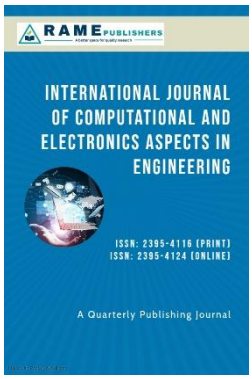
International Journal of Computational and Electronic Aspects in Engineering
Volume 7, Issue 3, July 2026, pp 30-36
Special Issue of National Conference on Emerging Innovative Trends in Computer Applications
https://doi.org/10.26706/ijceae.7.3.20260705

Cybercrime Detection and Prevention

Rupesh Bangre, Neha Chaudhari, Minakshi Hirwani, Ayushi Date

MCA, Suryodaya College of Engineering and Technology, Nagpur, India

Correspondence: rupesh.rpb@gmail.com



Abstract: Cybercrime has emerged as a serious and growing threat to individuals, organizations, and governments worldwide. It includes a wide range of malicious activities such as hacking, phishing, ransomware attacks, and financial fraud, all of which contribute to substantial financial losses each year. This paper provides a comprehensive overview of cybercrime, discussing its various forms and the techniques used for its detection, including tripwires, honeypots, anomaly detection systems, and operating system commands. It also explores preventive strategies and highlights relevant legal frameworks, particularly the IT Act of 2000. In addition, the paper introduces a hybrid detection model that integrates Random Forest, LSTM, and XGBoost algorithms with Apache Spark to enable real-time threat detection. By blending conventional security methods with advanced AI-driven approaches, the proposed system improves accuracy, scalability, and adaptability, making it more effective in addressing the constantly evolving nature of cyber threats.

Keywords: Cyber Crime, Cyber Security, Honey pots, Trip wires, Anomaly detection, Operating system commands.

1. Introduction

Cybercrime has emerged as a pervasive and escalating global threat, encompassing a diverse array of illicit activities conducted via digital networks, including unauthorized hacking, data breaches, and sophisticated financial fraud. As global reliance on interconnected digital infrastructure continues to expand, these malicious activities pose critical risks to the security and stability of individuals, private organizations, and national governments. The increasing complexity of cyber-attacks not only facilitates substantial annual financial losses but also jeopardizes the integrity of personal information and critical infrastructure. [8]

1.1 Historical Context and Origin

The genesis of cybercrime is inextricably linked to the evolution of computational systems. Early conceptual milestones, such as Charles Babbage's Analytical Engine, laid the foundational principles for modern computing; however, these advancements concurrently introduced unprecedented vulnerabilities that paved the way for technological exploitation. As computing transitioned from centralized mainframes to distributed networks, the potential for digital malfeasance grew exponentially. [5]

1.2 Paradigms of Cybersecurity

In the contemporary digital landscape, systemic challenges such as viral propagation, unsolicited spam, and targeted persistent threats are ubiquitous. Cybersecurity functions as the primary defensive framework designed to safeguard systems, networks, and sensitive data from compromise. By implementing robust security protocols, organizations can ensure the confidentiality, integrity, and availability of information in an increasingly hostile online environment. [7][8].

Article – Peer Reviewed
Received: 1 March 2026
Accepted: 30 June 2026
Published: 31 July 2026

Cite this article: Rupesh Bangre , Neha Chaudhari, Minakshi Hirwani, Ayushi Date, “Cybercrime Detection and Prevention”, *International Journal of Computational and Electronic Aspects in Engineering*, vol. 7, issue 3, pp. 30-36, 2026.
https://doi.org/10.26706/ijceae.7.3.20260705

1.3 The Imperative for Robust Cybersecurity

The necessity for comprehensive cybersecurity measures is driven by the urgent need to protect sensitive personal data and maintain individual privacy against intrusive attacks. Furthermore, robust security frameworks are essential to mitigate the deleterious effects of malware, ransomware, and unauthorized intrusions, which otherwise threaten the functional continuity of modern society. [7][8]

2. Types of cyber crime

Cybercrime manifests in several distinct forms, each posing unique threats to digital security and privacy.

Table 1: Types of Cyber Crime and Descriptions

Financial	Using fake websites to market products so as to get the credit numbers [7]
Marketing Strategies	Selling narcotics or weapons online [7]
Intellectual Property	Software piracy, copyright infringement, trademark, theft of the computer code [7]
Email spoofing	Hacking email/password; sending unwanted message to others [8].
E-Murder	Manipulating medical records [8].
Transfer Fraud	Hackers intercept them and divert the funds [8].

