Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 5-A, pp. 1611–1620
DOI : 10.47974/JDMSC-2161

Adaptive machine learning system for cybersecurity threats

Preeti Narooka *
Department of Artificial Intelligence and Machine Learning
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Suchita Arora †
Department of Computer Science and Engineering
Poornima University
Jaipur 303905
Rajasthan
India

Satyajee Srivastava §
School of Engineering and Technology (SET)
Manav Rachna International Institute of Research and Studies
Faridabad 121007
Haryana
India

Mohit Tiwari ‡
Department of Computer Science and Engineering
Bharati Vidyapeeth's College of Engineering
A-4 Rohtak Road
Paschim Vihar 110063
Delhi
India

* *E-mail:* preeti.narooka@jaipur.manipal.edu; (Corresponding author)
preeti.narooka@gmail.com
† *E-mail:* suchita.arora1@poornima.edu.in
§ *E-mail:* drsatyajee@gmail.com
‡ *E-mail:* mohit.tiwari@bharatividyapeeth.edu

© Taru Publications

Sanjay Yadav [@]
Department of Pure and Applied Mathematics
Alliance School of Sciences
Alliance University
Bangalore 562106
Karnataka
India

Abstract

With the proliferation of digital technologies, cybercrime has become a pervasive system where end users, government users and business industries worldwide. Addressing this complex challenge requires innovative approaches that leverage different technologies like machine learning and data science. This abstract presents a machine learning-based computational system designed to combat cybercrime offenses effectively. The proposed system integrates machine learning algorithms with computational systems that find a lot of information and its similar patterns which are the ways of cybercrimes. By leveraging supervised, unsupervised, and reinforcement learning methods, the system can detect anomalies, classify malicious behavior, and predict potential cyber threats in real-time. Cybercrime has become a significant concern in the modern system where most of the users are using digital devices which causes the identity theft to financial fraud. Traditional methods of combating cybercrime are often reactive and fall short in finding the rapidly evolving system of cyber threats. In response, there is a growing interest in developing proactive and intelligent systems to detect, prevent, and mitigate cybercrime offenses. This paper presents a machine learning-based computational system for controlling cybercrime offenses. By seeing the information in the data set it starts learning itself and adapting to emerging threats, the system can effectively detect and reaction on the cyber threats active in the real environment.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *Machine learning, Cybercrime offenses, Cybersecurity, Cyber threats, Pattern recognition, Cybercrime detection methods.*

1. Introduction

Model training involves using historical data to train many learning algorithms which define different recognizing patterns associated with cybercrime offenses. The system's effectiveness relies on its knowledge about the different threats. By leveraging machine learning, the system can evolve over time, becoming more accurate and efficient in detecting cybercrime offenses [1-2]. Most of the information is attacked by threats.

[@] *E-mail:* **sanjay.yadav@alliance.edu.in**

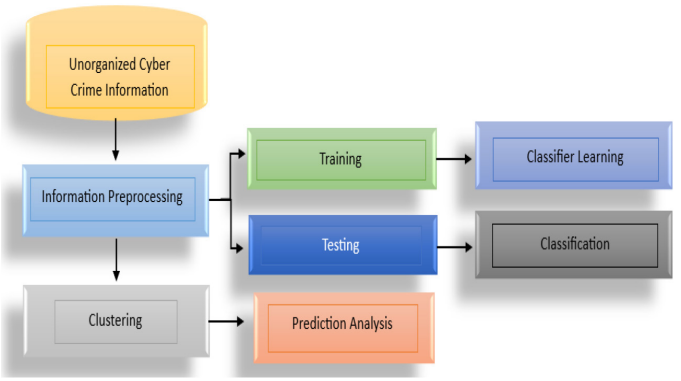

Figure 1

Dataflow diagram of a predictive model

Additionally, the digital environment relates to cloud security to maintain cybersecurity solution as shown with the help of figure 1.

