Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 47 No. 02 (2026)

Analyze and Forecast the Cyber Attack Detection Process Using Machine Learning Techniques

[1]D. Sri Vidya, [2] CH. Rahul, [3] M. Nandhini, [4]P. Alekya, [5] Mrs. T. S. Suhasini

[1,2,3,4]U. G Student, Dept COMPUTER SCIENCE AND ENGINEERING(AI&ML), CMR Engineering College, 1, Medchal Rd, Medchal, KandlaKoya, Seethariguda, Telangana 501401, India

[5]Associate professor, Dept COMPUTER SCIENCE AND ENGINEERING(AI&ML), CMR Engineering College, 1, Medchal Rd, Medchal, KandlaKoya, Seethariguda, Telangana 501401, India

Abstract

This project, titled "Analyze and Forecast the Cyber Attack Detection Process using Machine Learning Techniques", addresses the growing global concern of cybercrime. Cyberattacks cause significant financial losses and their frequency is steadily increasing worldwide. Identifying the criminals and understanding their strategies is essential to strengthen defense mechanisms. Machine learning techniques are applied to analyze real-world data and predict cyber-attack patterns. Five different ML techniques were compared, yielding similar accuracy in detection performance. Among them, the Support Vector Machine (SVM) linear model achieved the highest accuracy rate. The first model provided insights into the types of attacks likely to occur against victims. Logistic Regression proved effective in identifying malicious actors with high success rates. The second model compared offender and victim attributes for predictive identification. Findings show education and wealth reduce victimization risk, making the project valuable for cybercrime departments.

INTRODUCTION

In today's digital era, cyberattacks are becoming increasingly frequent and sophisticated, posing serious threats to individuals, organizations, and governments. Traditional security measures often fail to keep pace with these evolving challenges. Consequently, Machine Learning (ML) has emerged as a powerful approach for detecting and forecasting cyber threats by uncovering hidden patterns and anomalies in large-scale security data. This project leverages ML techniques to improve cyberattack detection and prediction. By applying algorithms such as Decision Trees, Random Forest, Support Vector Machines (SVM), and Deep Learning models, the system can identify suspicious activities and anticipate potential breaches. These models analyze network traffic, system logs, and user behavior to detect anomalies, offering a proactive and intelligent defense mechanism against cyber threats.

LITERATURE SURVEY

Cyber-attacks have emerged as one of the most critical global challenges, causing severe financial losses to individuals, organizations, and nations. Identifying perpetrators and understanding their attack strategies are essential in combating cybercrime, yet detecting and preventing such attacks remains difficult. Recent advancements in Artificial Intelligence (AI) and Machine Learning (ML) have introduced promising models for predicting and detecting cyber threats. Traditional crime prediction methods often fall short in addressing cybercrime effectively; however, utilizing real-world data such as type of crime, gender of perpetrator, damage, and attack methods can significantly improve accuracy. In this project, two ML-based models were analyzed to predict both cyber-attack methods and perpetrators using forensic data from victims. Five ML algorithms were compared, with the Support Vector Machine (SVM) Linear model achieving the highest accuracy rate of 95.02% in predicting attack methods, while Logistic Regression demonstrated 65.42% accuracy in detecting attackers. The second model revealed that the likelihood of victimization decreases with higher education and income levels.

Beyond this study, research in cyber-physical systems (CPS) highlights the importance of AI/ML in safeguarding critical infrastructures, where advanced models like Self-tuned Fuzzy Logic-based Hidden Markov Models (SFL-HMM) combined with optimization algorithms outperform traditional detection techniques. Overall, this project emphasizes the potential of machine learning to provide proactive, intelligent, and effective solutions for cyber-attack detection and future cybersecurity advancements.

EXISTING SYSTEM

Traditional cyber-attack detection systems rely heavily on methods such as intrusion detection systems (IDS), signature-based detection, and firewalls. While these approaches are effective at identifying known threats by matching predefined patterns of malicious behavior, they face significant limitations when dealing with new or evolving attack techniques. Zero-day exploits and sophisticated multi-stage attacks often bypass such systems, exposing their inability to adapt. Moreover, rule-based methods generate a high number of false positives and require frequent manual updates to remain effective. Another drawback is their lack of self-learning capabilities, which prevents them from improving over time. As cyber-attacks grow increasingly complex and diverse, traditional methods alone are no longer sufficient to secure modern networks, making the integration of advanced machine learning techniques essential for enhanced detection and response.

