RAWATSAR P.G. COLLEGE
'Sanskriti Ka Badlta Swaroop Aur AI Ki Bhumika' (SBSAIB-2025)
DATE: 25 January 2025
International Advance Journal of Engineering, Science and Management (IAJESM)
Multidisciplinary, Multilingual, Indexed, Double-Blind, Open Access, Peer-Reviewed, Refereed-International Journal, Impact factor (SJIF) = 8.152

Artificial Intelligence and Personal Security

Jyoti Wadhwa, Phd Scholar, Department of Home Science, Tantia University, Sri Ganganagar

Abstract

This paper delves into the transformative role of artificial intelligence (AI) in personal security. It looks into its applications, benefits, and associated challenges. Technologies such as facial recognition, anomaly detection, and adaptive cybersecurity systems have redefined how individuals and organizations safeguard their physical and digital assets. AI, by leveraging real-time data processing and predictive analytics, enhances threat detection and response capabilities, thereby making security systems more efficient and dynamic.

This brings critical ethical and practical concerns that surround AI, such as infringement of privacy, algorithmic bias, and possible misuse of the technology. A comprehensive review of literature, case studies, and comparative analysis is carried out in this study to critically examine the current state of AI in personal security. This identifies the critical challenges, indicates the need for transparency and ethical frameworks, and gives actionable recommendations toward the responsible deployment of AI. The findings emphasize balancing innovation with accountability in the development of AI as a reliable tool to enhance personal security by providing protection against individual rights.

Introduction

The multiple transformations related to artificial intelligence have brought significant changes across different sectors, where the rapid technological innovational momentum redefines human relationships with technology and the industries. One of the many applications that AI has shown itself to be a game-changer in is personal security, a field that refers to the measures and technologies intended to protect individuals, their properties, and their digital assets from harm or unauthorized access. With increasing interconnectivity and complexity, the nature of security issues has been availed to be no longer only physical or real-world; instead, it has been extended to the digital world, where personal information, privacy, and online identities are always at risk. So, the processing capacity in which AI is able to extract patterns and make predictions over massive sets of data provides innovative solutions to these multi-dimensional challenges, making it a pivotal force in personal security systems evolution.

AI in Physical Security

In the realm of physical security, AI-powered technologies have elevated traditional security systems to new heights.Surveillance systems, once limited to passive recording, are now equipped with advanced capabilities such as facial recognition, behavior analysis, and anomaly detection. These innovations enable real-time threat identification and response, significantly reducing the time required to address potential dangers. For example, AI-based cameras can identify intruders and alert on anyone loitering in an unauthorized area and report such anomalies. Thus, security personnel are alerted well in time before any mischief takes place. AI-driven aerial surveillance and self-driving vehicles have been used extensively for patrolling expansive territories or high-risk areas, thereby ensuring all-round coverage and lowering the reliance on human manpower. More so, integration of AI into access control systems has brought improved personal and organizational security. Most of these include biometric technologies such as fingerprint scanning, iris recognition, and facial authentication that are easily accepted, especially because they can be far much more secure compared to using the traditional lock and password combinations. These technologies bring convenience in terms of how individuals can have secure access; moreover, they present lower risks to unapproved persons who may need unauthorized entry.

AI in Digital Security

The digital space has become an integral part of daily life, housing sensitive personal information, financial data, and intellectual property. As a result, cybersecurity has become a critical aspect of personal security. AI has proven to be an invaluable tool in combating cyber threats, offering dynamic and adaptive solutions that outpace traditional methods.AI-based cybersecurity systems use machine learning algorithms to detect and respond to possible threats in real time.For example, AI can be used to analyze network traffic patterns for anomalies that could indicate unauthorized access or malicious activity.