2. Evolution of Machine Learning and Cyber Security in Last Decade

Over the past decade, the convergence of machine learning (ML) and cybersecurity has led to transformative developments in how organizations combat cyber threats [3-4]. Moreover, ML has revolutionized malware detection, enabling automated analysis of file attributes and code behavior to identify and classify malicious software [5-6]. Adversarial machine learning techniques have emerged to counter evolving threats, ensuring that ML-based systems remain effective against sophisticated adversaries defined in figure 2. Integration with threat intelligence feeds has enhanced

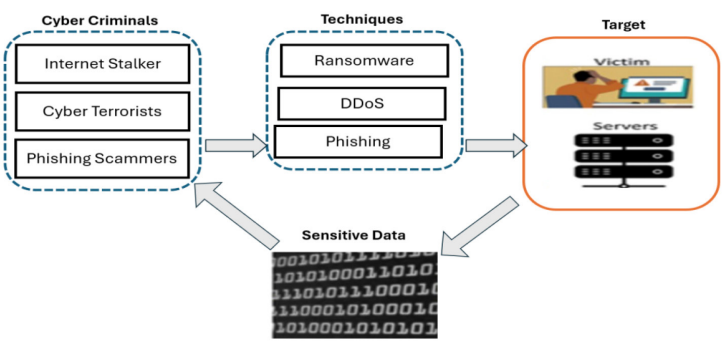

Figure 2

Cyber Security Strategy by using techniques

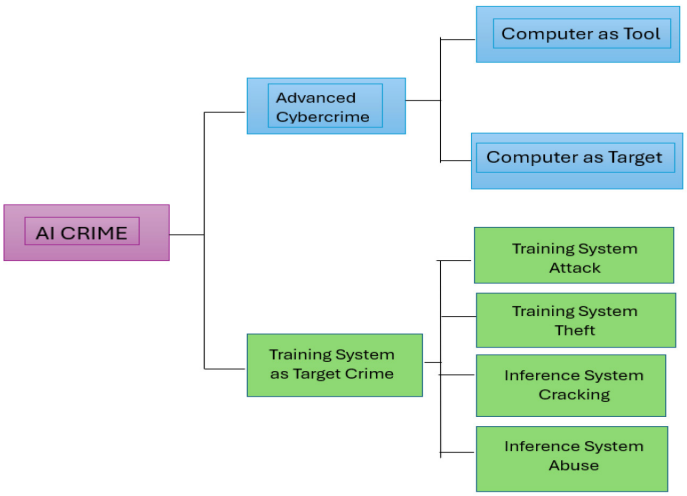

Figure 3

AI Crime Taxonomy

cybersecurity defenses, enabling proactive identification of emerging threats [7-8].

Overall, the literature survey serves as a foundational step in advancing knowledge and developing effective strategies for combating cyber threats through machine learning-based computational systems [9-10].

3. Cyber Crimes: Definition, Issues

Its definition often varies but generally refers to criminal acts committed using computer networks or digital devices [11-12]. These offenses may include but are not limited to hacking, online fraud, malware distribution shown in figure 3. One of the primary issues with cybercrime is its constantly evolving nature [13-14].

4. Classifications of Cybercrime

Combating phishing requires a combination of technical safeguards, user awareness, and vigilance [15-16]. Other preventative measures include verifying the authenticity of websites and emails by checking for HTTPS encryption defined in figure 4 [17-18]. By remaining vigilant and implementing best practices for online security for the end users and the providers to reduce the cyber-crimes and protect the information for the services [19-20].