3. Electronic Crime Detection

Cybercrime detection involves continuous monitoring of system resources, network traffic, and user behavior to identify potential threats or unusual activities. Effective detection acts as the first line of defense in maintaining system integrity. [7][8]

3.1 Tripwires

Tripwires function as early-warning systems that monitor critical files or registry settings. By establishing a baseline of known-good system states, they compare current data against this baseline; any unauthorized modification triggers an immediate alert, allowing security teams to respond to potential tampering before further damage occurs. [8]

3.2 Configuration Tools

Configuration tools are essential for system hardening. They systematically assess system settings, services, and policies against security benchmarks to identify misconfigurations, outdated software, or vulnerabilities that could be exploited by attackers. Regular audits with these tools help maintain a secure baseline. [8]

3.3 Honeypots

Honeypots are deceptive systems designed to mimic legitimate targets. By luring attackers into these isolated, monitored environments, security teams can observe their tools, techniques, and procedures (TTPs) without risking the actual production environment. This provides invaluable threat intelligence. [7]

3.4 Anomaly Detection

This approach creates a statistical baseline of "normal" user behavior or network traffic. Using machine learning or heuristic analysis, the system flags deviations from this norm, such as unexpected data exfiltration or unusual login times, which may indicate an ongoing breach or insider threat. [9]

3.5 OS Commands

System-level analysis involves utilizing native operating system commands and log file inspection to detect suspicious activity. Security analysts manually or automatically parse logs, audit running processes, monitor open network ports, and verify user permissions to spot evidence of intrusion or unauthorized access. [9]

4. Different legal acts against cyber crime

"There can be no peace without justice, no justice without law, and no real value of law without a system that determines what is fair and lawful in different situations," said Benjamin B. Ferencz. Similarly, Mahatma Gandhi stated, "We get the Government we deserve. When we improve, the Government is also bound to improve." These statements highlight the crucial role of a strong and effective legal system in any society. It is the government's responsibility to ensure that laws evolve alongside rapid scientific and technological advancements and are properly enforced.

With the surge in cybercrime cases, many countries have enacted specific laws to regulate and prevent such activities. Some notable legal frameworks addressing cybercrime include:

- The India Information Technology Act of 2000
- The Philippines Electronic Commerce Act No. 8792 of 2000
- The Philippines Cybercrime Prevention Act of 2012 No. 10175
- USA Cyber Intelligence Sharing and Protection Act of 2011 (CISPA)
- USA Cyber Security Enhancement Act of 2009 (S.773)

Table 2: Cyber Offences and Corresponding Sections under the IT Act

Offence	Section under IT Act
Tampering with Computer source documents	Sec.65
Hacking with Computer systems, Data alteration	Sec.66
Publishing obscene information	Sec.67
Un-authorized access to protected system	Sec.70
Breach of Confidentiality and Privacy	Sec.72
Publishing false digital signature certificates	Sec.73

NOTE: Sec.78 of I.T. Act empowers Deputy Superintendent of Police to investigate cases falling under this Act. Computer Related Crimes Covered under Indian Penal Code and Special Laws.

5. Architecture of Cybercrime Detection and Prevention

This system is designed in different layers to collect data, analyze it, and respond to cyber threats. It runs continuously to keep the system secure. [1][2][3]

