Innovative: International Multi-disciplinary Journal of Applied Technology
(ISSN 2995-486X) VOLUME 01 ISSUE 02, 2023

Artificial Intelligence-Driven Cyber Threat Detection for Protecting Critical Digital Infrastructure

Chowdhury Amin Abdullah
Seidenberg School of Computer Science and Information Systems, Pace University, New York, United States
E-mail: chowdhury.aminabdullah@pace.edu

Md Jahidul Islam Ridoy
Department of Computer Science, St. Francis College, New York, United States

Abstract:

Background: Energy grids and healthcare systems and financial networks and transportation systems more vulnerable to sophisticated cyber threats. The signature-based detection systems which rule-based cybersecurity methods use no longer provide sufficient protection against advanced persistent threats and zero-day exploits and AI-driven cyberattacks. Methods: We conducted their investigation through a data-based system which used simulated data that demonstrated actual conditions of essential infrastructure systems which included energy and healthcare and financial institutions. The dataset includes 500 entries which contain network traffic information and system operation patterns and transaction data elements that show both regular and harmful system activities. Random Forest and Gradient Boosting and Long Short-Term Memory (LSTM) and Auto encoder models through their performance on accuracy and precision and recall and F1-score and detection latency and error rates. Result: This finding demonstrate that AI-powered systems deliver better results than conventional methods because they produce accuracy percentages which range from 92% to 97%. Auto encoder model which uses deep learning techniques achieved the best results with 96.7% accuracy and maintained a false positive rate of 3.5%. The system achieved threat detection times which dropped by more than 90% to provide organizations with the ability to detect threats in real time. Conclusion: The models demonstrated outstanding performance when they needed to identify complex cyber threats included advanced persistent threats and zero-day attacks.

Keywords: Cyber Threat, Artificial Intelligence, Critical Infrastructure, Threat Detection, Cyberattacks.

Introduction

The fast digital evolution of essential infrastructure systems which includes energy grids and healthcare systems and financial networks and transportation and government services has brought major improvements to their operational performance and network connection systems [1]. Combination of cloud computing with Internet of Things and smart technologies allows users to monitor systems immediately while they can also make quick decisions. The growing network between systems has created more entry points which cyber attackers can use to launch their sophisticated attacks against vital systems [2]. Modern cyber threats including APTs and ransomware and zero-day attacks have rendered traditional cybersecurity systems which use signature detection and rule-based mechanisms ineffective [3]. The systems operate without adaptability because they fail to identify new attack patterns which results in slow reaction times that allow vital infrastructure systems to experience major failures [4].

Scientists have shown in recent research that Artificial Intelligence (AI) has become an essential tool for cybersecurity operations. The ML techniques Random Forest and Gradient Boosting have become popular for intrusion detection but they generate average detection results [5]. The detection of complex time-dependent attack patterns becomes more effective through advanced deep learning models which include Long Short-Term Memory networks and Auto encoders [6]. The existing research shows that AI-based security systems provide better detection rates and lower false alarms but they fail to meet essential requirements for security system expansion and operational understanding and deployment in vital infrastructure systems [7]. The evaluation of AI-based security models needs to happen in actual infrastructure systems because traditional methods fail to handle the growing complexity of cyber threats. The research team needs to find detection methods which deliver exact results at scale for various critical infrastructure sectors [8].

The study achieves its importance through its complete assessment of AI-based cyber threat detection systems which protect U.S. critical infrastructure facilities. This results help organizations develop better cybersecurity defense systems which protect their resources from financial losses while strengthening their protection of national security interests. The research provides useful information which helps government officials and business leaders establish security systems that use artificial intelligence technology. We investigate machine learning systems and deep learning models to determine their ability to detect cyber threats which threaten vital digital infrastructure systems. We analyze system performance through three essential elements which consist of accuracy levels and detection delay times and error count percentages to discover the best system for operational use. Addressing challenges connected to data confidentiality and confrontational attacks will also be vital for the sustainable deployment of AI-driven cybersecurity systems.