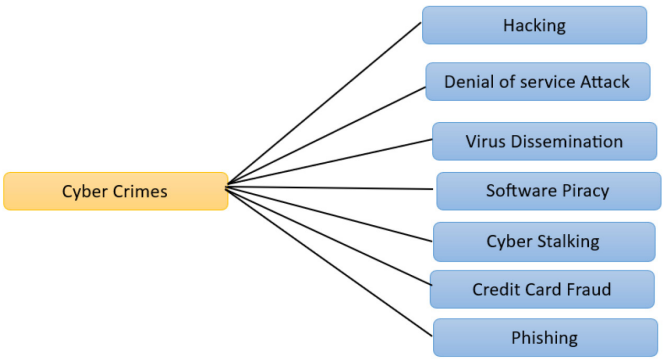

Figure 4
Classification of Cyber Crimes

5. Proposed Idea

A proposed idea for a machine learning-based computational system aimed at controlling cybercrime offenses could involve the development of a comprehensive and proactive cyber threat detection and prevention platform. The Computational Model for Controlling Cybercrime using Machine Learning (CMCCML) is a framework designed to detect, prevent, and mitigate cybercrimes by leveraging advanced machine learning techniques. By leveraging real-time monitoring systems, CMCCML captures data continuously, ensuring that the efficiency is maintained in both ends. Data preprocessing is a crucial step in the CMCCML framework, involving the cleaning and normalization of data to remove noise and ensure consistency. Feature engineering is then applied to extract meaningful features that help in identifying cybercrimes. Feature selection processes, such as correlation analysis and dimensionality reduction, are employed which find the feature selection that enhances the model's efficiency and accuracy.

Algorithm 1 CMCCML (Computational Model for controlling cybercrime using Machine Learning).

Input: Cybersecurity data from various sources.
Output: Selected features for training the machine learning model.
1. **procedure** (Method :)
2. def feature_selection(data):

```
    threshold_correlation = 0.1
    selected_features = [ ]
    preprocessed_data = preprocess_data(data)
    extracted_features = extract_features(preprocessed_data)
    all_features = combine_features(extracted_features)
    correlated_features=correlation_analysis(all_features, threshold_
    correlation)
    optimal_features = recursive_feature_elimination(correlated_
    features)
final_features = apply_regularization(optimal_features)
    reduced_features = apply_dimensionality_reduction(final_
    features)
    model = train_model(reduced_features, data['labels'])
    performance = evaluate_model(model, data['validation'])
    while not converged(performance):
        updated_data = collect_new_data()
        feature_selection(updated_data)
    return final_features
selected_features = feature_selection(cybersecurity_data)
end procedure
```

Anomaly detection techniques, including behavioral analysis, signature-based detection, and heuristic-based detection, are integral to the framework, allowing for the identification of deviations from normal patterns and known attack signatures. This algorithm outlines a systematic approach to feature selection in the CMCCML framework, ensuring that the most relevant features are utilized for detecting and controlling cybercrimes, thereby improving the model's performance and accuracy defined in figure 5. To enhance the effectiveness of the system, continuous

	support	F1-score	precision	recall
Identity Theft	241	0.99	1.00	0.99
Copyright attack	95	0.98	0.97	1.00
Hacking	84	1.00	1.00	1.00
Avg/total	420	0.99	0.99	0.99

Figure 5

Adaptive impact of machine learning and cybercrime with respect to time

monitoring and evaluation would be essential to assess its performance, identify areas for improvement, and refine the machine learning models and algorithms over time.

The proposed algorithm defines the learning system for controlling cybercrime offenses by leveraging advanced algorithms to analyze and predict cyber threats. By leveraging the power of machine learning, this system could help mitigate the risks associated with cybercrime and protect individuals and organizations from the growing threat of cyber-attacks.

6. Result Analysis

The outcome of the proposed algorithm computes all the cyber security parameters in an effective manner.

The proposed system aim is to identify the information which is detected and prevented from the various forms of cybercrime, including fraud, hacking, and phishing attacks defined in figure 6. The result analysis of a machine learning-based computational system for controlling