PROPOSED SYSTEM

The proposed system utilizes machine learning (ML) techniques to enhance the detection and prediction of cyber-attacks, overcoming the drawbacks of traditional security methods. By integrating supervised, unsupervised, and deep learning models, it can learn from historical attack data and identify patterns associated with malicious activities. Unlike conventional systems, this ML-based approach is capable of detecting both known and unknown threats, including zero-day exploits and complex multi-stage intrusions. The system continuously updates its models using real-time data, which improves accuracy and minimizes false positives over time. Furthermore, it adopts a hybrid strategy that combines multiple ML algorithms to strengthen adaptability and detection performance. In addition, anomaly detection techniques are employed to identify unusual network behaviors even in the absence of predefined attack signatures, making the system more robust and proactive in securing modern networks.

SYSTEM ARCHITECTURE

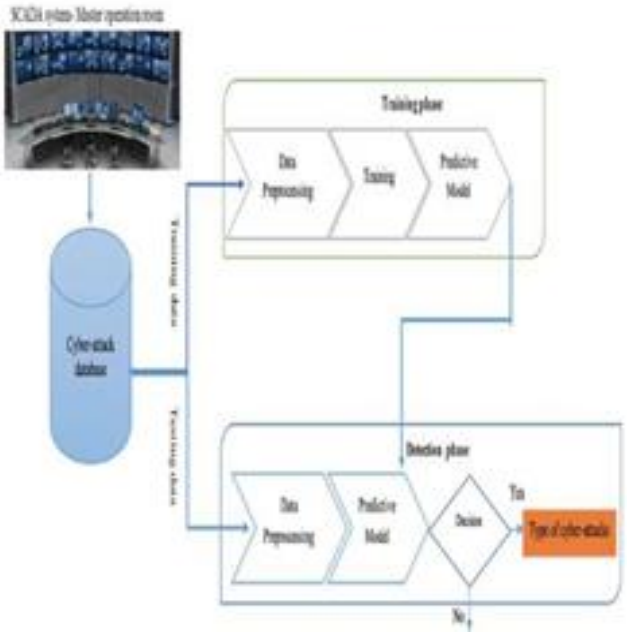

Fig:1 Project Architecture of Analyze and forecast the cyber attack detection process using Machine Learning Techniques

The SCADA system plays a vital role in monitoring and controlling industrial processes, with its master operation room displaying real-time data across multiple monitors. However, cyber-attacks on SCADA systems pose severe risks, as they can disrupt critical operations and essential services. To counter these threats, a centralized cyber-attack database is maintained, storing historical records, network traffic data, system logs, and anomaly reports. This data is divided into training and testing sets to support machine learning applications. In the training phase, raw data undergoes preprocessing, cleaning, and feature extraction, focusing on parameters such as network activity, login attempts, and system behavior. Machine learning models are then trained using algorithms like Random Forest, Support Vector Machines (SVM), Neural Networks, or Deep Learning to build predictive models capable of identifying attack patterns. In the detection phase, real-time data is processed and analyzed by the trained model to detect anomalies or potential intrusions. When an attack is identified, the system proceeds to classification, categorizing threats such as Denial of Service (DoS), malware, or phishing.

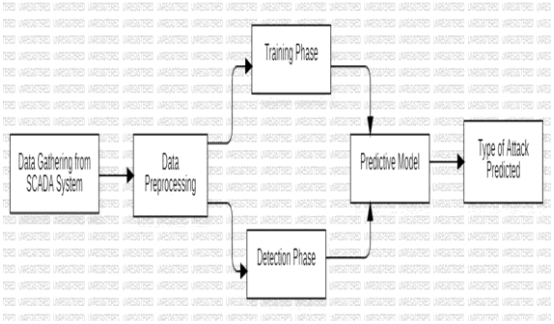

Fig:2 Dataflow Diagram of Analyze and forecast the cyber-attack detection process.

The proposed system applies multiple machine learning algorithms, including XGBoost, RNN/Logistic Regression, Naïve Bayes, Random Forest, and Support Vector Classifier (SVC), to improve cyber-attack detection. XGBoost delivers high accuracy and strong feature extraction but requires high memory and longer training time. RNN with Logistic Regression is simple, fast, and useful for binary classification, though it struggles with complex or multi-class attacks. Naïve Bayes is computationally efficient and suitable for real-time detection, but it performs poorly on zero-day or multi-stage attacks. Random Forest increases detection accuracy and reduces false positives by combining decision trees, but its high computational cost slows predictions. SVC works effectively with high-dimensional data and unseen threats, achieving 88% accuracy, though less than XGBoost. A cyber-attack database supports these models with details on attack types, methods, and victim/attacker attributes. The first model predicts attack strategies using victim-related features such as age, education, income, and occupation.

OUTPUTS

GUI/Main Interface:

In below screen, click on ‘USER’ button for register.

