ADVANCES IN CYBER-PHYSICAL SYSTEMS

Vol. 10, No. 1, 2025

PREDICTING CYBERSPACE INTRUSIONS USING MACHINE LEARNING ALGORITMS

Tinatin Mshvidobadze

Gori State University, 53 Chavchavadze Avenue, Gori, Georgia
Author's e-mail: *tinikomshvidobadze@gmail.com*

https://doi.org/10.23939/acps2025.01.059

Submitted on 16.04.2025

***Abstract*: The article presents possible strategies and approaches to address the growing cybersecurity threat landscape, new trends and innovations, such as artificial intelligence and machine learning for cyber threat detection and automation. The paper presents well-known machine learning classifiers for data classification. The dataset has been taken from a report by the Center for Strategic and International Studies. The presented model accuracy assessment study has been significant variation among algorithms based on different network intrusion detection systems.**

***Index terms*: cybersecurity, artificial intelligence, cyber incidents, machine learning**

I. INTRODUCTION

The widespread use of the Internet and the rapid development of cyberattacks have created a dynamic and complex environment in which cybersecurity is essential to protect personal data, critical infrastructure, and national security interests.

Governments, international organizations, and industry sectors have begun working to create and enforce cybersecurity rules and regulations in response to this evolving threat landscape. These legal frameworks aim to establish standards, requirements, and consequences for individuals and entities engaged in activities that affect the security and privacy of digital assets.

The security of data and information assets has become a top priority for companies and governments in an era of digital transformation and increasing dependence on technology.

Artificial intelligence (AI) and machine learning can be used to detect threats, detect network vulnerabilities and reduce IT workload. In addition, machine learning and artificial intelligence (AI) can be used to automate many tasks involved in cybersecurity, such as intrusion detection, malware analysis and vulnerability assessment.

This can free up security professionals to focus on more strategic tasks. Organizations are turning to machine learning (ML) and artificial intelligence (AI) as powerful tools in their cybersecurity arsenal to combat increasingly sophisticated cyber threats.

We explore the profound impact of ML and AI on cybersecurity and how they are transforming cyber defenses.

Biswas et al. used a text mining approach to detect cyber incidents in the digital healthcare sector. The authors used natural language processing (NLP) to extract news data and extract information [1].

Souri et al. presented an anomaly detector using crash reports. They worked on text data and used Local Outlier Factor (LoF) to detect anomalous conditions. The authors investigated various DM-ML approaches for malware detection, as well as a deep learning methodology used to predict cyberattacks based on data obtained from network traffic. [2].

Fang et al. developed cyberattack methods using support vector machine (SVM) in ML algorithm. The authors concluded that various DM-ML approaches such as Bayesian networks, decision trees, clustering, and artificial neural networks (ANN) can be used to detect cyber incidents in cybersecurity [3].

In this paper, we discuss cybersecurity challenges and future research directions, including the use of AI, machine learning, and other cutting-edge techniques to address cybersecurity challenges.

II. LITERATURE REVIEW AND PROBLEM STATEMENT

Zhang et al. [4] investigated the application of deep learning approaches to cybersecurity threat detection in Internet of Things (IoT) devices. The researcher discusses the application of deep learning for cybersecurity threat detection and proposes a combined deep learning approach to detect pirated and malware-infected files in Internet of Things (IoT) networks and achieve better classification performance with 97.46% accuracy. Their study provides a comprehensive overview of the application of artificial intelligence (AI) in cybersecurity and discusses the challenges and opportunities of using artificial intelligence (AI) in cybersecurity. The researchers discuss the potential of artificial intelligence (AI) for cybersecurity challenges and the field of AI for cybersecurity, including the use of AI for anomaly detection, intrusion detection, and malware analysis. It then considers the challenges and opportunities of using AI in cybersecurity, including the need for big data, the risks of attackers using AI, and the need for human oversight.

A study by Gunduz and Das [5] introduces cybersecurity threats and potential solutions in smart grids. The researcher discusses cyber threats such as denial of service (DoS) attacks, malware attacks, phishing attacks, and insider attacks and suggests solutions to the cybersecurity threats faced by the smart grid. Some of the potential solutions discussed by the researcher are implementing security measures and educating employees about cybersecurity threats and solutions.