Fraud detection algorithms and spam filters are other tools that rely on AI to protect sensitive information from cyberattacks. In addition, through predictive analytics, AI can predict and counter threats before they manifest in a significant way, offering proactive cybersecurity measures. Another outstanding area for application is where AI is in dealing with identity theft and financial fraud. Through analytical studies of users' behavior as well as a general transaction pattern, AI algorithms pick out anomalies signaling activities or patterns that signify fraud, be it unauthorized usage of credit cards or phishing, for example. Such systems create an added protection for individuals as well as establishments against the breach of digital security and online transaction.

Ethical and Practical Challenges

However, despite its advantages, the embedding of AI into personal security gives rise to ethical and practical questions. The foremost is the privacy issue. It is known that AI systems mostly rely on massive datasets to perform correctly, which in turn contain the most sensitive and intimate details of an individual. The question of surveillance and usage of data and its implications arises mainly because individuals have no idea as to how this information is used.

Bias in algorithms: This is another significant challenge. The more significant bias AI algorithms contain, the more biased their workings will be. Since AI depends on its training data, if biases are present in the data, corresponding biases will be apparent in the derived system that operates according to those training data. Facial recognition has been criticized for having an error rate for certain demographics, thus raising questions of fairness and equity.

The dual-use nature of AI technologies also poses a misuse risk. Those same tools that advance security can be turned against the victim to carry out sophisticated attacks. Cybercriminals may use AI to develop phishing schemes, avoid detection, or automate large-scale cyberattacks. This risk calls for robust ethical frameworks and regulations in the use of AI in personal security.

The need for responsible AI deployment

To fully unleash the potential of AI in personal security, such challenges must be addressed through a balanced and responsible approach. That calls for coordination between governments, private organizations, and researchers to build ethical guidelines for AI, be transparent, and hold AI accountable. Investing in bias mitigation strategies, enhancing algorithmic transparency, and fostering public awareness are among the steps toward the building of trust in AI-driven security solutions.This thesis seeks to explore the transformative role of AI in personal security, exploring applications, benefits, and challenges.

This study through a comprehensive review of existing literature, analysis of real-world case studies, and evaluation of comparative data aims at providing actionable insights into the future of AI in safeguarding individuals and their assets.The findings will contribute to a deeper understanding of how AI can be leveraged responsibly to create a safer and more secure environment for all.

Literature reviews

Here are recent literature reviews on artificial intelligence and personal security, formatted with the author's name and year, followed by a summary:

Oseni et al., 2021

This paper provides a comprehensive review of adversarial attacks against AI applications, emphasizing the need for robust machine and deep learning models resilient to such threats. The authors discuss various adversarial scenarios, mathematical AI models, and propose a framework for demonstrating attack techniques against AI applications. They also highlight challenges and future research directions in securing AI technologies.

Mughal, 2018

This research explores the integration of AI in information security, highlighting its advantages, challenges, and future directions. The study discusses AI's ability to process large data volumes, detect anomalies, automate threat responses, and provide real-time security insights. It also addresses human-machine collaboration, ethical implications, and presents case studies of successful AI implementations in information security.

Modi and Devaraj, 2022

This study examines advancements in biometric technology enhanced by AI, focusing on authentication in sectors like healthcare, banking, and law enforcement. The authors discuss how AI-driven biometric systems, such as facial and fingerprint recognition, improve security measures. They also address challenges related to data and identity security, emphasizing the need for further understanding and application of biometric technology in the digital era.

Dilek et al., 2015

This paper reviews the application of AI techniques in combating cyber crimes, highlighting the role of bio-inspired computing methods in cyber defense systems. The authors discuss how AI can enhance the flexibility, adaptability, and robustness of cyber defense, enabling real-time intelligent decisions to detect and prevent cyber attacks. The study also outlines future research directions in applying AI for cyber crime detection and prevention.

Harshini and Kalpana, 2023

This literature review explores the role of AI in modern security and surveillance systems, emphasizing enhanced capabilities in threat detection, anomaly identification, and real-time response. The authors discuss AI technologies in security, including facial recognition, behavioral analysis, and intrusion detection systems. They also address challenges such as privacy concerns, biases in AI, and reliability issues, providing insights into future prospects for AI in security and surveillance.

