ISSN (ELECTRONIC): 2945-3135

· Majigamkar Poonam & Parikh Vrittee (2025). *Artificial Intelligence used for Data Protection International Journal of Multidisciplinary Research & Reviews, 4(2), 57-62.*

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH & REVIEWS

journal homepage: www.ijmrr.online/index.php/home

ARTIFICIAL INTELLIGENCE USED FOR DATA PROTECTION

Ms. Poonam Majigamkar[1], Dr. Vrittee Parikh[2]

[1]Aditya Institute of Management Studies and Research, Mumbai, India.
[2] Aditya Institute of Management Studies and Research, Mumbai, India.

How to Cite the Article: Majigamkar Poonam & Parikh Vrittee (2025). *Artificial Intelligence used for Data Protection International Journal of Multidisciplinary Research & Reviews, 4(2), 57-62.*

https://doi.org/10.56815/ijmrr.v4i2.2025.57-62

Keywords	***Abstract***
Artificial Intelligence, Cyber security, Threat Detection, Machine Learning, Data Protection, Mobile Security, Privacy Preservation.	Artificial Intelligence (AI) plays an important role in enhancing data security by identifying threats and responding to them effectively. This paper explores how AI-directed security will help in data protection by identifying dangers, reducing cyber risks, and ensuring real-time threat management. AI-driven tools such as machine learning-based anomaly detection, deep learning models for malware identification, automated threat intelligence systems, and advanced encryption techniques empower individuals and organizations to safeguard sensitive data. Also, AI-powered security solutions like biometric authentication and AI-assisted cyber security frameworks enhance defence mechanisms against evolving threats. The method of qualitative approach that includes a systematic review of AI-based data protection techniques and to analyse the ethical challenges, privacy concerns, and adaptive capabilities of AI-based security solutions for mobile devices. The research involves a systematic review, expert interviews, and case studies to assess the effectiveness of AI in mitigating cyber threats. Findings indicate that AI significantly improves data protecting of mobile by detecting threats with high accuracy while raising ethical concerns regarding data privacy, false detection and adaptability. The paper emphasis on the development of an ethical, efficient, and adaptive AI-driven security framework for mobile devices.

1. INTRODUCTION

· Majigamkar Poonam & Parikh Vrittee (2025). *Artificial Intelligence used for Data Protection International Journal of Multidisciplinary Research & Reviews, 4(2), 57-62.*

With the growing reliance on digital platforms like mobile devices for communication and data storage, data security has become a concern for all organizations and individuals. The traditional security methods struggles to counter the cyber threats, this leads to increase in the number of data breaches and financial losses to many. AI-driven security solutions offer real-time threat detection, automated response mechanisms, and advanced encryption methods to mitigate cyber risks effectively (Moustafa N & Slay J, 2017). Even after the development in important aspects, gaps remain in AI's adaptability to evolving threats and integration with existing security systems. The objective of this paper is to identify the threats from unknown messages on mobile device and to address ethical concerns using AI-powered security framework.

2. REVIEW OF LITERATURE

Numerous studies have explored AI applications in cyber security, focusing on anomaly detection, malware identification, and automated threat intelligence (Buczak & Guven, E, 2016). Research highlights the superiority of AI models over security approaches due to their ability to learn and adapt. Various studies demonstrate that machine learning algorithms, including supervised and unsupervised learning models, effectively detect network intrusions and unusual patterns indicative of cyber threats which common for mobile device. Zhang et al. (2022) demonstrated the use of deep learning models, to detect phishing messages based on textual and contextual features. His study highlighted the effectiveness of deep learning in recognizing patterns that traditional rule-based systems often miss. However, their models struggled with real-time performance on resource-constrained mobile devices. Gupta & Sharma (2021) applied NLP techniques to analyse linguistic cues in phishing and scam messages.

Mobile device is the easy mode of communication for all. The usage of mobile device has increased the number of cybercrime and the methods of scamming people. These threats/scams have become more advanced. The traditional method finds it difficult to identify AI-generated threats. As a result, artificial intelligence (AI), particularly machine learning (ML) and natural language processing (NLP), has come with a solution for real-time threat detection while using mobile devices.

Even though there are advancements, there are several research gaps. One major challenge is ethical concerns in using AI to identify threats from unknown messages on mobile devices. This ethical concern leads to individual privacy concerns, incorrect acceptance and adaption to new threat. This study aims to

1. Use AI methods for real-time deployment on resource-constrained mobile devices without compromising detection accuracy.

2. Preserving the privacy.

By addressing these gaps, this research contributes to the development of an ethical, efficient, and adaptive AI-detected security solution for mobile device.

