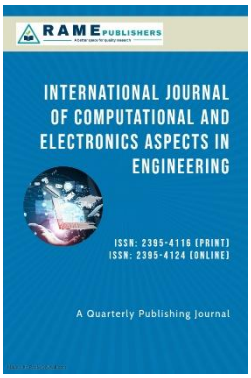
International Journal of Computational and Electronic Aspects in Engineering
Volume 7, Issue 3, July 2026, pp 22-29
Special Issue of National Conference on Emerging Innovative Trends in Computer Applications
https://doi.org/10.26706/ijceae.7.3.20260704

Cybercrime Detection and Prevention: A Human-Centric Approach

Rupesh Bangre, Nikhil Tiwari*, Rupam Shrivastava, Heena Kashi

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

*Correspondence: nikhilbaba131@gmail.com



Abstract- Cybercrime has become one of the most serious challenges in the digital era. With the rapid growth of the internet, cloud computing, mobile devices and online services, criminals are continuously finding new ways to exploit systems, steal data and harm individuals as well as organizations. This research paper focuses on cybercrime detection and prevention using a human-centric and practical approach. Instead of relying only on automated systems, this paper highlights the importance of combining technology, human awareness, policies and ethical practices. The study discusses types of cybercrimes, detection techniques, prevention strategies, challenges and future scope. Simple explanations and diagrams are used to make the concepts easy to understand and suitable for academic evaluation.

Keywords- Cybercrime, Detection Techniques, Prevention Strategies, Cyber Security, Intrusion Detection System

1. Introduction

In today's digital world, information technology has become a part of our everyday lives. From online banking and shopping to healthcare, education, social media and even government services, we rely heavily on computers, mobile devices and the internet. While these technologies make life faster, easier and more connected, they also bring serious risks. One of the biggest challenges we face today is cybercrime, which affects individuals, businesses and governments across the globe [1-5].

Cybercrime involves illegal activities carried out using computers, networks, or the internet. The goal is often to steal sensitive information, cause financial damage, disrupt systems, or invade people's privacy. Common examples include phishing scams, identity theft, malware attacks, ransomware, data breaches and even cyber terrorism. As technology becomes more advanced, these threats are also becoming more frequent and complex, making it clear that traditional security methods alone are no longer enough [6-10].

To deal with this growing problem, cybercrime detection and prevention have become extremely important. Detection focuses on identifying suspicious activities within systems, while prevention aims to reduce risks and stop attacks before they happen. However, technology alone cannot fully solve the problem. Many cyberattacks succeed because of human mistakes such as lack of awareness, weak passwords, careless behaviour, or poor security policies [11-15].

For this reason, this research paper takes a human-centric approach to cybercrime detection and prevention. Along with technical solutions like intrusion detection systems, machine learning and encryption, it highlights the importance of user awareness, proper training, strong organizational policies and ethical practices. By combining advanced technology with responsible human behaviour, we can build a safer and more effective cyber security environment [16-20].

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

Cite this article: Rupesh Bangre, Nikhil Tiwari*, Rupam Shrivastava, Heena Kashi, "Cybercrime Detection and Prevention: A Human-Centric Approach", *International Journal of Computational and Electronic Aspects in Engineering*, vol. 7, issue 3, pp. 22-29, 2026.
https://doi.org/10.26706/ijceae.7.3.20260704

1.1. Objectives of the Study

The main objectives of this research paper are as follows:

- To develop a clear understanding of cybercrime and its different types.
- To explore various techniques used for detecting cybercrime.
- To examine the prevention methods applied in real-world systems.
- To identify the key challenges involved in detecting and preventing cybercrime.
- To discuss future trends and possible improvements in the field of cybersecurity.

2. Types of Cybercrime

Cybercrime can be better understood by classifying it based on the target and the method used by attackers. This classification helps in identifying the nature of threats and taking appropriate preventive measures.