Abbasi et al. [6] agitates the valuable contribution of artificial intelligence in cybersecurity to prevent, detect, and mitigate cyber threats. The researcher identifies the role, extent, and capabilities of AI in mitigating cyber threats. The application of artificial intelligence (AI) in malware detection, network intrusion detection systems, vulnerability scanning, risk assessment, and security automation. The study is based on a comprehensive study to present the use of artificial intelligence (AI) in cybersecurity to automate tasks, improve decision-making, and detect threats more effectively than traditional methods.

Liew et al. [7] propose a new methodology for analyzing the safety and security of cyber-physical systems using custom metrics. To provide a more in-depth investigation of safety and security, the researcher proposes an approach that uses System Theoretical Process Investigation (STPA), a top-down threat analysis tool, and custom matrices. The researcher wants to overcome the limitations of STPA by integrating STPA and custom metrics. STPA is used to find risky control scenarios that can lead to unexpected losses. The possibility of using these scenarios by bad actors is then considered using custom matrices.

Cybersecurity is an emerging and huge challenge worldwide with various cyber incidents. An important part is identifying existing incidents using various DM-ML algorithms. DM-ML-based approaches are very well-known techniques used to detect cybersecurity vulnerabilities and that is why they are used in the BoW model, while NB, SVM, LR, and RF algorithms are used for the classifier.

AI-driven attacks. Cybersecurity challenges are becoming more complex and difficult due to the rapid growth of technological advancements and increasing digitalization in various domains, which makes cybersecurity more difficult. One of the technological advancements is artificial intelligence (AI) and machine learning, and the current trends in cyberattacks are the use of AI and machine learning technologies. Even if artificial intelligence (AI) has a positive impact on cybersecurity, there is also a negative impact, which is artificial intelligence (AI)-driven attacks. Attacks that use AI technology are of two types: 1) artificial intelligence (AI)-assisted attacks, which use artificial intelligence (AI) and machine learning technologies, and 2) autonomous artificial intelligence (AI). The attack uses artificial intelligence (AI) and machine learning technology or artificial intelligence (AI) agents to carry out cyberattacks on various industries autonomously. Artificial intelligence attacks:

- Deep fake attacks are carried out through artificially generated fake and convincing media that uses AI and machine learning technology to create realistic images, video, audio, or text that can deceive or trick humans or systems during social engineering attacks. AI-generated images, videos, audio, and text can be intentionally used to trick AI and machine learning models or systems used for cybersecurity purposes, to infiltrate and mislead security systems that rely on AI and machine learning systems, such as artificial intelligence, spam filtering, facial recognition, and other biometric security mechanisms.
- Botnet attacks are interconnected devices that are centrally controlled by cybercriminals to carryout various attacks on a target area. Some of the attacks carried out by botnets are denial of service, spam, data theft, and more. Botnet attacks use AI and machine learning technology to address security vulnerabilities and increase the speed of attacks by automating and increasing the number of attacks to find targets, coordinate attacks, and evade detection. [8].

Advanced AI and machine learning techniques are being used to develop defense technologies against cyber threats, improve cyber threat detection, automate cybersecurity processes, and prevent cyberattacks. As cyberattacks become more complex and sophisticated, it requires the automation of cyber defense mechanisms using AI and machine learning technology to strengthen cybersecurity. Real-time AI enables cyber threat detection systems to help cyber experts analyze large amounts of data, discover patterns in cyberattacks, identify threats and anomalies, and automate security responses to help cyber professionals respond to cyberattacks more effectively. In addition to artificial intelligence (AI) and machine learning (ML) technology, biometric authentication is the most effective technology for securing targeted industries. Biometric authentication, which verifies a user's identity using unique biological characteristics, such as fingerprints or facial recognition, can improve security. Biometric authentication, when combined with standard authentication techniques such as passwords, makes it difficult for thieves to access networks and data. [9].

In addition, the development of blockchain technology is also one of the important concerns to strengthen the cybersecurity of organizations. Blockchain technology and distributed ledger system provide excellent solutions for security and decentralized systems, and various researchers have explored the implementation of blockchain technology in various fields of cybersecurity. Even if blockchain technology has a great role in providing security mechanisms in the cybersecurity domain, there are difficulties and challenges such as immutable or unchangeable transactions, vulnerabilities in smart contracts, weaknesses in the protocols used in blockchain technology such as consensus protocols such as PoS and PoW attacks, dependence on external systems such as Oracles is also one of the security challenges of Blockchain technology. To solve or minimize such security problems and challenges in blockchain technology,

appropriate security measures should be adopted and implemented, such as using secure smart contract development methods, implementing strong consensus protocols, and incorporating and integrating privacy-enhancing strategies. All of these are part of it. To create a secure and robust system, it is critical to find a balance between the benefits of blockchain and DLT and the associated cybersecurity issues.