· Majigamkar Poonam & Parikh Vrittee (2025). *Artificial Intelligence used for Data Protection International Journal of Multidisciplinary Research & Reviews, 4(2), 57-62.*

3. METHODOLOGY

A qualitative research approach is used, to know the use of AI in identifying threats from unknown messages on mobile devices. It allows to understand the perceptions, experiences, and ethical implications of AI-driven driven threat detection. The methodology focuses on privacy concern, accuracy of using AI and adapting the upcoming cyber threats. It will also help to understand how various individual experience and perceive the ethical challenges while using AI-driven security systems. This will know real-world experiences from cyber security experts, AI researchers, and mobile users, helping to identify ethical concerns and its possible solutions.

To gather the information, data will be collected from a small group of AI researchers in cyber security, professionals working with mobile security solutions for data privacy, mobile users who have faced AI-driven threats. The major focus will be on the following:

- What are the major ethical concerns in AI-based threat detection?
- How do privacy risks impact user trust in AI security solutions?
- What are the challenges in balancing AI accuracy and privacy preservation?
- How can AI models adapt to new and evolving threats while remaining ethical?

The study evaluates existing AI security frameworks, encryption methods, and intrusion detection systems to determine their effectiveness in mitigating cyber threats. The systematic review involves identifying ethical risks of AI in cyber security, Privacy-preserving AI techniques and their effectiveness, real-world examples of AI-driven threats and possible policy frameworks for ethical AI in mobile security. This involves case studies of existing AI-driven security solutions, to provide real-world insights on how these technologies handle ethical concerns. Industry reports from cyber security firms and technology companies are analysed to assess trends, emerging threats, and the adoption rate of AI in security operations (Sharma, 2020).

The data is analysed by thematic analysis, where ethical concerns are identified, categorized, and interpreted to uncover patterns in individual's perspectives. Ethical considerations in the research process include ensuring informed consent, confidentiality, and transparency to protect participants' rights and integrity. By adopting this approach, the study aims to contribute to the development of privacy-preserving, ethically responsible, and adaptive AI security solutions for mobile devices, addressing concerns related to individual privacy, system accuracy, and the ethical deployment of AI in cyber security.

4. RESULTS & DISCUSSION

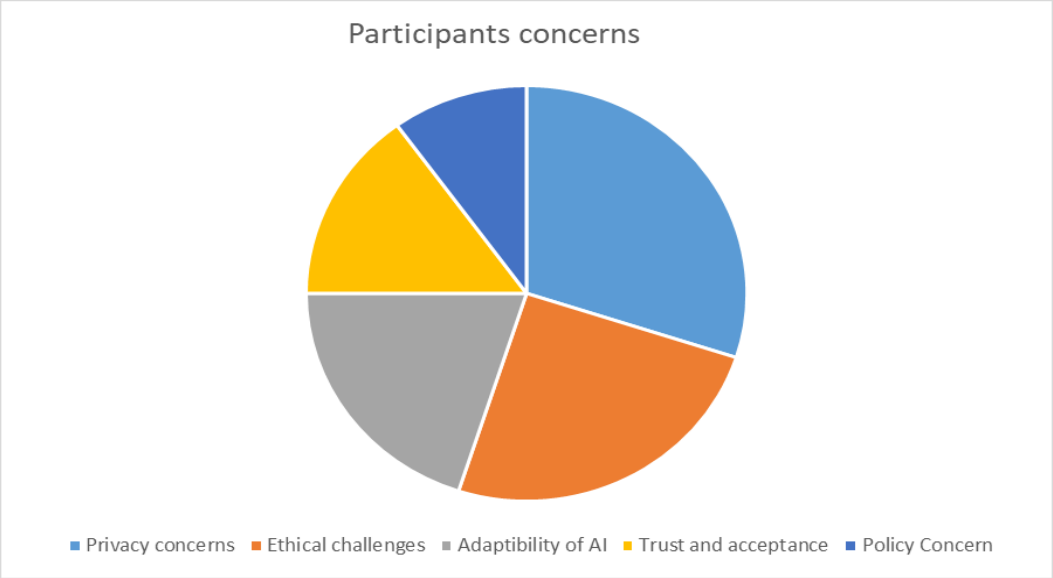
Findings reveal that AI-powered security systems significantly impacts the AI-powered security solutions exhibit high accuracy in identifying phishing attacks, malware, and scam messages. However, real-time performance on mobile devices varies based on computational resources and model efficiency. Many participants express concerns about AI accessing personal data, leading to

· Majigamkar Poonam & Parikh Vrittee (2025). *Artificial Intelligence used for Data Protection International Journal of Multidisciplinary Research & Reviews, 4(2), 57-62.*

potential privacy violations. The lack of transparency in AI decision-making also raises trust issues among users. While AI-driven models improve detection accuracy, ensuring privacy preservation remains a challenge. The research identifies the need for federated learning and differential privacy techniques to mitigate privacy risks. AI-based security frameworks must constantly update their models to combat new cyber threats. Participants emphasize the need for regulatory frameworks to ensure ethical AI deployment. The study finds that users are more likely to trust AI-driven security systems when transparency, privacy protection, and regulatory compliance are ensured.