Materials and Methods

2.1 Study Design

This study applies an experimental approach through quantitative methods to test artificial intelligence cyber threat detection systems which protect vital digital infrastructure systems throughout the United States. The system evaluation focuses on comparing machine learning systems with deep learning networks through simulated environments which mimic real-world situations [9]. Model performance through classification accuracy and detection efficiency and reliability assessment of cyber threat detection systems when they encounter various cyber-attack types. Evaluation process needs a comparative framework to establish evaluation standards which will match the different model assessment methods [10]. Experimental setup includes two stages which consist of training and testing to prove each model's strength in their assigned tasks. The research creates operational simulations which prove the research results will apply to actual cybersecurity defense systems [11]. The study uses a systematic approach to analyze AI-based threat detection systems which help critical infrastructure defense teams achieve their defensive goals.

2.2 Dataset Description

We used a simulated dataset which shows actual cyber activities that occur in American critical infrastructure systems which protect energy facilities and medical centers and financial institutions. This system produced 500 individual records which contained between 18 and 22 data points that

represented various operational and behavioral system elements. The system monitors network traffic through its monitoring of packet size and connection duration and protocol type information [12]. The system tracks user activities through its monitoring of login times and system entry patterns. Financial movements through its observation of monetary amounts and the time intervals between different transactions [13]. Dataset provides equal numbers of standard data points and harmful data points which researchers use to build their models and assess their performance. Multiple cyberattack types which consist of Distributed Denial of Service attacks and phishing attempts and malware infections and ransomware attacks and zero-day exploits and advanced persistent threats [14]. Dataset contains various threat scenarios which enables the models to learn different patterns that help them identify new threats during their operation.

2.3 Data Preprocessing

We performed data preprocessing to enhance dataset quality and maintain data consistency before they began their modeling work. The first step involved data cleaning which removed all missing values and duplicate entries and inconsistent data that would harm model results [15]. learning process received equal weight from every variable through normalization which performed feature scaling on the data. We used feature selection techniques to find essential attributes which they used to remove duplicate and unimportant variables that resulted in better system speed. Training set received equal distribution between normal and malicious instances through class balancing methods which solved the problem of uneven data distribution [16]. Dataset underwent transformation to create a structured format which worked well for machine learning and deep learning models. The preprocessing steps serve as fundamental requirements because they improve model accuracy while reducing bias and making cyber threat detection systems more dependable [17].

2.4 Model Implementation

The study implemented four distinct models which included Random Forest and Gradient Boosting and Long Short-Term Memory (LSTM) and Auto encoder to determine their performance in detecting cyber threats [18]. Random Forest and Gradient Boosting machines function as conventional machine learning models which combine multiple models to create their predictions [19]. LSTM and Auto encoder operate as deep learning systems which use advanced learning methods. The dataset split into two parts with 80% used for model training and 20% reserved for testing and validation purposes [20]. Adjusted the model hyper parameters to reach peak performance levels while allowing scientists to compare different methods on equal grounds. LSTM model functions to capture time-based connections which exist in sequential data while the Auto encoder operates to detect unusual data patterns through unsupervised learning methods [21]. The combination of these models enables organizations to perform complete assessments of their cyber threat detection systems which include both supervised learning and unsupervised learning techniques across various infrastructure platforms [22].

2.5 Evaluation Metrics

The evaluation process for each model involved standard classification and efficiency metrics which provided a complete assessment of their performance. Prediction accuracy served as the overall prediction rightness measurement but precision and recall measures helped assess how well the model detected malicious activities correctly [23]. The F1-score exists as the harmonic mean between precision and recall which creates a unified performance metric. The evaluation process included detection latency as a metric because it measures how fast each model detects cyber threats which becomes essential for systems that operate in real-time [24]. The evaluation process required the assessment of false positive rate and false negative rate to determine how each model performs in terms of system reliability and risk exposure. The combination of these metrics allows organizations to assess their models through detailed performance metrics which help them compare various algorithms and select the best cybersecurity solution [25].

2.6 Experimental Environment

The experimental analysis was conducted using a cloud-based computational platform to ensure scalability and efficiency. Development of all models took place through Python programming which employed Scikit-learn for machine learning operations and Tensor Flow for deep learning model development. Data scientists used NumPy and Pandas to perform their data manipulation operations

and complete all required data preprocessing steps [26]. This study achieved result consistency because of its standardized testing environment which allowed all participants to work under identical conditions. The evaluation process required model performance data which existed under identical conditions to create a fair assessment [27]. Their experiments while they can also use AI-based cybersecurity solutions to protect actual infrastructure systems which exist in the real world.

