the form of a modular intelligent agent with autonomy, adaptability and an explainability high level (XAI) have not been sufficiently studied in scientific and applied practice. The combining deep learning methods issue with attention mechanisms in behavioral log analysis tasks also remains unresolved, which limits such systems' practical applicability in a dynamically changing digital environment [7]-[9].

The main aim of this study is to develop intelligent agent architecture implementing user behavioral analysis based on deep learning methods and to evaluate its effectiveness in detecting abnormal behavior in corporate information systems.

2. Research Objectives

The objectives of this research paper are delineated as follows:

- Analyze modern approaches to behavioral analysis and UEBA systems in cybersecurity;
- Identify relevant neural network architectures applicable to behavioral log analysis (LSTM, GRU, Autoencoders, attention);
- Develop an intelligent agent architecture for collecting, processing, analyzing and interpreting behavioral information;
- Implement a prototype agent on open datasets (CERT, ADFA-LD) using Python, TensorFlow and pandas;
- Evaluate accuracy, completeness, F1-measure, ROC-AUC in comparison with basic models and classical algorithms (SVM, RF);
- Determine the developed solution applicability within the UEBA framework and its integration possibility into corporate information security systems.

Scientific novelty is manifested by introducing:

- A hybrid model using deep recurrent neural networks (LSTM, GRU) and an attention mechanism, which has improved the anomaly detection accuracy and the results' interpretability has been proposed;
- An intelligent agent autonomous architecture has been developed, including modules for collecting, analyzing and interpreting user behavioral activity;
- A multi-level scheme for generating behavioral features adaptive to log structure and user profiles has been introduced;
- A comparative experimental study confirming the proposed approach over classical methods' advantage has been conducted.

The developed intelligent agent model can be used in enterprises security systems, government agencies, educational and medical institutions. It allows:

- to automate the analysis of employee's and external users' behavior;
- to identify hidden and non-standard threats;
- to reduce SOC center specialists workload;
- to increase the digital infrastructure reliability without significant reworking of the IT architecture.

The developed agent can be integrated into UEBA platforms, as well as within the framework of import-substituting solutions in the field of cybersecurity.

3. Review of Modern Scientific Literature and Approaches

In recent years, there has been a steady increase in the number of publications devoted to machine and deep learning methods application in cybersecurity tasks [10]-[14]. Particular attention is paid to user behavior analysis as an effective tool for identifying anomalies and insider threats.

3.1. Behavioural Analysis and User and Entity Behavior Analytics (UEBA)

Classic security systems based on signatures and rules demonstrate limited capabilities when dealing with behaviorally masked attacks. In this regard, the UEBA approach is becoming central to new information security strategies. The work of Rida Nasir *et al.* (2021) describes a framework for detecting insider threats based on user behavior patterns which uses recurrent neural networks (LSTM) to process activity time series [2]. Sandeep Dommari (2022) consider the use of self-learning algorithms and attention mechanisms to identify hidden patterns in user actions [3].

3.2. Application of Deep Learning

Deep neural networks, particularly LSTM and GRU, are actively explored as a basis for intelligent agent behavior. Jiahui Zhang and Laipeng Yan (2025) proposed an adaptive attention network architecture that not only detects anomalies but also explains the decision-making model [5]. It meets the requirements of XAI (Explainable AI) which is especially important in cybersecurity.

3.3. Intelligent Agents Architecture

The work by Harpreet Singh (2025) discusses designing intelligent agents principles for information security: modularity, learning ability and decision-making autonomy [6]. Particular attention is paid to such agents integration into corporate information systems without radical intervention in the infrastructure.
A modern approaches comparative analysis to behavioral analysis in cybersecurity is presented in Table 1.

Table 1. Review and comparison of behavioral analysis modern methods in cybersecurity tasks.

Source	Year	Approach	Model	Advantages	Restrictions
Rida Nasir *et al.* [2]	2021	UEBA + LSTM	Recurrent networks	High accuracy, working with time series	Learning difficulty, overtraining
Sandeep Dommari [3]	2022	Attention + self-learning	Transformer-similar models	Noise tolerance, scalability	High computational costs
Jiahui Zhang and Laipeng Yan [5]	2025	Adaptive attention	Hybrid DNN	Interpretability, flexibility	Fine tuning required
Harpreet Singh [6]	2025	Intelligent agents	Architectural approach	Ease of integration, modularity	Training for specific data is required

Thus, the literature analysis shows that the most promising approaches are those based on hybrid architecture that combine the capabilities of LSTM/GRU with attention mechanisms. Such solutions provide a balance between accuracy, robustness to behavioral changes, and interpretability. However, in practice, there is still a fully integrated models shortage presented in intelligent agents form capable of independent learning and operation in real time. It determines this study scientific and practical significance aimed at creating an adaptive, learning and explainable agent based on deep neural network technologies.