III. SCOPE OF WORK AND OBJECTIVES

In this paper, we discuss the effective results obtained by various researchers to eliminate these incidents.

The results of the research conducted by Usman Ashraf and other researchers within the framework of the project [10] are presented. The benefits of a centralized classifier for future SCI eradication are also shown.

ML algorithms such as Naive Bayes (NB) [11], Support Vector Machine (SVM) [12], Logistic Regression (LR) [13], and Decision Forest (RF) [14] are used for data classification [15], prevention, and prediction of cyber incidents.

IV. DIRECT PATHFINDING PROBLEM

A cyber incident (SCI) is an incident that causes significant damage to national security and the economy [16]. With the increase in SCI, cybersecurity measures have also improved to address these incidents. Data mining and machine learning (DM-ML) plays an important role in predicting, preventing, and detecting cyber incidents using various approaches [17].

Ashraf and other researchers have shown the effectiveness of using a centralized classifier. The dataset was used to train a centralized classifier for each continent. The dataset is the type of SCI that occurred in 6 continents of the world (from September 2004 to October 2024), according to a report by the Center for Strategic and International Studies (CSIS). The number of SCI is higher for Asia, as it is the largest continent in the world. (Table. 1.).

Table 1

Data Distribution

Type	Africa	Asia	Europe	North America	Oceania	SCI
APT	6	62	27	23	5	123
DDoS	0	15	13	6	3	38
DoS	0	2	0	10	0	1
Espionage	1	8	7	7	1	248
Malware	4	52	53	27	53	125
M-Middle	1	1	1	1	1	5
Phishing	3	55	86	47	6	205
QL Inj.	47	3	98	2	0	20
Total	21	301	197	116	25	752

This study identified, investigated, and solved how to calculate the name of a continent based on the type of SCI. Four different machine learning classifiers are used for classification: Naive Bayes (NB) - It is based on Bayes' theorem [18], which is derived from conditional probability. It is commonly used in supervised learning for text data classification. NB is effective for nonlinear problems. Support Vector Machine (SVM) – This is a supervised learning classifier. SVM is a vector approach and is very effective if the problem is linear and the data set is limited. Logistic Regression (LR) – Predicts binary problems and their outcomes efficiently. It provides information about the statistical significance of features and uses a probabilistic approach [19].

Decision Forest (RF) – Random Forest consists of many decision trees, increasing the efficiency of the model. It also works on nonlinear problems. Technically, it is a method for generating decision trees from a subset of the data set. The concept of unigram and bigram models was used in the project to filter words from the data with a minimum frequency.

The result of using classifiers in the experimental study is the prediction of the name of the continent based on the type of SCI. To evaluate the performance of the classifiers, accuracy and F1-measure are used as performance indicators. The accuracy measures NB, LR and RF are (0.952396, 0.920829), (0.984139, 0.962375), (0.978099, 0.962375) respectively. The SVM, NB, LR, and RF classifiers were evaluated individually and it was determined that Asia is the most affected region in terms of SCI.

Today, network intrusion detection systems (NIDS) are essential for protecting digital assets in an increasingly interconnected world. As cyber threats evolve, so do the strategies for detecting and remediating them. According to the World Economic Forum’s Global Cybersecurity Outlook 2024, cyberattacks have evolved into more sophisticated attacks, and the cloud environment is increasing the penetration and emergence of malware-free attacks.

Evaluating Machine Learning Algorithms for Network Intrusion Detection. Machine learning (ML) models can also be computationally intensive and require large amounts of processing power, which may not be practical for real-time deployment. Network traffic often contains lost packets, which leads to incomplete data and a loss of detection accuracy. Thus, such improvements, in the range of dynamic cyber threats, are important for enhancing the reliability and robustness of NIDS. In our work, several ML models are used, such as Random Forest(RF), Support Vector Machine (SVM), AdaBoost. K-Nearest Neighbor (KNN).

By integrating these models, the system achieves a compromise between accuracy and computational cost, which makes it possible to build a large-scale network strategy. Moreover, experimental analysis is performed on a publicly available NIDS database. The effectiveness of the approach is also determined by testing on multiple instances, using recall, precision, and F1 score.