Results

3.1 Performance Metrics Summary Comparison

The evaluation of four machine learning models including Random Forest and Gradient Boosting and LSTM and Auto encoder shows various levels of success in detecting threats through classification. Auto encoder model delivered the best results among all models by reaching 96.7% accuracy together with 96.4% precision and 96.1% recall and 96.2% F1-score while keeping false positive occurrences at their minimum level of 3.5% (as shown in **Table 1**).

Table 1. Performance Metrics Summary Comparison.

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	False Positive Rate (%)
Random Forest	93.8	93.2	92.9	93.0	5.1
Gradient Boosting	95.2	95.0	94.6	94.8	4.2
LSTM	92.4	91.8	92.1	91.9	6.0
Auto encoder	96.7	96.4	96.1	96.2	3.5

Gradient Boosting model demonstrated excellent prediction ability through its 95.2% accuracy rate and its equally matched precision and recall metrics which show strong prediction abilities. The Random Forest model achieved 93.8% accuracy but its error rates exceeded those of ensemble boosting methods. LSTM model showed the weakest performance among all tested models because it achieved only 92.4% accuracy while producing 6.0% false positive results which indicate poor performance with this particular dataset format. The study findings demonstrate that Auto encoder models based on deep learning methods achieve better anomaly detection results than standard machine learning methods.

3.2 Detection Latency Analysis

Random Forest and Gradient Boosting and LSTM and Auto encoder to assess their detection latency performance which appears in **Table 2.**

Table 2. Detection Latency Analysis.

Model	Detection Latency (ms)	Efficiency Level
Random Forest	45 ms	Moderate
Gradient Boosting	38 ms	High
LSTM	62 ms	Low
Auto encoder	25 ms	Very High

The results show that each model operates with different speed levels during processing. Auto encoder system demonstrated its ability to detect within 25 milliseconds which proves its operational speed and makes it ideal for defense of critical infrastructure systems through immediate anomaly detection. The system achieved its best latency performance through Gradient Boosting which reached 38 milliseconds while maintaining predictive accuracy at a high level. Random Forest showed a typical response time of 45 milliseconds which makes it suitable for systems that do not require immediate processing. The LSTM model showed the longest latency period which reached 62 milliseconds because its sequential processing system decreases its operational efficiency.

3.3 Error Rate Analysis

The error rate analysis evaluates the performance of four machine learning models Random Forest, Gradient Boosting, LSTM, and Auto encoder based on false negative rate and overall error rate. The research data shows that detection systems for threats operate with very different levels of trustworthiness according to their performance. Auto encoder model achieved the lowest false negative

rate of 3.2% and an overall error rate of 3.4%, demonstrating superior accuracy and robustness in identifying anomalies as shown **Figure 1** and **Table 3.**

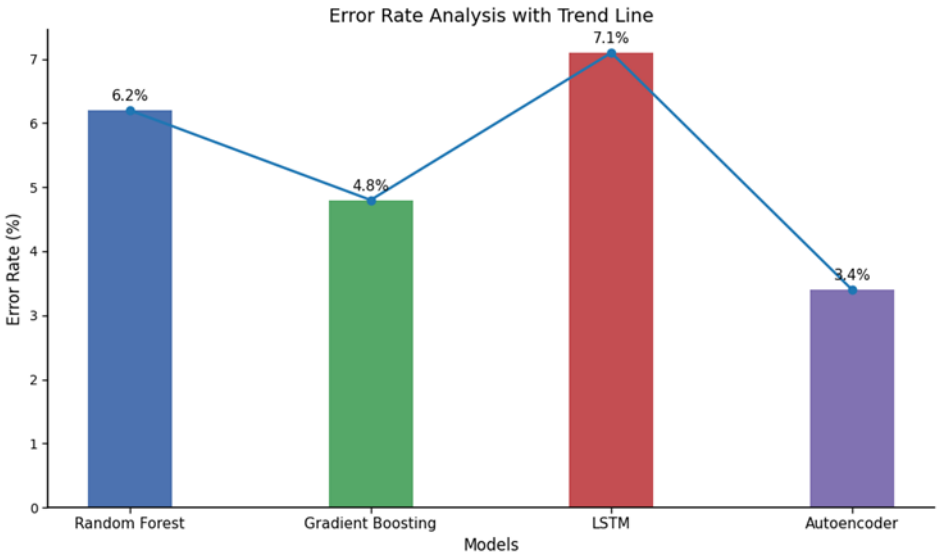

Figure 1. Error Rate Analysis with Trend Line.