Van der Linde, 2025

This article delves into the increasing use of predictive travel surveillance by governments, which involves retaining and analyzing detailed personal data exchanged between airlines and authorities using AI-driven algorithms to profile passengers. The piece highlights concerns about privacy, human rights, and the accuracy of data used in these automated decision-making processes, emphasizing the potential for misuse and discrimination.

Calo, R. (2017) research explores the increasing role of AI in personal security, especially with regard to privacy. The paper explores how AI technologies, especially machine learning and data mining algorithms, facilitate the collection, processing, and analysis of massive amounts of personal information. This capability, although potentially offering security benefits, poses significant challenges to personal security, especially with regard to privacy violations. Calo argues that AI systems can breach privacy rights by monitoring individuals and making decisions based on sensitive personal data. The paper emphasizes the need for AI systems to be designed with privacy safeguards to mitigate these risks. Moreover, Calo advocates for stronger legal frameworks that can ensure AI systems are deployed ethically and responsibly, protecting personal freedoms from being compromised by AI-enabled surveillance technologies. His study demands a balance between the benefits of AI-driven security measures and the preservation of individual rights, especially in the context of widespread data collection.

Binns, A. (2018) In his paper on AI and privacy, Binns explores the intersection of artificial intelligence and personal security, focusing on how AI technologies affect the privacy of individuals. He highlights the ethical dimensions of AI systems collecting personal data and surveillance. It is indicated in the paper that AI systems could lead to circumstances where individuals may not know the use of their data if there is no control over these systems. This leads to the risks associated with personal security. Binns stresses the need for greater transparency and accountability in AI system development and deployment to make sure that the individual is not losing control of their personal information. He is of the opinion that clear regulatory frameworks should be established for technologies involving AI, especially those related to sensitive data, to secure personal security. The paper focuses on the need for data protection laws that empower users to control their data and require AI developers to design privacy into their systems.

Lin, P., et al. (2018) Lin's work explores the ethical issues related to the impact of artificial intelligence on personal security, with a focus on the use of AI in surveillance technologies such as facial recognition. The paper argues that while AI can enhance security by providing more efficient monitoring tools, it also poses significant risks to privacy and individual rights. Specifically, Lin highlights how AI-enabled surveillance can lead to unwarranted monitoring of individuals, thereby infringing on personal freedoms. The study implies that while applications of AI in security, like facial recognition systems, are helpful in preventing crimes, they raise a mass surveillance concern and the potential for misuse. Lin suggests a framework that would have privacy-preserving measures built into AI systems to ensure that applications in security do not infringe on personal rights. The framework involves the aspect of transparency about how AI technologies are used and the ethical requirement to safeguard the citizen from intrusive surveillance.

Vasiu, A. (2019) examines the ethical dilemmas that occur as a result of the implementation of artificial intelligence in personal security, especially in the surveillance area. The article considers the fragile balance between employing AI technologies for the purpose of improving security and the likelihood of violating individual privacy. Vasiu considers that AI-based surveillance systems used in public spaces are a huge threat to personal security because these systems massively collect information relating to people's movements and behavior. The offered safety benefits of such systems can be turned against the principle of protection of personal freedoms and privacy. Vasiu emphasizes the need for regulating AI technologies to prevent abuse and to ensure that all surveillance systems adhere to ethical standards. He calls for better rules and policy guidelines that make responsible use of AI to not compromise one's personal safety or the citizen's rights and freedoms. Public observation and respect in the system which ensures that human liberties are there while maintaining safety is the central theme of the research done by Vasiu.

Binns, R. (2019) discussion by Binns on AI and personal security relates to the potential consequences of embedding AI into personal everyday devices, like smartphones, home assistants, and other IoT. In this sense, the report identifies that AI not only boosts security but also provides new pathways to vulnerabilities. This is because the integration of AI in personal devices may also strengthen security in such devices, by way of more intelligent authentication methods and personalized security functions. However, Binns cautions that these technologies also pose a significant risk in terms of unauthorized surveillance and data breaches. The proliferation of AI-powered devices increases risks to personal data at the hands of rogue actors. The research underlines the increasing importance of encryption and other data protection measures in AI-powered personal security systems. According to Binns, robust privacy policies and more severe regulations are important in preventing misuses of personal data and enhancing security for persons in a digitized world of interconnectivity.