Dong et al. [20] reported an ML-based IDS that combines multivariate correlation analysis (MCA) and short-term short-term memory (LSTM). They used an information retrieval method feature selection strategy. The test accuracy of MCA-LSTM was 82.15% for the experiment on the NSL KDD dataset for five-way classification. In addition, the accuracy was 77.74% for the 10-way classification task in UNSW NB15. Injadat et al. [21] proposed a multi-level ML-based framework for NIDS evaluation using RF and KNN algorithms for attack type classification.

Random Forest Classifier. This ensemble learning technique produces several decision trees and then combines their predictions. It also helps to reduce the noise level in the dataset, which is achieved by averaging the result from many trees to reduce the chances of getting overfitted [22]. RF, which averages several decision trees to prevent overfitting, can easily handle large datasets and provide accurate categorization. Each tree is built using a random collection of features and examples. The final prediction F(x) for a sample x-is given by:

$$F\ x\ = \frac{1}{N}\ \ \sum_{i=1}^{N} h_i\ (x)\ , \qquad (1)$$

where N - is the number of trees and $h_i(x)$ is the prediction from the i^{th} tree.

V. RESULTS

Model Evaluation. Understanding the effectiveness of models in categorizing network traffic depends on their evaluation. To facilitate comparison of accuracy and other performance measures, each model is evaluated based on how well it performs on a test set. Important measurements include - Accuracy - the ratio of correctly predicted instances to total instances:

$$\boldsymbol{Accuracy} = \frac{\mathrm{TP+TN}}{\mathrm{TP+FP+TN+FN}}\ , \qquad (2)$$

where

$$\boldsymbol{Precision} = \frac{\mathrm{TP}}{\mathrm{TP+FP}} \cdot 100$$

$$\boldsymbol{Recall\ R}\ = \frac{\mathrm{TP}}{\mathrm{TP+FN}} \cdot 100.$$

TP (True positive): A spam email correctly classified as a spam email. These are the spam messages automatically sent to the spam folder.

TN (True negative): A not-spam email correctly classified as not-spam. These are the legitimate emails that are sent directly to the inbox.

FP (False positive): A not-spam email misclassified as spam. These are the legitimate emails that wind up in the spam folder.

FN (False negative): A spam email misclassified as not-spam. These are spam emails that aren't caught by the spam filter and make their way into the inbox.

Recall is the ratio of true positive predictions to the total actual positives.

After implementing ML models, the following results were achieved, as shown in Table 2.

TN (True negative): A not-spam email correctly classified as not-spam. These are the legitimate emails that are sent directly to the inbox.

FP (False positive): A not-spam email misclassified as spam. These are the legitimate emails that wind up in the spam folder.

FN (False negative): A spam email misclassified as not-spam. These are spam emails that aren't caught by the spam filter and make their way into the inbox.

Recall is the ratio of true positive predictions to the total actual positives.

After implementing ML models, the following results were achieved, as shown in Table 2.

Table 2

Achieved accuracy of the machine learning models

Models	Accuracy
Random Forest	0.9978
SVM	0.5314
AdaBoost	0.9908
KNN	0.9849
Gaussian Naive Bayes	0.5572
Multinomial Naive Bayes	0.5514

A comparative study of model accuracy reveals significant variation among different NIDS algorithms. With an accuracy of 99.78%, the RF model is the most accurate, demonstrating its usefulness in handling large datasets and identifying complex patterns associated with network intrusion. [23].

By achieving an accuracy of 98.49%, the KNN model is considered to have mediocre performance. Similarly, the accuracies of multinomial Naive Bayes and Gaussian models are 55.72% and 55.14%, respectively.

Fig. 1 shows confusion of miscellaneous machine learning models.

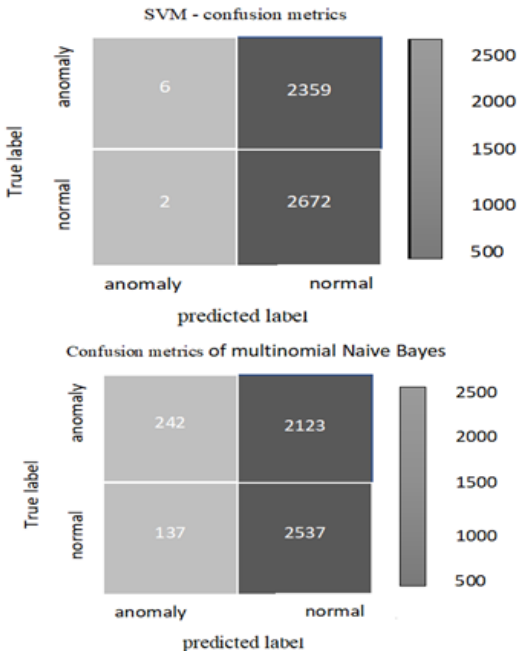

Fig.1. Confusion of machine learning models.

