HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

HYBRID ARTIFICIAL INTELLIGENCE MODEL FOR NETWORK ANOMALY DETECTION IN UZBEKISTAN'S DIGITAL ECONOMY: AN INTEGRATION ANALYSIS OF LSTM, RANDOM FOREST, AND AUTOENCODER

Salimov Nurali Ramazon ugli
PhD student, Department of Digital Technologies and Artificial Intelligence, Tashkent State University of Economics (State Institution)
doi:https://doi.org/10.5281/zenodo.22784932

Abstract. The rapid development of digital technologies has significantly increased the dependence of Uzbekistan's economy on networked information systems, cloud services, electronic government platforms, digital banking, telecommunications, and online commercial services. At the same time, the expansion of digital infrastructure has increased the potential exposure to network anomalies and cyberattacks. This study proposes a hybrid artificial intelligence model for network anomaly detection that integrates Long Short-Term Memory (LSTM), Random Forest (RF), and Autoencoder (AE) algorithms. The proposed architecture combines the temporal pattern recognition capability of LSTM, the classification and feature-importance capabilities of Random Forest, and the unsupervised anomaly detection capability of Autoencoder. The main objective is to develop a multidimensional detection framework capable of identifying both known and previously unseen abnormal network behavior. The proposed methodology includes data collection, preprocessing, feature engineering, Autoencoder-based representation learning, LSTM-based temporal analysis, Random Forest classification, and hybrid risk-score calculation. The model is particularly relevant to Uzbekistan because cybercrime and technology-enabled offenses have increased substantially alongside digital transformation. Official Uzbek government information indicates that 58,800 technology-related crimes across 62 categories were registered in 2024, compared with 863 crimes across 18 categories in 2019. The proposed hybrid approach provides a conceptual foundation for developing adaptive, scalable, and proactive network security systems for Uzbekistan's banking, telecommunications, e-government, and corporate digital infrastructure.

Keywords: artificial intelligence, cybersecurity, network anomaly detection, Long Short-Term Memory, Random Forest, Autoencoder, machine learning, deep learning, intrusion detection, digital economy, Uzbekistan, network security.

Introduction. Digital transformation has become one of the most important drivers of economic development in the twenty-first century. Governments, financial institutions, telecommunications operators, enterprises, educational organizations, and citizens increasingly rely on digital platforms for communication, financial transactions, data exchange, and public services. As a result, the stability

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

and security of digital infrastructure have become essential components of national economic security. Uzbekistan has also experienced rapid digital transformation. The increasing use of electronic government services, digital banking, mobile applications, online commerce, cloud technologies, and telecommunications infrastructure has created significant opportunities for economic development. However, the increasing volume and complexity of network traffic also creates new cybersecurity risks. Official information from Uzbekistan's Ministry of Internal Affairs demonstrates the growing scale of technology-related crime. In 2019, 863 crimes in 18 categories were registered, whereas in 2024 the number reached 58,800 crimes across 62 categories. The share of cybercrime in total crime increased from 6.2% in 2023 to 44.4% in 2024. This rapid increase demonstrates that cybersecurity cannot rely exclusively on traditional signature-based protection mechanisms. Signature-based intrusion detection systems are effective against previously identified threats but have limited capabilities when dealing with novel attack patterns, zero-day attacks, polymorphic malware, and sophisticated behavioral anomalies. Consequently, machine learning (ML) and deep learning (DL) have become important technologies for intelligent intrusion detection systems. Modern research increasingly investigates hybrid architectures that combine supervised, unsupervised, and sequential learning mechanisms. For example, recent research has demonstrated the potential of combining Random Forest, LSTM, Autoencoder, and other machine learning models within a single network intrusion detection framework. Among deep learning models, Long Short-Term Memory networks are particularly suitable for analyzing sequential network data because they can capture temporal dependencies. Autoencoders, in contrast, can learn representations of normal traffic and identify deviations using reconstruction error. Random Forest provides an effective supervised classification mechanism and can also provide information about the relative importance of input features. Therefore, the integration of these three approaches may provide a more comprehensive detection mechanism than using a single algorithm. The purpose of this research is to develop and theoretically justify a hybrid artificial intelligence model that integrates LSTM, Random Forest, and Autoencoder technologies for network anomaly detection in Uzbekistan's digital economy.

Literature review. Network intrusion detection systems are traditionally divided into signature-based and anomaly-based approaches. Signature-based systems identify known attack patterns, whereas anomaly-based systems attempt to recognize deviations from normal behavior. The rapid evolution of cyberattacks has increased interest in anomaly-based detection. Machine learning algorithms can analyze large amounts of network traffic and identify patterns that may be difficult to detect through manually designed rules. Recent studies have demonstrated that hybrid ML/DL architectures can improve the flexibility of intrusion detection systems by combining different learning paradigms. A recent hybrid NIDS study integrated Random Forest, LSTM, Autoencoder, and other models and used weighted ensemble prediction to combine their outputs. However, the use of multiple algorithms introduces additional challenges, including computational complexity, model coordination, data preprocessing requirements, and interpretation of the final prediction.