Fig:3 GUI/Main Interface of a Analyze and forecast the cyber-attack detection process using Machine Learning Techniques

User Login Page:

In below screen, User can register first by valid email and mobile to login.

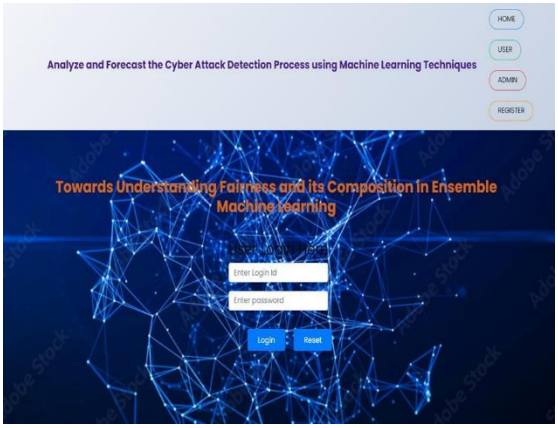

Fig:4 User Login Page of a Analyze and forecast the cyber-attack detection process using Machine learning techniques

Admin Login Page:

In below screen, Admin can login with his details and activate the registered users. Once he activates then only the user can login into our system. Then user can upload the dataset.

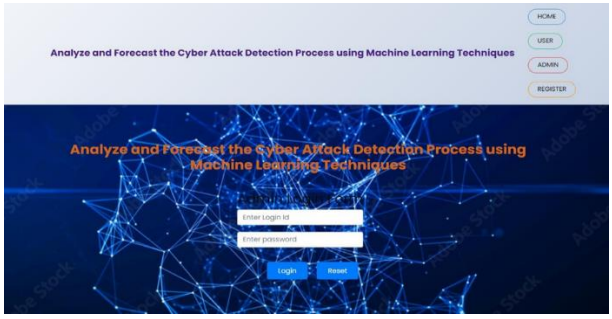

Fig:5 Admin Login Page of a Analyze and forecast the cyber-attack detection process using Machine Learning Techniques.

Users page:

In below screen, Admin can view Users and Overall data in the browser and he load the data.

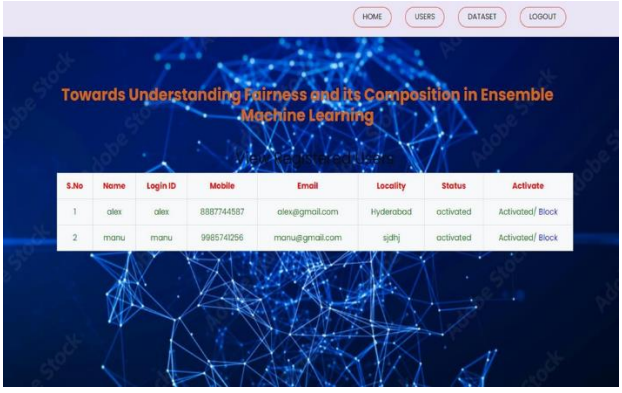

Fig:6 Users page of Analyze and forecast the cyber-attack detection process using Machine Learning Techniques

Prediction Form

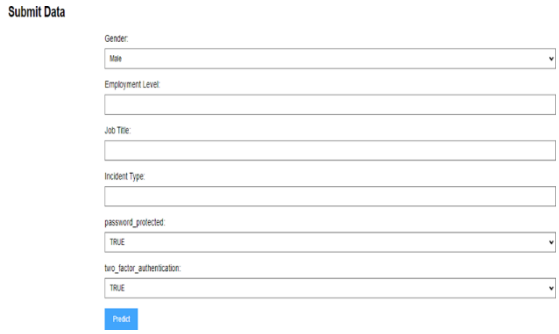

Fig:7 Prediction Form of Analyze and forecast the cyber-attack detection process using Machine Learning Techniques

Output Values

In below screen, The output is displays. It will shows the type of attack. if it is

0- Hacking

1- Phishing

2- Physical Theft

3- Weak Security

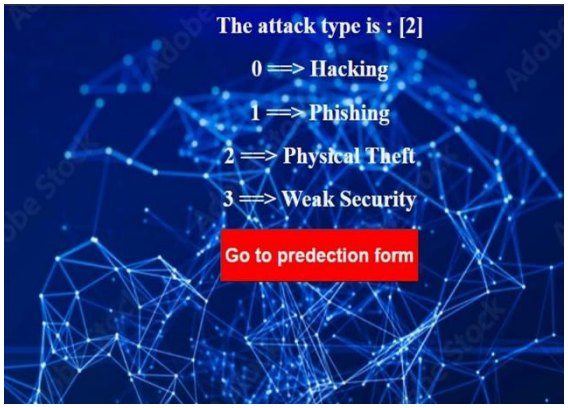

Fig:7 Output values of Analyze and forecast the cyber-attac detection process using Machine Learning Techniques