Fig. 2 shows the accuracy distribution. Resultantly, it is shown that RF and AdaBoost are emerging as the best choices because of their better intrusion detection rate.

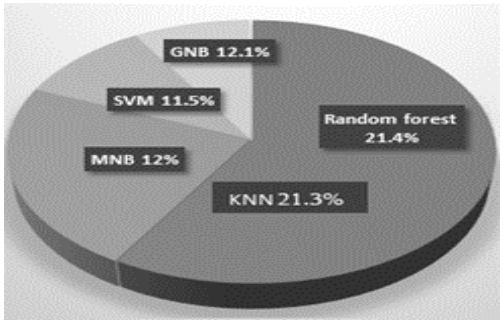

Fig. 2. Accuracy distribution

V. CONCLUSION

Real-time AI was used in cyber threat detection systems to help cyber experts analyze big data, detect patterns of cyberattacks, identify anomalies, and automate security responses, allowing cyber professionals to respond more effectively to cyberattacks.

In addition, the development of blockchain technology was also one of the important concerns to strengthen the cybersecurity of the organization. There were difficulties and challenges such as immutable or immutable transactions, vulnerability of smart contracts, weakness of protocols used in blockchain technology such as consensus protocols such as PoS and PoW for attacks, dependence on external systems, is also one of the security challenges of Blockchain technology. To solve or minimize such security problems and challenges in blockchain technology, appropriate security measures should be adopted and implemented, such as using secure smart contract development methods, implementing strong consensus protocols, and incorporating and integrating privacy-enhancing strategies.

This study proposed an intrusion detection method using ML models to make the network robust and reliable. The discovery was made by investigating the performance of RF, SVM, AdaBoost, KNN, Gaussian Naive Bayes, and Multinomial Naive Bayes using the NIDS dataset. Experimental results were shown, and the best intrusion detection model was identified. In the future, this work will be expanded to use more features and also hybrid technologies to make the method more robust and flexible in terms of selection parameters.

References

[1] Biswas B., Mukhopadhyay A., Bhattacharjee S., Kumar A., and Delen D. (2022). A text-mining based cyber-risk assessment and mitigation framework for critical analysis of online hacker forums. *Decision Support Systems,* vol. 152. 113651. DOI: https://doi.org/10.1016/j.dss.2021.113651;

[2] Souri A., and Hosseini R. (2018) A state-of-the-art survey of malware detection approaches using data mining techniques. *Human-centric Computing and Information Sciences,* vol. 8. 1-22. DOI: https://doi.org/10.1186/s13673-018-0125-x

[3] Fang, X., Xu, M., Xu, S., & Zhao, P. (2019). A deep learning framework for predicting cyber attacks rates. *EURASIP Journal on Information security, 2019*, 1-11. DOI: https://doi.org/10.1186/s13635-019-0090-6;

[4] Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., & Choo, K. K. R. (2022). Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artificial Intelligence Review*, 1-25., DOI:https://doi.org/10.1007/s10462-021-09976-0;

[5] Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer networks*, *169*, 107094. DOI: https://doi.org/10.1016/j.comnet.2019.107094

[6] Abbas, N. N., Ahmed, T., Shah, S. H. U., Omar, M., & Park, H. W. (2019). Investigating the applications of artificial intelligence in cyber security. *Scientometrics*, *121*, 1189-1211. DOI:https://doi.org/10.1007/s11192-019-03222-9

[7] Liew, L. S., Sabaliauskaite, G., Kandasamy, N. K., & Wong, C. Y. W. (2021, December). A novel system-theoretic matrix-based approach to analysing safety and security of cyber-physical systems. In *Telecom* (Vol. 2, No. 4, pp. 536-553). MDPI. DOI: https://doi.org/10.3390/telecom2040030

[8] AsSadhan, B., & Moura, J. M. (2014). An efficient method to detect periodic behavior in botnet traffic by analyzing control plane traffic. *Journal of advanced research*, *5*(4), 435-448. DOI: https://doi.org/10.1016/j.jare.2013.11.005

[9] Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The emerging threat of ai-driven cyber attacks: A review. *Applied Artificial Intelligence*, *36*(1), 2037254. DOI: https://doi.org/10.1080/08839514.2022.2037254