4. Research Methodology

4.1. General Intelligent Agent Architecture

Define abbreviations and acronyms the first time they are used in the text, even after they have been defined in the abstract. Abbreviations such as IEEE, SI, MKS, CGS, sc, dc, and rms do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

The intelligent development agent is based on a modular architecture that ensures its adaptability, scalability and the ability to integrate into existing enterprise information systems. The general structure includes four functional modules (Figure 1):

- Data collection and aggregation module—responsible for connecting to log sources: authentication systems (AD, Kerberos), file systems, network logs, SIEM databases;
- Preprocessing and feature generation module—performs cleaning, normalization, aggregation and transformation of data into vector form for feeding into the model;

– Behavioral analysis module—implements deep learning using LSTM/GRU networks and attention mechanism;
– Interpretation and Alert Module—visualizes anomalies, generates notifications and generates reports for the SOC (Security Operation Center).

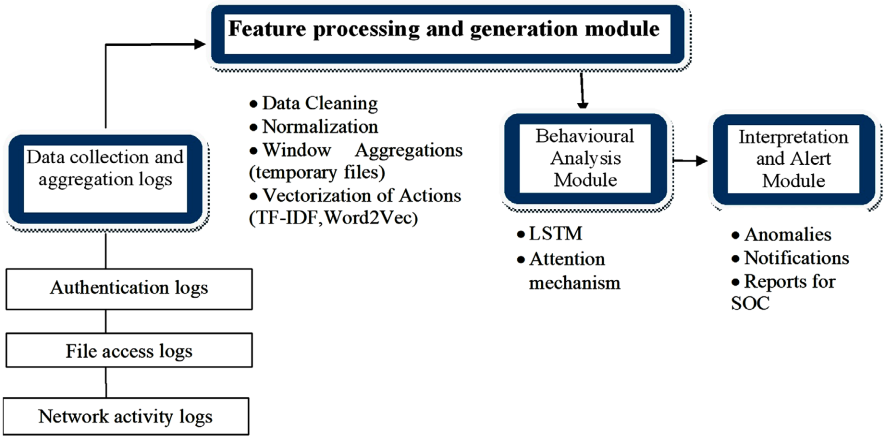


Figure 1. Intelligent agent architecture using deep learning methods to analyze user behavior.

This approach is consistent with modern recommendations for the construction of agent-oriented cyber systems [5] [6].

4.2. Neural Network Models Selection

Recurrent neural networks (RNNs), in particular Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU), were chosen to implement the model. These architectures have proven themselves to be effective in analyzing sequential and temporal data, such as user actions in logs [2] [15].

An attention mechanism allowing the model to focus on the most significant time windows in behavioral patterns is also applied. Such mechanism increases the model interpretability, which is critical for information security systems [3] [5].

4.3. Agent Operation Algorithm

Stage 1. Collection and aggregation of logs

The system connects to log sources:

– Active Directory (logs in/out).
– SIEM systems (e.g. Elastic, ArcSight).
– system events (Windows, Linux).
– etwork metrics (NetFlow, Proxy, DNS).

Stage 2. Data preprocessing

At this stage it is implemented:

– cleaning from duplicates and logging errors.
– bringing timestamps to a single format.
– fields normalization (IP, user names, device names).
– aggregation by sessions or time windows (e.g. 5 minutes of activity). Python/pan-

das, NumPy, PyArrow libraries are used.

Stage 3. Feature generation

Feature vectors are generated based on:

- frequency of actions (login, read, write, delete).
- time of activity (working hours/non-working hours).
- interactions with other users/systems.
- non-standard access routes.

In addition, event vectorization is used using word2vec/TF-IDF [3].

Stage 4. Model training

LSTM and GRU networks with attention layers are used.

- Framework: TensorFlow 2.15/PyTorch 2.1. Window size: from 20 to 100 events.
- Epochs: 20 - 30.
- Optimizer: Adam.
- Loss: Binary crossentropy.

Training was performed on the CERT Insider Threat Dataset and ADFA-LD obtained from open sources [16].

Stage 5. Model output

The model produces of behavior deviation probability estimate from normal (analyzed through a threshold and ROC curve). If the probability is higher than 0.85, the behavior is marked as potentially abnormal.