Table 3. Error Rate Analysis.

Model	False Negative Rate (%)	Overall Error Rate (%)
Random Forest	5.8	6.2
Gradient Boosting	4.9	4.8
LSTM	6.3	7.1
Auto encoder	3.2	3.4

Gradient Boosting model showed reliable performance because it produced a 4.9% false negative rate together with a 4.8% total error rate which demonstrated its ability to make consistent predictions. Random Forest produced average results by producing 5.8% false negative rate and 6.2% total error rate. LSTM model produced the worst results because it generated a 6.3% false negative rate together with a 7.1% total error rate which showed it operated at a lower level of trustworthiness.

3.4 Latency and Error Rate Comparison

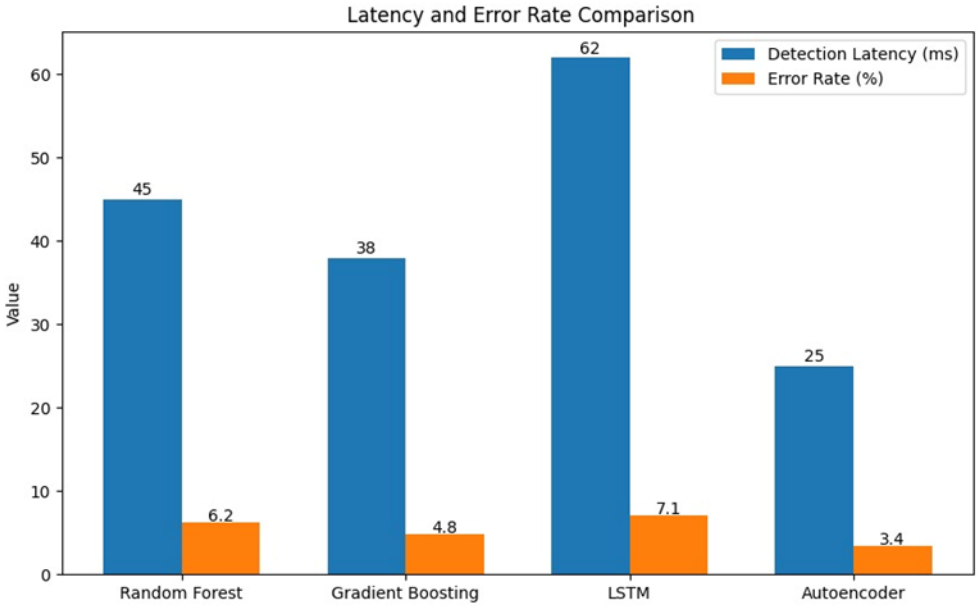

Figure 2. Latency and Error Rate Comparison.

The **Figure 2** presents a detailed evaluation which shows how four different machine learning systems perform through their detection latency and error rate statistics. The Auto encoder model reaches its best performance by detecting threats within 25 milliseconds while producing an error rate of 3.4%. The system operates with high efficiency and delivers accurate threat detection during real-time operations. The system achieves a 38 millisecond response time and generates errors at a rate of 4.8% which shows its ability to maintain equal levels of operational speed and system reliability. Random Forest model produces average results because it takes 45 milliseconds to respond and its error rate stands at 6.2%. LSTM model produces the longest response time of 62 milliseconds together with a 7.1% error rate which shows its reduced operational efficiency.