[10] Mumtaz, G., Akram, S., Iqbal, M. W., Ashraf, M. U., Almarhabi, K. A., Alghamdi, A. M., & Bahaddad, A. A. (2023). Classification and prediction of significant cyber incidents (SCI) using data mining and machine learning (DM-ML). *IEEE Access*, *11*, 94486-94496. DOI: https://doi.org/ 10.1109/ACCESS.2023.3249663

[11] Alqahtani, H., Sarker, I. H., Kalim, A., Minhaz Hossain, S. M., Ikhlaq, S., & Hossain, S. (2020). Cyber intrusion detection using machine learning classification techniques. In *Computing Science, Communication and Security: First International Conference, COMS2 2020, Gujarat, India, March 26–27, 2020, Revised Selected Papers 1* (pp. 121-131). Springer Singapore. DOI: https://doi.org/ 10.1007/978-981-15-6648-6_10

[12] Bhusal, N., Gautam, M., & Benidris, M. (2021). Detection of cyber attacks on voltage regulation in distribution systems using machine learning. *IEEE Access*, *9*, 40402-40416. DOI: https://doi.org/10.1109/ACCESS.2021.3064689

[13] Bapat, R., Mandya, A., Liu, X., Abraham, B., Brown, D. E., Kang, H., & Veeraraghavan, M. (2018, April). Identifying malicious botnet traffic using logistic regression. In *2018 systems and information engineering design symposium (SIEDS)* (pp. 266-271). IEEE. DOI: https://doi.org/ 10.1109/SIEDS.2018.8374749

[14] Ustebay, S., Turgut, Z., & Aydin, M. A. (2018, December). Intrusion detection system with recursive feature elimination by using random forest and deep learning classifier. In *2018 international congress on big data, deep learning and fighting cyber terrorism (IBIGDELFT)* (pp.

71-76). IEEE. DOI: https://doi.org/10.1109/IBIGDELFT.2018.8625318

[15] Chayal, N. M., & Patel, N. P. (2020). Review of machine learning and data mining methods to predict different cyberattacks. *Data Science and Intelligent Applications: Proceedings of ICDSIA 2020*, 43-51. DOI: https://doi.org/10.1007/978-981-15-4474-3_5

[16] Maeda, R., & Mimura, M. (2021). Automating post-exploitation with deep reinforcement learning. *Computers & Security*, *100*, 102108. DOI: https://doi.org/10.1016/j.cose.2020.102108

[17] Handa, A., Sharma, A., & Shukla, S. K. (2019). *Machine learning in cybersecurity: A review. WIREs Data Mining and Knowledge Discovery, 9 (4)*. DOI: https://doi.org/10.1002/widm.1306

[18] Xu, S. (2018). Bayesian Naïve Bayes classifiers to text classification. *Journal of Information Science*, *44*(1), 48-59. DOI:https://doi.org/10.1177/0165551516677946

[19] Susilo, B., & Sari, R. F. (2020). Intrusion detection in IoT networks using deep learning algorithm. *Information*, *11*(5), 279. DOI:https://doi.org/10.3390/info11050279

Tinatin Mshvidobadze was born in 1969 in Gori, Georgia. She completed Georgian Technical University. She is a Doctor of Technical Sciences professor of Gori State University. Also, she is a member of Cyber Security Association. She is the author of up to 100 scientific articles, 12 textbooks and 7 monographs.

[20] Dong, R. H., Li, X. Y., Zhang, Q. Y., & Yuan, H. (2020). Network intrusion detection model based on multivariate correlation analysis–long short- time memory network. *IET Information Security*, *14*(2), 166-174. DOI:https://doi.org/10.1049/iet-ifs.2019.0294

[21] Injadat, M., Moubayed, A., Nassif, A. B., & Shami, A. (2020). Multi-stage optimized machine learning framework for network intrusion detection. *IEEE Transactions on Network and Service Management*, *18*(2), 1803-1816. DOI:https://doi.org/10.1109/TNSM.2020.3014929

[22] Barrenada, L., Dhiman, P., Timmerman, D., Boulesteix, A. L., & Van Calster, B. (2025). Understanding overfitting in random forest for probability estimation: a visualization and simulation study (vol 8, 14, 2024). *Diagnostic and Prognostic Research*, *9*(1). DOI: https://doi.org/10.1186/s41512-024-00177-1

[23] Sarker, I. H., Abushark, Y. B., Alsolami, F., & Khan, A. I. (2020). Intrudtree: a machine learning based cyber security intrusion detection model. *Symmetry*, *12*(5), 754. DOI:https://doi.org/10.3390/sym12050754