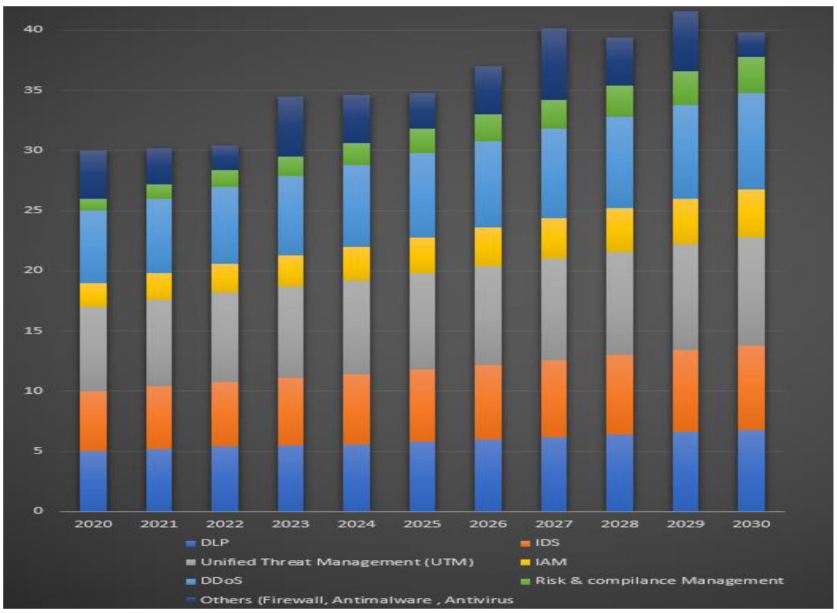

Figure 6

Analysis of statistical impact of machine learning and cybercrime with respect to time

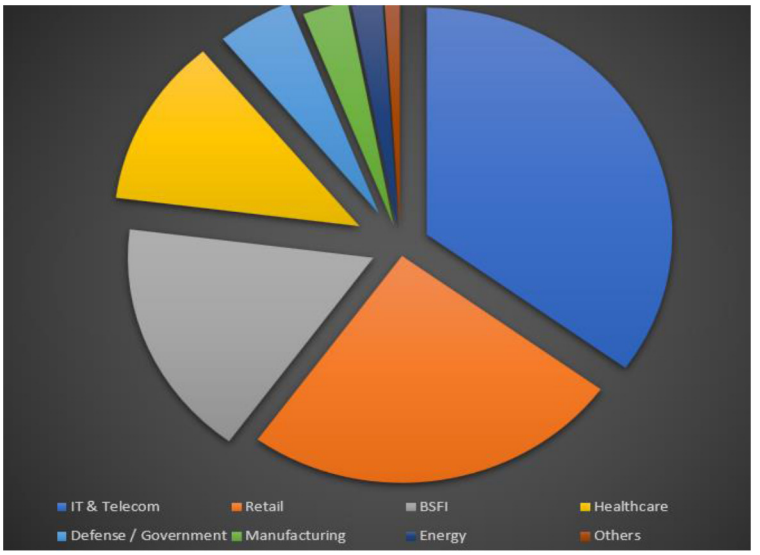

Figure 7

Multi-dimensional cybersecurity measures

cybercrime offenses involves evaluating its performance, effectiveness, and impact in mitigating cyber threats defined in figure 7.

7. Conclusion and Future Work

The research article dealing with the learning algorithm in computational system for controlling cybercrime offenses represents a promising approach to enhancing cybersecurity efforts. In summary, while machine learning-based computational systems have made significant strides in controlling cybercrime offenses, there is still much work to be done to realize their full potential. There are several challenges which are being solved using the prosed system.

References

[1] R. Kaur, D. Gabrijelčič, and T. Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions," *Information Fusion*, vol. 101804 (2023).

[2] L. Elluri, V. Mandalapu, P. Vyas, and N. Roy, "Recent Advancements in Machine Learning for Cybercrime Prediction," *J. Comput. Inf. Syst.*, pp. 1–15 (2023).

[3] I. H. Sarker, "Machine learning for intelligent data analysis and automation in cybersecurity: current and future prospects," *Ann. Data Sci.*, vol. 10, no. 6, pp. 1473–1498 (2023).

[4] A. Tiwari and R. M. Sharma, "Realm Towards Service Optimization in Fog Computing," in Research Anthology on Architectures, Frameworks, and Integration Strategies for Distributed and Cloud Computing, IGI Global, pp. 1530–1563 (2021).