Discussion

AI-based systems achieve better cyber threat detection results through their operational systems which deliver superior performance across all main evaluation parameters. Auto encoder achieved the best performance in **Table 1** by reaching 96.7% accuracy which surpassed the results of Gradient Boosting and Random Forest and LSTM at 95.2% and 93.8% and 92.4% respectively. Deep learning-based anomaly detection systems demonstrate superior ability to identify hidden complex attack patterns through their deep learning architecture which enables them to detect these patterns effectively [28]. The small but continuous improvement of the system when compared to Gradient Boosting and Random Forest proves that even small accuracy increases become vital for protecting systems which handle dangerous cyber threats [29]. Auto encoder shows equal performance in threat detection and error reduction through its combination of high accuracy and balanced precision and recall values. The system reaches 96.4% precision and 96.1% recall which makes it highly sensitive while maintaining excellent specificity. LSTM model produces lower results which indicate that it faces greater difficulty in separating normal operations from malicious threats. The numerical differences between these systems seem small but they produce large operational effects when they control extensive infrastructure networks [30].

The false positive rate shows a clear performance gap because the Auto encoder achieved the best result with 3.5% while LSTM reached 6.0%. The twofold difference between them creates a severe problem because security teams must handle an excessive number of false positive alerts which disrupt their operations. Auto encoder produces fewer false alarms than Gradient Boosting which has a 4.2% false alarm rate and Random Forest which produces 5.1% false alarms. The Auto encoder system produces operational excellence through its false positive reduction which leads to resource allocation improvements. The error rate analysis presented in **Table 3** further reinforces these findings. Auto encoder reached its best performance with an error rate of 3.4% while LSTM produced a 7.1% error rate which shows a big gap between their reliability. The Auto encoder generates 3.2% false negatives which shows LSTM produces 6.3% false negatives thus making Auto encoder better at detecting actual cyber threats. Critical infrastructure systems need this type of defense because they face the risk of severe operational disruptions and financial damage when attackers manage to bypass their security systems. The Auto encoder produces the most stable results when compared to Random Forest and Gradient Boosting which perform at moderate levels [31].

The detection system requires an urgent solution because its current latency period remains too long for all systems which demand immediate response. According to Table 2, the Auto encoder achieved the fastest detection time of 25 ms, significantly outperforming LSTM (62 ms). The system allows the Auto encoder to detect threats at half the time which leads to quicker threat response and better cyber-attack protection. The system runs Gradient Boosting and Random Forest models at 38 ms and 45 ms respectively which produces adequate results but these models function at slower speeds than the Auto encoder. Small delays in time-critical operations result in increasingly harmful operational failures [32]. The visual patterns support the numerical data from demonstrates that the Auto encoder achieves the lowest error rates in all cases. The Auto encoder separates from LSTM through distinct boundaries which prove that deep learning models produce better results. Auto encoder shows the best performance through its combination of minimum latency and minimum error rate which Figure 2 displays. The model operates with two major benefits which make it the best performing model from our selection of tested models [33].

Conclusion

AI-based systems use Auto encoder models achieve major improvements in detecting cyber threats through their various performance assessment. Auto encoder model achieves better performance than LSTM and Random Forest and Gradient Boosting through its higher accuracy and precision and recall and its improved false positive and negative rates and reduced error rate and faster detection latency. The system shows its actual worth for critical infrastructure protection because it identifies complicated attack patterns while producing the fewest possible false alerts. Artificial data sets the findings prove that detection systems achieve better performance in system reliability and operational efficiency.

References

[1] A. Chehri, I. Fofana, and X. Yang, "Security risk modeling in smart grid critical infrastructures in the era of big data and artificial intelligence," *Sustainability*, vol. 13, no. 6, p. 3196, 2021, doi: 10.3390/su13063196.

[2] A. B'ecue, I. Praça, and J. Gama, "Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities," *Artif. Intell. Rev.*, vol. 54, no. 5, pp. 3849–3886, 2021, doi: 10.1007/s10462-020-09942-2.

[3] E. Vigan`o, M. Loi, and E. Yaghmaei, "Cybersecurity of critical infrastructure," in *The International Library of Ethics, Law and Technology*, Springer, 2020, pp. 157–177. doi: 10.1007/978-3-030-29053-5_8.