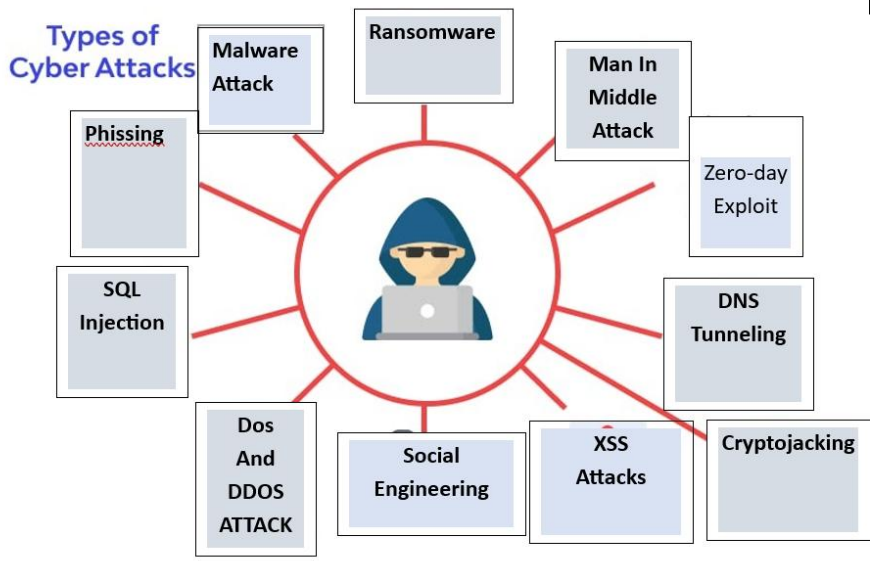


Figure 1 Types of Cybercrime

2.1 Cybercrime Against Individuals

This type of cybercrime focuses on targeting individual users. It includes activities such as identity theft, online fraud, cyberstalking, phishing, and email scams. Attackers often exploit human weaknesses like a lack of awareness, weak passwords, or careless online behavior, making individuals easy targets.

2.2 Cybercrime Against Organizations

Organizations are frequently targeted to gain financial benefits or to disrupt their operations. Common forms of attacks include data breaches, ransomware, insider threats and denial-of-service (DoS) attacks. These incidents can result in heavy financial losses and may also harm the organization's reputation and customer trust.

2.3 Cybercrime Against Government and Society

This category involves attacks directed at government systems or society at large. Examples include cyber terrorism, attacks on critical infrastructure, spreading false information and hacking government databases. Such activities can pose serious threats to national security, disrupt essential services and create fear and instability among the public.

Table 1. Classification of Cybercrime Types

Category	Target	Examples	Impact
Cybercrime Against Individuals	Personal users	Phishing, Identity Theft, Online Fraud	Financial loss, privacy breach
Cybercrime Against Organizations	Companies, Institutions	Ransomware, Data Breach, DoS Attack	Revenue loss, reputation damage
Cybercrime Against Government & Society	Government systems, Public	Cyber Terrorism, Website Hacking	National security threat

These include cyber terrorism, hacking of government websites, spreading fake information and attacks on critical infrastructure. Such crimes can impact national security [3],[4],[21].

3. Cybercrime Detection Techniques

Cybercrime detection is the process of identifying suspicious or malicious activities within a computer system or network. These detection methods can generally be divided into traditional approaches and more advanced, intelligent techniques.

3.1 Signature-Based Detection

This method works by comparing system activities with a database of known attack patterns, also called signatures. If a match is found, the system identifies it as a threat. While this approach is very effective for detecting known attacks, it has a major limitation—it cannot identify new or unknown threats that do not match existing signatures.

3.2 Anomaly-Based Detection

Anomaly-based detection focuses on identifying unusual behaviour. It works by first understanding what "normal" system activity looks like and then comparing current behaviour against this baseline. If there is a significant deviation, it is flagged as suspicious. This method is useful for detecting new or unknown attacks, but it may sometimes produce false alarms.

3.3 Intrusion Detection Systems (IDS)

An Intrusion Detection System (IDS) is designed to continuously monitor network traffic and system activities to identify potential security breaches. It acts as a security layer that alerts administrators whenever suspicious activity or possible intrusions are detected

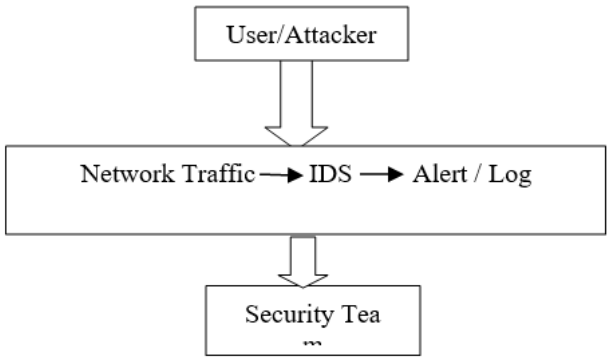


Figure 2 Basic Working of Intrusion Detection System

3.4 Machine Learning-Based Detection

Machine learning–based detection works by studying large volumes of data to understand patterns in how systems normally behave and how attacks occur. Instead of relying only on predefined rules, these systems learn from past data and can identify hidden or complex patterns that may indicate a cyber threat. One of the biggest advantages is that they keep improving over time—as more data is collected, the system becomes smarter and more accurate in detecting new and evolving threats. [5, 22]

4. Cybercrime Prevention Strategies

Prevention is all about reducing the chances of cybercrime before it even happens. This can be done by combining technology, proper organizational practices and user awareness to create a strong overall defense system.