[5] D. Dudeja, A. Gupta, R. Dhanjani, and P. J. Shah, "Sales-based models for resource management and scheduling in artificial intelligence systems," *Engineering Proceedings*, vol. 59, no. 1, p. 43 (2023).

[6] A. Tiwari, N. Gupta, S. Mishra, and R. Srivastava, "Efficient cloud orchestration services in computing," in Proceedings of the 3rd International Conference on Machine Learning, Advances in Computing, Renewable Energy and Communication (MARC 2021), Springer Nature Singapore, pp. 739–746 (Sep. 2022).

[7] R. Manikandan, M. M. Sathik, and R. Ranjith, "Adaptive cloud orchestration resource selection using rough set theory," *Journal of Interdisciplinary Mathematics,* vol. 26, pp. 311–320 (2023).

[8] C. T. Dora Pravina, A. J. L. Lavanya, and R. R. J. Priyanka, "A sustainable and secure cloud resource provisioning system in Industrial Internet of Things (IIoT) based on image encryption," in Proceedings of the 4th International Conference on Information Management and Machine Intelligence, pp. 1–5 (Dec. 2022).

[9] S. Rani and S. Babbar, "Emerging Global Cyber Security Trends in Sustainable Business Practices," *MSW Manag. J.,* vol. 33, no. 1, pp. 109–120 (2023).

[10] A. Tiwari and R. Garg, "Adaptive ontology-based IoT resource provisioning in computing systems," *Int. J. Semant. Web Inf. Syst*., vol. 18, no. 1, pp. 1–18 (2022).

[11] K. Chakraborty et al., "Multilevel Cloud resource Scheduling approach based on image-based signature system," in Proc. 5th Int. Conf. Inf. Manag. Mach. Intell., pp. 1–7 (Nov. 2023).

[12] G. K. Arora, M. Singh, A. Jindal, and V. Khetani, "Multi-objective Eagle optimization feature selection for cloud systems," in *Computer Science Engineering and Emerging Technologies*, CRC Press, pp. 690–696 (2024).

[13] S. Kumar, R. Sharma, V. Khetani, and D. Dhabliya, "Detection of recurring vulnerabilities in computing services," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 25, no. 4, pp. 1063–1071 (2022).

[14] S. Kumar, R. Sharma, V. Khetani, and D. Dhabliya, "Protecting location privacy in cloud services," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 25, no. 4, pp. 1053–1062 (2022).

[15] S. Kumar, H. Gautam, S. Singh, and M. Shafeeq, "Top Vulnerabilities in Cloud Computing," *ECS Trans.,* vol. 107, no. 1, p. 16887 (2022).

[16] Y. V. Rangaiah, P. Yalamanchili, and P. C. S. Reddy, "A taxonomy towards blockchain-based multimedia content security," in Proceedings of the 2022 2nd International Conference on Innovative Sustainable Computational Technologies (CISCT), pp. 1–4 (Dec. 2022).

[17] N. K. Singh, A. Kumar, R. Rani, and A. K. Tripathi, "Attack detection taxonomy system in cloud services," in Proceedings of the 2022 2nd International Conference on Innovative Sustainable Computational Technologies (CISCT), pp. 1–5 (Dec. 2022).

[18] A. Tiwari and R. Garg, "Reservation System for Cloud Computing Resources (RSCC): Immediate Reservation of the Computing Mechanism," *Int. J. Cloud Appl. Comput.,* vol. 12, no. 1, pp. 1–22 (2022).

[19] A. Tiwari and R. M. Sharma, "Potent cloud services utilization with efficient revised rough set optimization service parameters," in Proc. Int. Conf. Adv. Inf. Commun. Technol. Comput., pp. 1–7 (Aug. 2016).

[20] A. Tiwari and R. M. Sharma, "Realm Towards Service Optimization in Fog Computing," in Research Anthology on Architectures, Frameworks, and Integration Strategies for Distributed and Cloud Computing, IGI Global, pp. 1530–1563 (2021).

Received November, 2024