[4] I. H. Sarker, M. H. Furhad, and R. Nowrozy, "{AI}-Driven Cybersecurity: An Overview, security intelligence modeling and research directions," *SN Comput. Sci.*, vol. 2, no. 3, 2021, doi: 10.1007/s42979-021-00557-0.

[5] A. Djenna, S. Harous, and D. E. Saidouni, "Internet of Things meet Internet of Threats: New concern Cyber security Issues of critical cyber infrastructure," *Appl. Sci.*, vol. 11, no. 10, p. 4580, 2021, doi: 10.3390/app11104580.

[6] R. Montasari, F. Carroll, S. Macdonald, H. Jahankhani, A. Hosseinian-Far, and A. Daneshkhah, "Application of artificial intelligence and machine learning in producing actionable cyber threat intelligence," in *Advanced Sciences and Technologies for Security Applications*, Springer, 2020, pp. 47–64. doi: 10.1007/978-3-030-60425-7_3.

[7] Z. Chen *et al.*, "A cloud computing based network monitoring and threat detection system for critical infrastructures," *Big Data Res.*, vol. 3, pp. 10–23, 2015, doi: 10.1016/j.bdr.2015.11.002.

[8] P. Radanliev *et al.*, "Cyber risk at the edge: Current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains," *Cybersecurity*, vol. 3, no. 1, 2020, doi: 10.1186/s42400-020-00052-8.

[9] A. Jarrett and K. R. Choo, "The impact of automation and artificial intelligence on digital forensics," *Wiley Interdiscip. Rev. Forensic Sci.*, vol. 3, no. 6, 2021, doi: 10.1002/wfs2.1418.

[10] P. Radanliev *et al.*, "Design of a dynamic and self-adapting system, supported with artificial intelligence, machine learning and real-time intelligence for predictive cyber risk analytics in extreme environments -- cyber risk in the colonisation of Mars," *Saf. Extrem. Environ.*, vol. 2, no. 3, pp. 219–230, 2020, doi: 10.1007/s42797-021-00025-1.

[11] A. Ayodeji, Y. Liu, N. Chao, and L. Yang, "A new perspective towards the development of robust data-driven intrusion detection for industrial control systems," *Nucl. Eng. Technol.*, vol. 52, no. 12, pp. 2687–2698, 2020, doi: 10.1016/j.net.2020.05.012.

[12] L. Haghnegahdar and Y. Wang, "A whale optimization algorithm-trained artificial neural network for smart grid cyber intrusion detection," *Neural Comput. Appl.*, vol. 32, no. 13, pp. 9427–9441, 2019, doi: 10.1007/s00521-019-04453-w.

[13] I. Ghafir *et al.*, "Security threats to critical infrastructure: The human factor," *J. Supercomput.*, vol. 74, no. 10, pp. 4986–5002, 2018, doi: 10.1007/s11227-018-2337-2.

[14] P. Radanliev, D. De Roure, M. Van Kleek, O. Santos, and U. Ani, "Artificial intelligence in cyber physical systems," *AI Soc.*, vol. 36, no. 3, pp. 783–796, 2020, doi: 10.1007/s00146-020-01049-0.