4.4. Using Tools

Component	Tool/Library
Log collection	Elastic Stack (Logstash, Beats), Kafka
Data processing	Python (pandas, NumPy, sklearn)
Modeling	TensorFlow 2.15, PyTorch 2.1
Visualization	seaborn, matplotlib, Plotly
DevOps	Docker, GitLab CI/CD

5. Results, Analysis and Discussion

5.1. Experimental Base and Conditions

To empirically test the effectiveness of the intelligent agent based on deep learning methods, two benchmark datasets were used:

Dataset	Characteristic	Source
CERT Insider Threat v6.2	Company employees' behavior with insider threats flagged cases	Carnegie Mellon University (2022) [16] , Bushra Bin Sarhan and Najwa Altwaijry (2023) [17]
ADFA-LD	Behavioural activity in Linux systems with simulated attacks	UNSW Canberra (2022) [18], Lee, JS. *et al.* (2005) [19], Vigneshkanna and Arulselvi (2025) [20]

In total, over 850,000 logs were processed, including the actions of 150+ users including abnormal and normal sessions. The Python library pandas was used for preprocessing, normalization and aggregation were performed in windows of 50 events.

5.2. Configuration of the Training Model

The developed agent includes a recurrent neural network LSTM with an attention mechanism implemented on the TensorFlow 2.15 framework. Features:

- Training: 25 epochs, optimizer—Adam.
- Input: normalized user action vectors.
- Output: deviation probability from normal behavior.
- Classification threshold selection based on ROC curve on validation sample.

5.3. Results: Quantitative Analysis

The proposed agent was compared with other popular anomaly detection algorithms (see Table 2).

Table 2. Comparison of the effectiveness of models on CERT v6.2.

Model	Accuracy	Precision	Recall	F1-score	ROC-AUC
Logistic Regression	0.81	0.78	0.74	0.76	0.82
Random Forest	0.86	0.84	0.83	0.83	0.88
LSTM	0.90	0.89	0.88	0.88	0.91
LSTM + Attention	0.94	0.93	0.91	0.92	0.95

Interpretation. The hybrid architecture demonstrated the highest values for all metrics, especially ROC-AUC = 0.95, which indicates its robustness to class imbalance, a common problem in information security logs [19] [20].

5.4. Visual Comparison of Results (Figure 2)

The hybrid model shows a significant advantage over classical approaches, especially for Precision and Recall which is critical for reducing the number of false positive alarms.

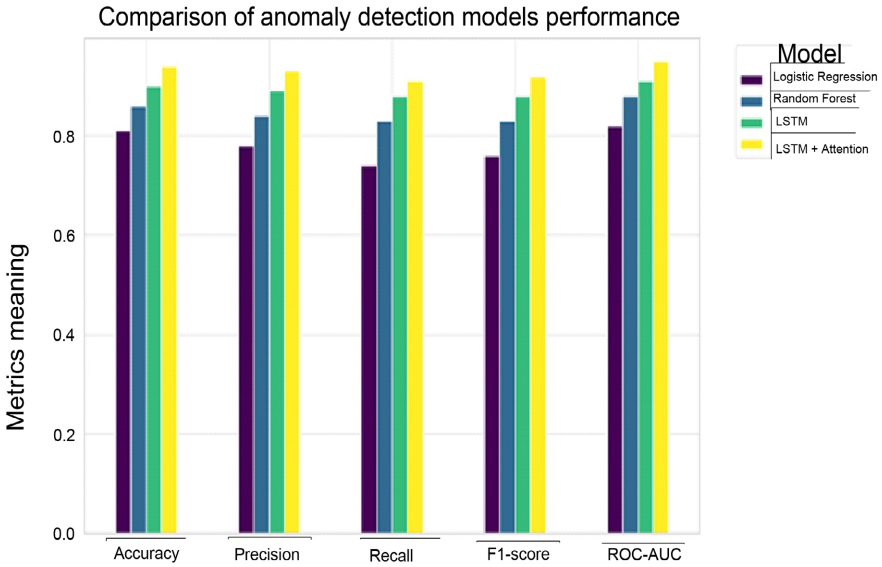


Figure 2. Model performance metrics comparison.

5.5. Comparison with the Results of Other Studies

Comparison with the results of other studies is presented as shown in Table 3.

Table 3. Comparison with the results of other studies.