4.1 Technical Prevention Methods

Technical methods act as the first line of defense against cyber threats. Tools like firewalls help monitor and control incoming and outgoing network traffic, blocking suspicious activity. Antivirus and anti-malware software protect systems from harmful programs. Encryption ensures that sensitive data remains secure, even if it is intercepted. Additionally, regularly updating software and installing security patches helps fix vulnerabilities that attackers might exploit [17],[22],[23].

4.2 Organizational Policies

Organizations play a crucial role in preventing cybercrime by setting clear security rules and guidelines. This includes defining who can access what information through proper access control policies. Having a well-prepared incident response plan ensures quick action if a security breach occurs. Limiting employee access based on their job roles also reduces the risk of internal misuse or accidental data leaks.

4.3 Human Awareness and Training

People are often the weakest link in cybersecurity, as many cyberattacks target human mistakes. Regular training programs can help individuals recognize common threats like phishing emails, fake links, and unsafe websites. By increasing awareness and encouraging safe online behavior, organizations can significantly reduce the risk of cybercrime. [3],[9],[24].

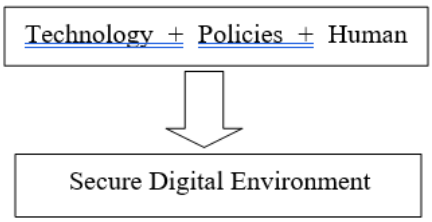


Figure 3: Cybercrime Prevention Framework

5. Challenges in Cybercrime Detection and Prevention

Even though we have advanced tools and technologies today, dealing with cybercrime is still quite difficult. Detecting and preventing these threats involves many challenges that make the process more complicated and demanding. [2][29]

5.1 Rapidly evolving attack techniques

Cybercriminals are always changing their methods and coming up with new ways to break into systems. Whenever one type of attack is identified and blocked, they quickly switch to another, making it hard for security systems to stay ahead.

5.2 Large volume of data to analyze

Every day, systems generate an enormous amount of data. Going through all this information to spot suspicious activity is not only time-consuming but also requires powerful tools and even then, some threats can go unnoticed.

5.3 Lack of skilled cybersecurity professionals

There is a high demand for cybersecurity experts, but not enough trained professionals are available. This shortage makes it challenging for organizations to properly handle and respond to cyber threats.

5.4 High cost of advanced security solutions

Strong cybersecurity systems often come with a high price tag. For smaller organizations, investing in such advanced tools can be difficult, leaving them more vulnerable to attacks.

5.5 Privacy and ethical concerns

To detect cyber threats, organizations often need to monitor user activities, which can raise concerns about privacy. It becomes important to maintain a balance between ensuring security and respecting users' personal data and rights.

6. Future Scope

The future of cybercrime detection and prevention is moving toward systems that are not just smarter, but also more adaptive and focused on human behavior. As technologies like cloud computing, the Internet of Things (IoT), artificial intelligence, and large-scale data sharing continue to grow, cyber threats are also becoming more complex and harder to predict. [2], [5], [25]

To tackle these challenges, future security systems will depend heavily on artificial intelligence and machine learning. These technologies will be able to study user behavior, identify unusual activities in real time and even respond to threats automatically without waiting for human intervention. This will make cybersecurity faster, more accurate and more efficient. [5],[10],[26].

At the same time, human awareness will remain just as important. In fact, it will play a key role in strengthening cybersecurity. Governments, educational institutions and organizations are expected to invest more in spreading cyber awareness and education. People will be trained to follow basic safety practices like creating strong passwords, protecting personal data and using the internet responsibly. [3],[4],[27-30] An informed and cautious user can often prevent attacks before they even begin.

Overall, the future of cybercrime prevention will depend on a balanced combination of advanced technology, well-defined policies, and responsible user behavior. Together, these elements will help create a safer and more trustworthy digital world.