[15] I. Lee, “Cybersecurity: Risk management framework and investment cost analysis,” *Bus. Horiz.*, vol. 64, no. 5, pp. 659–671, 2021, doi: 10.1016/j.bushor.2021.02.022.
[16] S. Gerke, T. Minssen, and G. Cohen, “Ethical and legal challenges of artificial intelligence-driven healthcare,” in *Elsevier eBooks*, Elsevier, 2020, pp. 295–336. doi: 10.1016/B978-0-12-818438-7.00012-5.
[17] D. Mhlanga, “Industry 4.0 in Finance: The impact of Artificial intelligence ({AI}) on digital financial inclusion,” *Int. J. Financ. Stud.*, vol. 8, no. 3, p. 45, 2020, doi: 10.3390/ijfs8030045.
[18] N. J. Daras and M. T. Rassias, *Computation, Cryptography, and Network Security*. Springer, 2015. doi: 10.1007/978-3-319-18275-9.
[19] J. Andraško, M. Mesarč’ik, and O. Hamu\vl’ak, “The regulatory intersections between artificial intelligence, data protection and cyber security: Challenges and opportunities for the {EU} legal framework,” *AI Soc.*, vol. 36, no. 2, pp. 623–636, 2021, doi: 10.1007/s00146-020-01125-5.
[20] D. Chen, P. Wawrzynski, and Z. Lv, “Cyber security in smart cities: A review of deep learning-based applications and case studies,” *Sustain. Cities Soc.*, vol. 66, p. 102655, 2020, doi: 10.1016/j.scs.2020.102655.
[21] P. Radanliev *et al.*, “Artificial intelligence and machine learning in dynamic cyber risk analytics at the edge,” *SN Appl. Sci.*, vol. 2, no. 11, 2020, doi: 10.1007/s42452-020-03559-4.
[22] B. D. Deebak and F. Al-Turjman, “Privacy-preserving in smart contracts using blockchain and artificial intelligence for cyber risk measurements,” *J. Inf. Secur. Appl.*, vol. 58, p. 102749, 2021, doi: 10.1016/j.jisa.2021.102749.
[23] J. Chen, L. Ramanathan, and M. Alazab, “Holistic big data integrated artificial intelligent modeling to improve privacy and security in data management of smart cities,” *Microprocess. Microsyst.*, vol. 81, p. 103722, 2020, doi: 10.1016/j.micpro.2020.103722.
[24] M. Kalech, “Cyber-attack detection in {SCADA} systems using temporal pattern recognition techniques,” *Comput. Secur.*, vol. 84, pp. 225–238, 2019, doi: 10.1016/j.cose.2019.03.007.
[25] U. P. D. Ani, H. He, and A. Tiwari, “Review of cybersecurity issues in industrial critical infrastructure: Manufacturing in perspective,” *J. Cyber Secur. Technol.*, vol. 1, no. 1, pp. 32–74, 2016, doi: 10.1080/23742917.2016.1252211.
[26] B. Mahbooba, M. Timilsina, R. Sahal, and M. Serrano, “Explainable Artificial Intelligence ({XAI}) to Enhance Trust Management in Intrusion Detection Systems Using Decision Tree Model,” *Complexity*, vol. 2021, no. 1, 2021, doi: 10.1155/2021/6634811.
[27] T. Braun, B. C. Fung, F. Iqbal, and B. Shah, “Security and privacy challenges in smart cities,” *Sustain. Cities Soc.*, vol. 39, pp. 499–507, 2018, doi: 10.1016/j.scs.2018.02.039.
[28] N. N. Abbas, T. Ahmed, S. H. U. Shah, M. Omar, and H. W. Park, “Investigating the applications of artificial intelligence in cyber security,” *Scientometrics*, vol. 121, no. 2, pp. 1189–1211, 2019, doi: 10.1007/s11192-019-03222-9.
[29] M. Kuzlu, C. Fair, and O. Guler, “Role of Artificial Intelligence in the Internet of Things ({IoT}) cybersecurity,” *Discov. Internet Things*, vol. 1, no. 1, 2021, doi: 10.1007/s43926-020-00001-4.
[30] W. Ahmad, A. Rasool, A. R. Javed, T. Baker, and Z. Jalil, “Cyber Security in {IoT}-Based Cloud Computing: A Comprehensive survey,” *Electronics*, vol. 11, no. 1, p. 16, 2021, doi: 10.3390/electronics11010016.
[31] P. Trakadas *et al.*, “An Artificial Intelligence-Based Collaboration Approach in Industrial {IoT} manufacturing: Key concepts, architectural extensions and potential applications,” *Sensors*, vol. 20, no. 19, p. 5480, 2020, doi: 10.3390/s20195480.
[32] M. Al-Omari, M. Rawashdeh, F. Qutaishat, M. Alshira’H, and N. Ababneh, “An intelligent Tree-Based Intrusion Detection Model for cyber security,” *J. Netw. Syst. Manag.*, vol. 29, no. 2, 2021, doi: 10.1007/s10922-021-09591-y.
[33] K. Tsiknas, D. Taketzis, K. Demertzis, and C. Skianis, “Cyber Threats to Industrial {IoT}: A survey on attacks and countermeasures,” *IoT*, vol. 2, no. 1, pp. 163–186, 2021, doi: 10.3390/iot2010009.