1. Data Collection Layer
Collects data from system logs, user activity, and other sources in one place.

2. Data Preprocessing Layer
Cleans and arranges the data so it is ready for use.

3. Detection Layer
Uses multiple models together to identify suspicious activities.

4. Detection Output Layer
Generates alerts and reports when any threat is detected.

5. Monitoring & Response Layer
Takes quick actions like blocking access or isolating affected systems.

6. Threat Intelligence Layer
Shares threat details with security systems and legal authorities.

7. Feedback Layer
Continuously updates and improves the system based on new threats

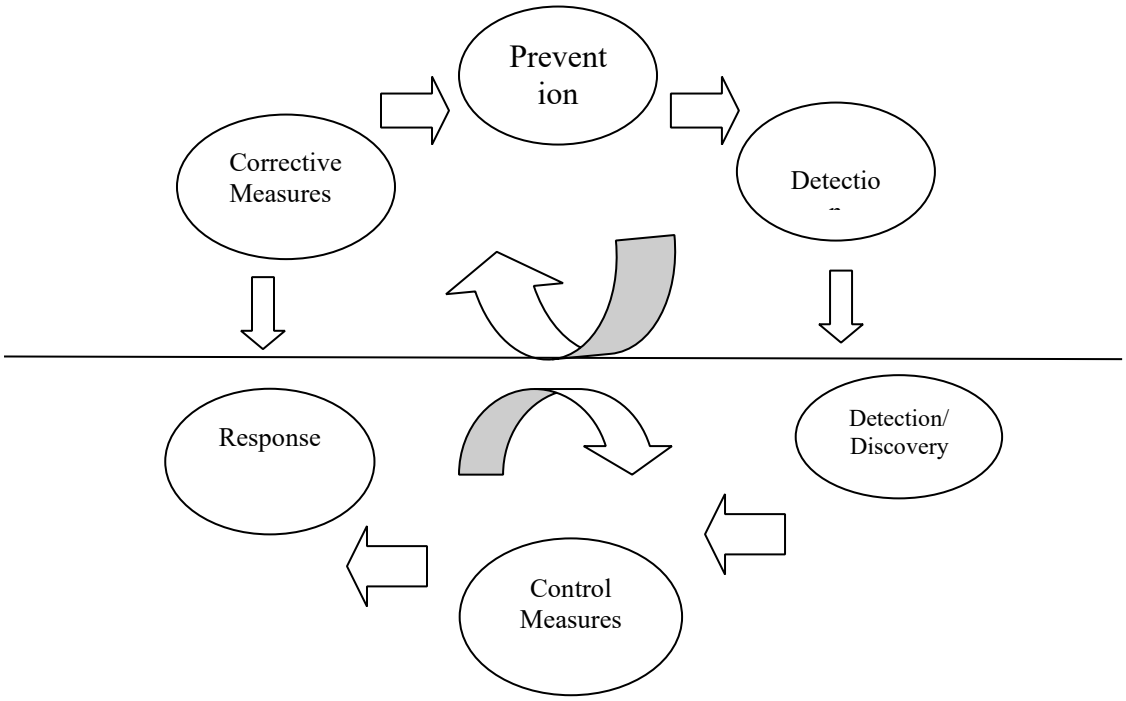


Figure 1: Cybercrime Detection and Prevention Architecture

6. Methodological Approach

6.1 Proposed Framework

The system uses a combination of Random Forest, LSTM, and XGBoost to improve cybercrime detection. Random Forest helps in selecting important data, LSTM analyzes patterns over time, and XGBoost improves the final results. Together, they make the system more accurate and reliable. [1][2][3]

6.2 Data Preparation

Before training, the data is cleaned and properly organized. It is arranged in a way that helps in understanding patterns, especially for time-based data. [1][2]

6.3 Model Integration

- Random Forest: Used to select important features
- LSTM: Used to find patterns in sequence data
- XGBoost: Used to give final prediction results [1][3]

6.4 Training and Evaluation

The model is built using Python tools and trained using suitable methods. Its performance is measured using accuracy, precision, recall, and F1-score. [2][3]

7. Challenges of Cybercrime Detection and Prevention

The hybrid model using Random Forest, LSTM, and XGBoost improves accuracy by combining different methods and handling data effectively. [1][3][4]

Apache Spark helps in processing large data faster, but there are still challenges like high computational cost and difficulty in real-world use.

In the future, more simple and flexible models are needed to make cybercrime detection better. [1][3][4]

8. Future Directions / Research Gaps

A. Real-Time Protection

Future systems should focus on detecting and preventing cyber-attacks instantly, rather than responding only after damage has occurred. Rapid detection and immediate response are crucial for reducing risks and minimizing potential losses.

B. Data Privacy Protection

There is an increasing need for advanced methods that safeguard user data while still allowing effective cyber threat detection. Striking a balance between privacy and security remains a key area of research.

C. Lightweight Security Tools

Security solutions should be designed to operate efficiently on devices with limited resources, such as IoT devices and mobile phones. These tools must provide strong protection while consuming minimal power and memory. **[1][2]**.

9. Result And Discussion

To evaluate the performance of the proposed framework, the hybrid model was tested against several individual machine learning algorithms, including Random Forest, LSTM, and XGBoost. This comparative analysis demonstrates the efficacy of the integrated approach in achieving superior detection accuracy and reliability across multiple evaluation metrics.

The table below compares how different models perform in cybercrime detection using key evaluation parameters:

Table 3: Comparative Performance of Detection Models

Sr. No.	Model Used	Precision (%)	Recall (%)	F1-Score (%)	Accuracy (%)
1	Random Forest	92	90	91	93
2	LSTM	94	93	93.5	95
3	XGBoost	95	94	94.5	96
4	Hybrid Model (RF + LSTM + XGBoost)	97	96	96.5	98

Discussion

The results show that the Hybrid Model, which combines Random Forest, LSTM, and XGBoost, performs the best, reaching 98% accuracy. Each model helps in its own way: Random Forest picks out important features, LSTM finds patterns over time, and XGBoost makes predictions more accurate. The individual models also work well, but their accuracy is a little lower.

Although the hybrid model needs more computing power, it is still reliable and can be used effectively for real-time cybercrime detection.

10. Conclusion

Cybercrime is constantly evolving and remains a serious threat to individuals, businesses, and governments. Effectively managing these threats requires a combination of robust preventive measures and advanced technologies capable of detecting attacks in real time. Integrating modern AI-based tools with traditional security methods enhances both the speed and accuracy of cyber threat detection. Ongoing research, collaboration, and awareness are essential for maintaining a secure digital environment and minimizing the risk of data breaches and financial losses.