7. Result

This section presents a comparative analysis of various cybercrime detection and prevention methods. Table 2 evaluates detection techniques based on their strengths, limitations, and accuracy levels, highlighting the trade-offs between speed and adaptability. Similarly, Table 3 outlines common prevention methods and their respective advantages and limitations, emphasizing the necessity of a layered security approach. Additionally, the figure illustrates the accuracy distribution of these detection techniques, showcasing their varying effectiveness in identifying potential threats.

Table 2. Comparative Analysis of Detection Techniques

Technique	Strengths	Limitations	Accuracy Level
Signature-Based Detection	Fast, accurate for known attacks	Cannot detect new threats	High (for known attacks)
Anomaly-Based Detection	Detects unknown attacks	High false positives	Medium
Intrusion Detection System (IDS)	Real-time monitoring	Requires tuning	Medium–High
Machine Learning Based Detection	Adaptive, improves over time	Requires large data & training	High

Table 3. Comparative Analysis of Prevention Methods

Method	Advantage	Limitation
Firewalls	Blocks unauthorized access	Cannot stop internal attacks
Antivirus	Detects malware	Needs regular updates
Encryption	Protects data privacy	Key management complexity
Awareness Training	Reduces human errors	Depends on user behavior

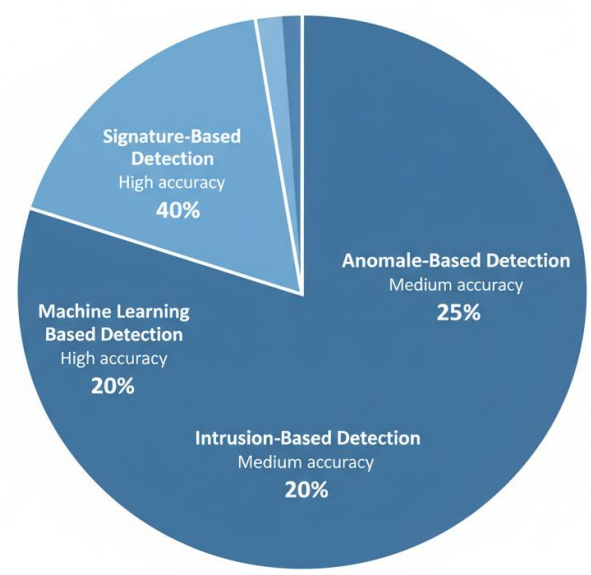


Figure 4. Cybersecurity detection techniques accuracy levels

9. Discussion

The findings clearly show that no single method of detecting cybercrime is fully reliable on its own. For example, signature-based detection works very well when it comes to identifying known threats, but it struggles to detect new or unknown attacks. On the other hand, techniques like anomaly-based detection and machine learning are better at spotting unfamiliar or emerging threats. However, these methods can sometimes produce false alarms or require large amounts of data to work effectively.

In the same way, prevention strategies cannot rely on just one approach. Technical tools such as firewalls, antivirus software and encryption provide a strong layer of protection, but they are not enough by themselves. Human factors play a crucial role as well. When users are properly trained and aware of common cyber risks, the chances of attacks caused by carelessness or lack of knowledge are greatly reduced.

Because of this, the most effective way to ensure cybersecurity is by using a combination of different approaches. A hybrid model that brings together advanced detection technologies, user awareness, organizational policies, and ethical practices offers the best protection. This balanced, human-focused approach matches the idea presented in this research paper, emphasizing that both technology and people are equally important in building a secure digital environment.

10. Conclusion

Cybercrime has become one of the most serious challenges in today's digital world, affecting individuals, organizations, and even governments. As our reliance on digital systems continues to grow, the risks related to cyber threats are also increasing. [11, 12] This study shows that detecting and preventing cybercrime cannot depend only on technical tools or automated systems.

A human-centered approach is equally important for building strong cybersecurity. Technologies like intrusion detection systems, encryption and machine learning provide powerful support, but they are not enough on their own. Human factors—such as awareness, ethical behavior, proper training and following security policies—play a major role in preventing cyberattacks. [1][16][5] In fact, many cyber incidents happen not because of weak technology, but due to simple human mistakes like clicking on malicious links, using weak passwords, or ignoring basic security guidelines. [4][19]

The study concludes that cybersecurity should be seen as a shared responsibility between technology and people. By combining advanced detection systems with clear organizational policies and continuous user education, the risks of cybercrime can be greatly reduced. [3][4] A safer digital future can only be achieved when individuals, organizations and governments work together with awareness, responsibility and a proactive approach.