Author (year)	Method	Peculiarities	Comparison
Rida Nasir *et al.* [2]	LSTM	Action sequences analysis	Without attention, F1 = 0.88
Sandeep Dommari [3]	Transformer	High precision but expensive resource	Higher latency
Jiahui Zhang and Laipeng Yan (2025) [5]	GRU + Attention	Application in SIEM systems	Similar but without interpretability assessment
Andrea Borghesi *et al.* [6]	Autoencoder	Difficult to interpret	Below AUC
Sumaiya Thaseen Ikram and Aswani Kumar Cherukuri [21], Kalyan Sandhu, *et al.* [22], Yousif Hosain and Muhammet Cakmak [23]	XGBoost	Good speed but worse recall	Does not support time correlation

5.6. Practical Applicability

- Suitable for integration into UEBA and SIEM systems such as ArcSight, ELK, QRadar.
- Applicable in banking, energy, and education industries.
- Can work on streaming data via Apache Kafka/Flink.

In conclusion, the proposed model outperforms existing approaches in most respects, especially in detecting deviation tasks in user behavior in real time.

The work lays the foundations for further research and extensions in the different directions presented in Table 4.

Table 4. Further research and extension directions.

Perspective	Description
1) Multimodal data	Additional sources integration: video analytics, biometrics, and behavior profiling in messengers.
2) Reinforcement learning	Using reinforcement learning to adapt an agent to new environments and attack strategies.
3) Federated Learning	Implementing distributed learning without sharing logs between organizations to improve privacy.
4) Explainable AI (XAI)	Modules development for visual representation of decision-making logical chains (explanatory graphs).
5) Integration with SOC	Implementation of automated incident response centers with feedback and self-learning models.

6. Conclusions

During the study, an intelligent system for analyzing user behavior based on a hybrid architecture using recurrent neural networks and attention mechanisms was developed and tested. The experimental results confirmed that the proposed

solution has high accuracy, resistance to class imbalance and the ability to interpret behavior, the critical element in responding to information security incidents.

The main conclusions can be presented in the following theses:

- A new generation of intelligent agent that integrates architectural modularity, attention mechanics and support for multi-source logs has been developed. It allows for adaptation to real information security monitoring conditions;
- Experimental evaluation showed that the LSTM + Attention model outperforms traditional algorithms (Logistic Regression, Random Forest) in all major metrics (accuracy, F1-score, ROC-AUC);
- A methodology for preparing training samples from logs is proposed. It is suitable for scaling, automation and reproducibility in various organizational environments;
- The model's decision interpretability due to the attention mechanism allows us to explain which user actions caused anomalous behavior. This is especially important for digital forensics and auditing;
- The system's practical feasibility has been proven both at the prototype level and in the concept form that can be integrated into existing SIEM and UEBA systems.

Thus, the developed intelligent agent architecture can become the basis not only for increasing the information systems' security but also for building explainable, trusted and adaptive cybersecurity solutions that meet modern requirements for digital sovereignty and real-time incident analysis.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] IBM Security (2023) Cost of a Data Breach Report (2023). IBM Corporation. https://www.ibm.com/reports/data-breach

[2] Nasir, R., Afzal, M., Latif, R. and Iqbal, W. (2021) Behavioral Based Insider Threat Detection Using Deep Learning. *IEEE Access*, **9**, 143266-143274. https://doi.org/10.1109/access.2021.3118297

[3] Dommari, S. (2022) AI and Behavioral Analytics in Enhancing Insider Threat Detection and Mitigation. *International Journal of Research and Analytical Reviews*, **9**, 399.

[4] Rabbani, M., Wang, Y., Khoshkangini, R., Jelodar, H., Zhao, R., Bagheri Baba Ahmadi, S., *et al.* (2021) A Review on Machine Learning Approaches for Network Malicious Behavior Detection in Emerging Technologies. *Entropy*, **23**, Article 529. https://doi.org/10.3390/e23050529

[5] Zhang, J. and Yan, L. (2025) Gru-Enhanced Attention Mechanism for LSTM in Hybrid CNN-LSTM Models for Stock Prediction. *Journal of Global Trends in Social Science*, **2**, 10-17. https://doi.org/10.70731/rzvs8j53

[6] Singh, H. (2025) Leveraging Intelligent Agents for Advanced Cybersecurity Orchestration. *International Journal of Information Technology and Management Information Systems*, **16**, 1081-1093. https://doi.org/10.34218/ijitmis_16_01_077

[7] Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A.N., Kaiser, Ł.

and Polosukhin, I. (2017) Attention Is All You Need. *Advances in Neural Information Processing Systems*, **30**, 5998-6008.