References

[1] Y. Zhang, X. Li, and H. Chen, "Predicting server failures with big data log mining," *Journal of Cloud Computing*, vol. 11, no. 4, pp. 1–14, 2022.

[2] R. Kumar and P. Singh, "Machine learning approaches for early detection of server crashes," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 12, no. 7, pp. 45–52, 2021.

[3] J. Liu, Z. Wang, and Q. Zhou, "Anomaly detection in cloud systems using isolation forest and Spark," *IEEE Access*, vol. 9, pp. 12345–12356, 2021.

[4] Y. Chen and L. Zhao, "Big data analytics for predictive maintenance in cloud environments," *Future Generation Computer Systems*, vol. 124, pp. 234–246, 2021.

[5] J. Friedman, T. Hastie, and R. Tibshirani, *The Elements of Statistical Learning*, 2nd ed. Springer, 2009.

[6] L. Breiman, "Random forests," *Machine Learning*, vol. 45, pp. 5–32, 2001.

[7] S. Behal and R. Sharma, "Cybercrime: Types, detection, and prevention techniques," *International Journal of Computer Applications*, vol. 175, no. 33, pp. 12–21, 2020.

[8] S. Islam and M. Shah, "A review of cybercrime detection techniques," *Journal of Information Security and Applications*, vol. 45, pp. 36–50, 2019.

[9] S. Bhattacharya and S. Bansal, "Anomaly-based intrusion detection system using machine learning for cybersecurity," *Journal of Cyber Security and Mobility*, vol. 10, no. 2, pp. 101–120, 2021.

[10] W. Stallings, *Computer Security: Principles and Practice*, 4th ed. Pearson, 2018.

[11] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. MIT Press, 2016.

[12] S. Hochreiter and J. Schmidhuber, "Long short-term memory networks," *Neural Computation*, vol. 9, no. 8, pp. 1735–1780, 1997.

[13] T. Chen and C. Guestrin, "XGBoost: A scalable and efficient tree boosting system," in *Proceedings of the ACM SIGKDD Conference*, 2016, pp. 785–794.

[14] R. Sommer and V. Paxson, "On the use of machine learning for network intrusion detection," in *Proceedings of the IEEE Symposium on Security and Privacy*, 2010, pp. 305–316.

[15] A. Patcha and J. M. Park, "An overview of anomaly detection techniques and current trends," *Computer Networks*, vol. 51, no. 12, pp. 3448–3470, 2007.

[16] D. E. Denning, "An intrusion detection model for secure systems," *IEEE Transactions on Software Engineering*, vol. SE-13, no. 2, pp. 222–232, 1987.

[17] S. Axelsson, "Intrusion detection systems: Survey and classification," Technical Report, Chalmers University, 2000.

[18] K. Scarfone and P. Mell, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, NIST Special Publication 800-94, 2007.

[19] C. Modi *et al.*, "A survey of intrusion detection techniques in cloud computing environments," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 42–57, 2013.

[20] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: Concepts and techniques," *ACM Computing Surveys*, vol. 41, no. 3, pp. 1–58, 2009.

[21] M. Tavallaee *et al.*, "Analysis of the KDD CUP 99 dataset for intrusion detection," in *Proceedings of IEEE CISDA*, 2009, pp. 1–6.

[22] A. L. Buczak and E. Guven, "Survey of data mining and machine learning methods for cybersecurity intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.

[23] S. Sahu and B. Mehtre, "Machine learning-based network intrusion detection system," *Procedia Computer Science*, vol. 45, pp. 202–210, 2015.

[24] S. Aljawarneh *et al.*, "An anomaly-based intrusion detection system using feature selection techniques," *Future Generation Computer Systems*, vol. 80, pp. 548–562, 2018.

[25] A. Javaid *et al.*, "Deep learning-based intrusion detection system for network security," *Procedia Computer Science*, vol. 103, pp. 101–108, 2016.

[26] G. Kim *et al.*, "Long-term anomaly detection in network traffic data," *Computers & Security*, vol. 44, pp. 33–44, 2014.

[27] K. Singh and P. Singh, "Cyber attack detection using machine learning techniques," *International Journal of Information Security*, vol. 19, no. 3, pp. 321–335, 2020.

[28] B. Gupta *et al.*, "Machine learning approaches for intrusion detection systems," *IEEE Access*, vol. 6, pp. 1–15, 2018.

[29] A. Sharma *et al.*, "Artificial intelligence applications in cybersecurity," *Journal of Ambient Intelligence and Humanized Computing*, vol. 13, no. 4, pp. 567–580, 2021.

[30] R. Verma and A. Das, "Recent trends and prevention techniques in cybercrime," *Journal of Cybersecurity*, vol. 8, no. 1, pp. 1–15, 2022.