Machine learning-based anomaly detection detects deviations in network behaviour, while deep learning models identify sophisticated malware variants (Moustafa N & Slay J, 2017) AI-driven encryption techniques bolster data security by dynamically adapting encryption standards. Challenges include AI's vulnerability to adversarial attacks and the need for continuous updates to AI models. Graphs and tables illustrate AI's impact on cyber security efficiency compared to traditional methods.

These findings suggest that while AI enhances mobile device security, ethical concerns must be addressed through transparent decision-making, privacy-preserving AI techniques, and regulatory guidelines.



5. CONCLUSION

This study highlights the role of AI in enhancing mobile device security while addressing ethical concerns related to data privacy, accuracy, and algorithmic bias. The findings contribute to the

· Majigamkar Poonam & Parikh Vrittee (2025). *Artificial Intelligence used for Data Protection International Journal of Multidisciplinary Research & Reviews, 4(2), 57-62.*

development of privacy-preserving, ethically responsible, and adaptive AI security solutions. By understanding the ethical implications and technical challenges, this research paves the way for a balanced approach to AI-driven cyber security, ensuring both security effectiveness and user trust in mobile security systems.

AI-driven security solutions outperform traditional cyber security measures by dynamically adapting to emerging threats, reducing data breaches, and enhancing resilience. Despite advancements, limitations such as adversarial attacks and ethical concerns need to be addressed (Goodfellow, McDaniel, P.,, & Papernot, N., 2018). Future research should focus on improving AI model robustness, integrating AI with block chain for enhanced security, and developing ethical AI governance frameworks.

6. AUTHOR(S) CONTRIBUTION

The writers affirm that they have no connections to, or engagement with, any group or body that provides financial or non-financial assistance for the topics or resources covered in this manuscript.

7. CONFLICTS OF INTEREST

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

8. PLAGIARISM POLICY

All authors declare that any kind of violation of plagiarism, copyright and ethical matters will taken care by all authors. Journal and editors are not liable for aforesaid matters.

9. SOURCES OF FUNDING

The authors received no financial aid to support for the research.

REFERENCES

[1] Goodfellow, I., McDaniel, P., & Papernot, N. (2018). Making Machine Learning Robust Against Adversarial Inputs. Communications of the ACM, 61(7), 56-66.

[2] Buczak, A. L., & Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Communications Surveys & Tutorials, 18(2), 1153-1176.

[3] Sharma, P. (2020). Artificial Intelligence in Cybersecurity: The Future of Protecting Digital Assets. CRC Press.

[4] Moustafa, N., & Slay, J. (2017). The Evaluation of Network Anomaly Detection Systems: Statistical Analysis of the UNSW-NB15 Dataset and the Comparison with the KDD99 Dataset. Information Security Journal: A Global Perspective, 26(2), 78-85.

· Majigamkar Poonam & Parikh Vrittee (2025). *Artificial Intelligence used for Data Protection International Journal of Multidisciplinary Research & Reviews, 4(2), 57-62.*

[5] Hubert Baniecki, Przemyslaw Biecek (2024) Adversarial attacks and defenses in explainable artificial intelligence: A survey. Information Fusion

[6] Adversarial Threats to AI-Driven Systems: Exploring the Attack Surface of Machine Learning Models and Countermeasures. Journal of Engineering Research and Reports.

[7] Parikh, V. & Pirani, S (2025). Integrating Sustainable HRM, Digital HRM, And Remote Work Practices: A Conceptual Framework for Enhancing Job Satisfaction. International Journal of multidisciplinary Research & Reviews, 4(1), 68-81.

[8] Pirani, S. (2024). Navigating the complexity of sample size determination for Robust and Reliable Results, International Journal of Multidisciplinary Research & Reviews, Vol 03, No. 02, PP.73-86.

[9] Pirani, S. (2024). Simplifying statistical Decision Making: A Research Scholar's Guide to parametric and Non-Parametric Methods, International Journal of Multidisciplinary Research & Reviews, Vol 03, No. 03, pp. 184-192.