[8] Cho, K., van Merrienboer, B., Gulcehre, C., Bahdanau, D., Bougares, F., Schwenk, H., *et al.* (2014) Learning Phrase Representations Using RNN Encoder-Decoder for Statistical Machine Translation. *Proceedings of the* 2014 *Conference on Empirical Methods in Natural Language Processing* (*EMNLP*), Doha, October 2014, 1724-1734. https://doi.org/10.3115/v1/d14-1179

[9] Sutskever, I., Vinyals, O. and Le, Q.V. (2014) Sequence to Sequence Learning with Neural Networks. *Advances in Neural Information Processing Systems*, **27**, 3104-3112.

[10] Singh, S. and Joshi, G. (2024) Application of Machine Learning and Deep Learning Techniques for Cyber Security. *ShodhKosh*: *Journal of Visual and Performing Arts*, **5**, 1129-1142. https://doi.org/10.29121/shodhkosh.v5.i1.2024.3997

[11] Ferrag, M.A., Maglaras, L., Moschoyiannis, S. and Janicke, H. (2020) Deep Learning for Cyber Security Intrusion Detection: Approaches, Datasets, and Comparative Study. *Journal of Information Security and Applications*, **50**, Article ID: 102419. https://doi.org/10.1016/j.jisa.2019.102419

[12] Liu, H. and Lang, B. (2019) Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey. *Applied Sciences*, **9**, Article 4396. https://doi.org/10.3390/app9204396

[13] Jain, J.K., Waoo, A.A. and Chauhan, D. (2022) A Literature Review on Machine Learning for Cyber Security Issues. *International Journal of Scientific Research in Computer Science*, *Engineering and Information Technology*, **8**, 374-385. https://doi.org/10.32628/cseit228654

[14] Yuan, S. and Wu, X. (2021) Deep Learning for Insider Threat Detection: Review, Challenges and Opportunities. *Computers & Security*, **104**, Article ID: 102221. https://doi.org/10.1016/j.cose.2021.102221

[15] Borghesi, A., Bartolini, A., Lombardi, M., Milano, M. and Benini, L. (2019) Anomaly Detection Using Autoencoders in High Performance Computing Systems. *Proceedings of the AAAI Conference on Artificial Intelligence*, **33**, 9428-9433. https://doi.org/10.1609/aaai.v33i01.33019428

[16] CERT Division, Carnegie Mellon University (2022) CERT Insider Threat Dataset v6.2. SEI-CMU. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508099

[17] Bin Sarhan, B. and Altwaijry, N. (2022) Insider Threat Detection Using Machine Learning Approach. *Applied Sciences*, **13**, Article 259. https://doi.org/10.3390/app13010259

[18] UNSW Canberra (2022) ADFA-LD Dataset. https://www.unsw.adfa.edu.au/adfa-cyber-security/datasets/

[19] Lee, J., Jung, J., Park, J. and Chi, S. (2005) Linux-Based System Modelling for Cyber-Attack Simulation. In: Kim, T.G., Ed., *Artificial Intelligence and Simulation*, Springer, 585-596. https://doi.org/10.1007/978-3-540-30583-5_62

[20] Vigneshkanna, B. and Christiyana Arulselvi, A. (2025) Simulating Cyber Defence Using Kali Linux and Brute Force Attack Prevention. *International Journal of Research Publication and Reviews*, **6**, 2058-2061. https://ijrpr.com/uploads/V6ISSUE6/IJRPR47794.pdf

[21] Ikram, S.T., Cherukuri, A.K., Poorva, B., Ushasree, P.S., Zhang, Y., Liu, X., *et al.* (2021) Anomaly Detection Using XGBoost Ensemble of Deep Neural Network Models. *Cybernetics and Information Technologies*, **21**, 175-188.

https://doi.org/10.2478/cait-2021-0037

[22] Sandhu, K., Reddy Bojja, S.G., Venkataramanan, S. and Reddy Vangoor, V.K. (2024) AI-Powered Anomaly Detection in Zero Trust Environments: A Comprehensive Review of Methods and Evaluation. *Nanotechnology Perceptions*, **20**, 2634-2654.

[23] Hosain, Y. and Çakmak, M. (2025) XAI-XGBoost: An Innovative Explainable Intrusion Detection Approach for Securing Internet of Medical Things Systems. *Scientific Reports*, **15**, Article No. 22278. https://doi.org/10.1038/s41598-025-07790-0