CONCLUSION

In conclusion, this project has successfully met its objectives, showing notable progress in cyber-attack detection and prevention. The implementation was well-planned and executed, leading to meaningful improvements and insights. Future developments aim to broaden the scope, integrate advanced technologies, and ensure long-term sustainability. Using machine learning algorithms, particularly linear SVMs, the system achieved an accuracy of 61% in identifying potential attackers, though this can be improved with more advanced AI techniques. The study also emphasizes the importance of awareness regarding malware and social engineering threats. It was observed that higher education and wealth levels lower the chances of becoming a victim. By analyzing victim traits, the model can support the design of training and warning systems for individuals at greater risk. The proposed system addresses key limitations of traditional methods, such as high false positives and weak adaptability. With real-time processing and adaptive learning, it minimizes manual intervention and strengthens defenses. As cyber threats continue to grow in complexity, machine learning-driven solutions emerge as a scalable and proactive approach to digital security.

REFERENCE

[1] Bilen, Abdulkadir & Özer, Ahmet. (2021). Cyber-attack method and perpetrator predictionusing machine learning algorithms. PeerJ Computer Science. 7. e475. 10.7717/peerj- cs.475.

[2] Al-majed, Rasha & Ibrahim, Amer & Abualkishik, Abedallah & Mourad, Nahia & Almansour, Faris. (2022). Using machine learning algorithm for detection of cyber-attacks in cyber physical systems. Periodicals of Engineering and Natural Sciences (PEN). 10. 261.10.21533/pen.v10i3.`3035.

[3] Sarker, I.H. Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects.Ann. Data. Sci. (2022). https://doi.org/10.1007/s40745-022-004442

[4] A. Alshehri, N. Khan, A. Alowayr and M. Yahya Alghamdi, "Cyberattack detection framework using machine learning and user behavior analytics," Computer Systems Science and Engineering, vol. 44, no.2, pp. 1679–1689, 2023.

[5] Khuphiran, Panida, et al. "Performance comparison of machine learning models for DDoS attacks detection." 2018 22nd International Computer Science and Engineering Conference.

[6] Ibor, A.E., Oladeji, F.A., Okunoye, O.B. et al. Conceptualisation of Cyberattack prediction with deeplearning. Cybersecurity 3, 14 (2020).

[7] Ahsan, M.; Nygard, K.E.; Gomes, R.; Chowdhury, M.M.; Rifat, N.; Connolly, J.F. Machine Learning Techniques in Cybersecurity. Encyclopedia. Available online: https://encyclopedia.pub/entry/25675 (accessed on 30 April 2023).

[8] Jiang, Y.-G., et al. (2018). Exploiting feature and class relationships in video categorization with regularized deep neural networks. IEEE Transactions on Pattern Analysis and Machine Intelligence.

[9] Rani, S., & Kumar, S. (2019). Survey of intrusion detection systems using machine learning.International Journal of Computer Applications, 975, 8887.

[10] Jha, A., & Kaur, M. (2018). A survey on intrusion detection using machine learning techniques.International Journal of Computer Applications, 975, 8887.

[11] Stojanovic, J., & Sokolovic, B. (2019). Machine learning in cybersecurity: A survey. International Journal of Computer Applications, 975, 8887.

[12] Ahmed, M., & Mahmood, A. N. (2019). A review of machine learning techniques in intrusion detection. International Journal of Computer Applications, 975, 8887.

[13] Liu, H., & Wu, L. (2018). A survey of machine learning for cyber security. International Journal of Information Security, 17(1), 1-14.

[14] Mehmood, A., & Awan, M. (2020). A comprehensive review of machine learning techniques for network intrusion detection systems. Journal of Information Security and Applications, 54, 102522.

[15] Al-Ali, A., & Al-Ghamdi, S. (2020). Anomaly detection for cyber security using machine learning: A survey. Computers & Security, 88, 101633.

[16] Barros, J., & Almeida, R. (2019). Machine learning techniques applied to network intrusion detection systems: A systematic review. Computers & Security, 81, 53-70.

[17] Szewczyk, R., & Bąk, I. (2020). A survey of machine learning techniques for cyber security applications. Computers & Security, 96, 101914.

[18] Dube, P., & Shukla, A. (2020). A survey of machine learning techniques for intrusion detection systems. International Journal of Computer Applications, 975, 8887.