References

[1] W. Stallings, *Cryptography and Network Security: Principles and Practice*. Pearson Education, 2022. [Online]. Available: https://www.pearson.com/en-us/subject-catalog/p/cryptography-and-network-security/P200000003321

[2] J. M. Kizza, *Guide to Computer Network Security*. Springer Nature, 2024. [Online]. Available: https://link.springer.com/book/10.1007/978-3-031-33577-4

[3] Government of India, *National Cyber Security Policy*. Ministry of Electronics and Information Technology (MeitY), 2013. [Online]. Available: https://www.meity.gov.in/content/national-cyber-security-policy-2013

[4] CERT-In (Government of India), *Guidelines on Information Security Practices*. Indian Computer Emergency Response Team, 2023. [Online]. Available: https://www.cert-in.org.in

[5] Various Authors, "Research Articles on Cybercrime Detection and Prevention," *IEEE*, *Springer*, and *Elsevier Journals*, 2019–2024. [Online]. Available: https://ieeexplore.ieee.org

[6] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley, 2020. [Online]. Available: https://www.cl.cam.ac.uk/~rja14/book.html

[7] M. Bishop, *Computer Security: Art and Science*. Pearson Education, 2019. [Online]. Available: https://www.pearson.com

[8] R. Sommer and V. Paxson, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," *IEEE Security & Privacy*, 2018. [Online]. Available: https://ieeexplore.ieee.org/document/4531146

[9] K. D. Mitnick and W. L. Simon, *The Art of Deception: Controlling the Human Element of Security*. Wiley, 2017. [Online]. Available: https://www.wiley.com/en-in/The+Art+of+Deception

[10] A. Sharma and S. K. Sahay, *Cyber Security and Cyber Laws*. Oxford University Press, 2021. [Online]. Available: https://global.oup.com

[11] W. Stallings, *Cryptography and Network Security: Principles and Practice*. Pearson Education, 2022.

[12] J. M. Kizza, *Guide to Computer Network Security*. Springer Nature, 2024. [Online]. Available: https://scholar.google.com

[13] Government of India, *National Cyber Security Policy*. Ministry of Electronics and Information Technology (MeitY), 2013.

[14] CERT-In (Government of India), *Guidelines on Information Security Practices*. Indian Computer Emergency Response Team, 2023.

[15] Various Authors, "Research Articles on Cybercrime Detection and Prevention," *IEEE*, *Springer*, and *Elsevier Journals*, 2019–2024. [Online]. Available: https://scholar.google.com

[16] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley, 2020.

[17] M. Bishop, *Computer Security: Art and Science*. Pearson Education, 2019.

[18] R. Sommer and V. Paxson, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," *IEEE Security & Privacy*, 2018.

[19] K. D. Mitnick and W. L. Simon, *The Art of Deception: Controlling the Human Element of Security*. Wiley, 2017.

[20] A. Sharma and S. K. Sahay, *Cyber Security and Cyber Laws*. Oxford University Press, 2021.

[21] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. MIT Press, 2016. [Online]. Available: https://www.deeplearningbook.org

[22] M. E. Whitman and H. J. Mattord, *Principles of Information Security*. Cengage Learning, 2021.

[23] T. R. Peltier, *Information Security Policies, Procedures and Standards*. Auerbach Publications, 2016.

[24] P. Sharma and R. Verma, "Cybercrime Detection Using Machine Learning Techniques," *International Journal of Computational and Electronics Aspects in Engineering*, vol. 5, no. 2, 2022. [Online]. Available: https://scholar.google.com

[25] A. Khan and D. Singh, "Anomaly-Based Intrusion Detection System for Network Security," *International Journal of Computational and Electronics Aspects in Engineering*, vol. 6, no. 1, 2023. [Online]. Available: https://global.oup.com

[26] S. Patel and K. Mehta, "A Study on Cyber Security Awareness and Human Factors," *International Journal of Computational and Electronics Aspects in Engineering*, vol. 6, no. 3, 2023.

[27] R. Gupta and P. Jain, "Cybercrime Prevention Strategies in Cloud Computing Environment," *International Journal of Computational and Electronics Aspects in Engineering*, vol. 7, no. 1, 2024.

[28] V. Iyer and S. Nair, "AI-Based Cyber Threat Detection and Prevention Systems," *International Journal of Computational and Electronics Aspects in Engineering*, vol. 7, no. 2, 2024. [Online]. Available: https://scholar.google.com

[29] W. Stallings and L. Brown, *Computer Security: Principles and Practice*. Pearson Education, 2018.

[30] A. Behl and K. Behl, *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press, 2017.