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

Long Short-Term Memory for Network Security. Long Short-Term Memory is a specialized recurrent neural network architecture designed to address the limitations of conventional recurrent neural networks in learning long-term dependencies. An LSTM network contains memory cells and gating mechanisms that regulate the flow of information. This enables it to retain important information over time and discard irrelevant information. In network security, this characteristic is useful because cyberattacks frequently consist of a sequence of related activities rather than a single isolated event.

For example, a potential intrusion may involve the following sequence:

Repeated login attempts → unusual IP address → privilege escalation → abnormal data request → data transfer.

A conventional static classifier may treat these events independently. An LSTM model can analyze them as a temporal sequence. Previous research has demonstrated that combining Autoencoder-based feature learning with LSTM classification can improve intrusion detection performance compared with several conventional machine learning approaches.

Autoencoder for Anomaly Detection. An Autoencoder is an artificial neural network designed to learn a compressed representation of input data and reconstruct the original input.

Its general architecture is:

$$X \rightarrow \text{Encoder} \rightarrow \text{Latent Representation} \rightarrow \text{Decoder} \rightarrow \hat{X}$$

The reconstruction error can be expressed as:

$$E(X) = \| X - \hat{X} \|^2$$

where:

−Xrepresents the original input;

−$\hat{X}$represents the reconstructed input;

−E(X)represents the reconstruction error.

When the model is trained primarily on normal traffic, anomalous traffic can generate a higher reconstruction error.

Thus:

$$E(X) > \tau$$

can indicate an anomaly, where τis the predefined anomaly threshold. The major advantage of this approach is that the system does not necessarily require labeled examples of every possible attack. This is particularly important for detecting previously unknown or zero-day attacks. Recent research has continued to investigate Autoencoder-based hybrid architectures for intrusion detection, including combinations with LSTM and other deep learning models.

Random Forest for Network Traffic Classification. Random Forest is an ensemble learning algorithm based on multiple decision trees.

The final prediction is generally determined by aggregating the predictions of individual trees:

$$\hat{y} = \text{mode}\{h_1'(x), h_2'(x) \ldots h_T(x)\}$$

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

where $h_i(x)$represents the prediction of the i-th decision tree.

Random Forest has several advantages for cybersecurity applications:

- relatively strong performance on structured data;
- resistance to overfitting compared with individual decision trees;
- ability to process nonlinear relationships;
- feature importance estimation;
- suitability for multiclass classification.

Recent research has also demonstrated the value of combining Autoencoder and Random Forest models. Such architectures use Autoencoder-based representation learning together with Random Forest classification to improve intrusion detection.

Results and discussion. Because the proposed study is primarily a methodological and architectural investigation, numerical experimental results are not fabricated. Instead, the expected behavior of the hybrid model is discussed based on the characteristics of the integrated algorithms and recent research.

Complementarity of the Models. The three algorithms address different weaknesses of network intrusion detection.

Model	Learning paradigm	Primary function	Main advantage
Autoencoder	Unsupervised	Anomaly detection	Detects deviations from normal behavior
LSTM	Deep sequential learning	Temporal analysis	Captures sequential attack patterns
Random Forest	Supervised ensemble learning	Classification	Classifies known attack categories
Hybrid Model	Integrated	Risk assessment	Combines complementary detection mechanisms

The Autoencoder is particularly useful when labeled examples of new attacks are unavailable. LSTM contributes temporal context, while Random Forest provides interpretable classification and feature-importance information. Recent research supports the general principle of combining different ML/DL models because different architectures capture different characteristics of network traffic.

Performance evaluation framework. The proposed system should be evaluated using multiple performance indicators rather than accuracy alone.

Accuracy

$$\text{Accuracy}=\frac{TP+TN}{TP+TN+FP+FN}$$

Precision

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

$$\text{Precision}=\frac{TP}{TP+FP}$$

Recall

$$\text{Recall}=\frac{TP}{TP+FN}$$

F1-score

$$F1=2\times\frac{\text{Precision}\times\text{Recall}}{\text{Precision}+\text{Recall}}$$

Additional metrics should include:

- ROC-AUC;
- PR-AUC;
- False Positive Rate;
- False Negative Rate;
- Detection Rate;
- inference latency;
- memory consumption;
- computational cost.

In cybersecurity, F1-score, recall, and false-positive rate are particularly important because a model with high overall accuracy can still perform poorly on rare but dangerous attack classes.

Application to uzbekistan's digital economy. The proposed model has potential applications across several sectors of Uzbekistan's digital economy.

Banks process large volumes of digital transactions and authentication events. The proposed system could analyze:

- abnormal login behavior;
- repeated authentication failures;
- unusual API requests;
- suspicious IP activity;
- automated attacks;
- abnormal transaction-related network traffic.

The relevance of cybersecurity to Uzbekistan's financial sector is particularly significant because official government information reports that 98% of recorded cybercrimes in 2024 involved bank-card fraud or cyber theft. Future research should focus on experimental validation using real or realistically simulated network traffic from Uzbekistan.

Several directions are particularly important. First, a national cybersecurity dataset should be developed. Such a dataset could contain anonymized network flows from different economic sectors.

Second, the proposed model should be compared experimentally with individual baseline models:

- Random Forest;
- LSTM;

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

- Autoencoder;
- LSTM-Autoencoder;
- Random Forest-Autoencoder;
- conventional IDS.

Third, hyperparameter optimization should be performed using systematic methods such as Bayesian optimization or evolutionary optimization. Fourth, Explainable Artificial Intelligence (XAI) techniques should be incorporated to provide interpretable explanations of model decisions. Fifth, the model should be tested against adversarial examples and concept drift. Finally, real-time deployment using distributed data-processing technologies should be investigated.

Conclusion. This study proposed a hybrid artificial intelligence framework for network anomaly detection in Uzbekistan's digital economy through the integration of Long Short-Term Memory, Random Forest, and Autoencoder models. The analysis demonstrates that these algorithms provide complementary capabilities. The Autoencoder is appropriate for learning normal network behavior and identifying deviations through reconstruction error. LSTM provides temporal analysis and can identify sequential patterns associated with sophisticated attacks. Random Forest provides supervised classification and feature-importance analysis. The integration of these approaches provides a broader analytical perspective than a single-model architecture. Instead of relying exclusively on predefined attack signatures, the proposed system combines behavioral, temporal, and classification-based evidence. The relevance of this approach is particularly strong for Uzbekistan. Official data indicate a substantial increase in technology-enabled crime, with 58,800 technology-related crimes registered in 2024 compared with 863 in 2019. The share of cybercrime in total crime also increased considerably, highlighting the importance of preventive and intelligent cybersecurity mechanisms. The proposed LSTM–Random Forest–Autoencoder architecture therefore provides a theoretical foundation for developing proactive network security systems capable of supporting Uzbekistan's banking sector, telecommunications infrastructure, e-government platforms, cloud services, and enterprise networks. However, the proposed architecture should not be considered experimentally validated until it is tested on representative datasets under controlled conditions. Future experimental research should measure accuracy, precision, recall, F1-score, false-positive rate, detection latency, computational cost, and robustness against previously unseen attacks. Overall, the integration of deep learning, machine learning, and unsupervised anomaly detection represents a promising direction for strengthening cybersecurity in Uzbekistan's rapidly developing digital economy.

References

1. Breiman, L. (2001). Random forests. Machine Learning, 45, 5–32.
2. Breiman, L. (2001). Random forests. Machine Learning, 45, 5–32.
3. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176.

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

4. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.
5. Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. Neural Computation, 9(8), 1735–1780.
6. Mushtaq, E., Zameer, A., Umer, M., & Abbasi, A. A. (2022). A two-stage intrusion detection system with auto-encoder and LSTMs. Applied Soft Computing. The study demonstrated the value of combining Autoencoder-based feature learning with LSTM classification for intrusion detection.
7. Mhamdi, L., & Isa, M. M. (2024). Securing SDN: Hybrid autoencoder-random forest for intrusion detection and attack mitigation. Journal of Network and Computer Applications.
8. Almuhanna, R., & Dardouri, S. (2025). A deep learning/machine learning approach for anomaly based network intrusion detection. Frontiers in Artificial Intelligence.
9. HAE-HRL: A network intrusion detection system utilizing a novel autoencoder and a hybrid enhanced LSTM-CNN-based residual network. (2025). Computers & Security.
10. Russell, S., & Norvig, P. (2021). Artificial Intelligence: A Modern Approach (4th ed.). Pearson.
11. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. 2010 IEEE Symposium on Security and Privacy, 305–316.
12. Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. IEEE Access, 5, 21954–21961.
13. Chawla, N. V., Bowyer, K. W., Hall, L. O., & Kegelmeyer, W. P. (2002). SMOTE: Synthetic minority over-sampling technique. Journal of Artificial Intelligence Research, 16, 321–357.
14. Ministry of Internal Affairs of the Republic of Uzbekistan. (2025). Creating a Safe Cyberspace by Combating Cybercrime: Uzbekistan's Experience in Preventing Cybercrime and Ensuring a Safe Cyberspace.
15. Ministry of Internal Affairs of the Republic of Uzbekistan. (2025). Information on the activities of the Cybersecurity Center and the growth of technology-related crimes in Uzbekistan.