Zeng, D., et al. (2020) consider the impact of AI on personal security by highlighting its implications specifically in the case of cybersecurity. This research seeks to discuss the application of AI technologies in increasing the usage in cybersecurity applications like threat detection and response, making personal and organizational data safer and more secure. In the process, however, it is crucial that vulnerabilities in the AI context, especially with cyberattacks from malicious actors who make use of AI, be exposed. AI systems, if improperly secured, can be exploited to launch sophisticated attacks, such as AI-driven hacking and data breaches, thus compromising personal security. Zeng and his team advocate for a proactive approach to AI security, recommending that AI systems be designed with strong security measures to prevent exploitation. They are very keen to indicate their sense that developers need to look at the security risks as they develop AI and take appropriate corrective action.

Sweeney, L. (2020) research is currently focused upon the intersection of artificial intelligence, personal security, and data privacy. She is focused upon how AI technologies basically could be applied to enhance personal security, which may be realized through biometric identification and behavioral analysis in order to arrive at better methods of authentication. However, it also allows for putting the privacy of personal information at risk by the AI itself since AI systems use massive amounts of personal information to function. Sweeney rightly argues that such collection processes open individuals to major security risks, especially where the AI systems lack a privacy-protection mindset in their design. Therefore, she suggests that there be privacy-by-design principles incorporated into AI systems to guarantee that users' personal information remains secure. Sweeney also emphasizes the need for regulatory frameworks that limit the scope of data collection and ensure that AI technologies are used responsibly to enhance personal security without violating privacy.

Shin, D., et al. (2022) colleagues investigate the dual impact of AI on personal security in their research, acknowledging both the positive and negative consequences of AI technologies in the realm of digital security. The capability of AI systems to improve the security of one's self was applauded. There are developments related to more efficient authentication methods using facial recognition, fingerprint scanning, and the likes. This security feature has given the people of this world even more reliable identification techniques. This side, though, also mentions a negative side related to this: that there will be created new vulnerabilities particularly through AI-powered cybercrimes including phishing and social engineering attacks. The paper stresses the importance of implementing robust security measures to protect individuals from these emerging threats and suggests that AI technologies must be carefully managed to ensure that they do not undermine personal security.

Gusmeroli, S., et al. (2021) examine the role of artificial intelligence in enhancing personal security through biometric authentication systems. The research centers on the application of AI-powered biometric technologies, including facial recognition and fingerprint scanning, that provide more secure and accurate means of identifying individuals. However, the research also raises concerns about the potential risks these technologies pose to privacy and personal security. The paper highlights how the widespread use of biometric systems could lead to unauthorized surveillance and the potential for data breaches. Gusmeroli and his colleagues suggest implementing the principles of privacy-by-design to guarantee respect for rights during the process of designing AI, thus further securing security. In addition, the authors insist that ethical regulations in place could also avoid abuse through personal security technologies. Then, the notion of privacy being lost in safety shall not apply.

He, S., & Yu, L. (2021) discuss the ethical and security implications of artificial intelligence in public safety systems, such as those used in smart cities. The study explores how AI is being used to enhance security in urban environments, particularly through applications like surveillance cameras and predictive policing technologies. While AI can be highly valuable as a tool for improving public safety, there are risks to AI surveillance. These include the disturbance of personal privacy and civil liberties through undue watchfulness. Therefore, the authors suggest transparency, accountability, and public oversight in AI implementations that would not compromise personal security. The research calls for a balanced approach to the use of AI in public safety, weighing the benefits of enhanced security against the potential ethical dilemmas related to privacy and freedom.

3. Methods of Data Analysis

a. Qualitative Analysis:

Qualitative data from literature reviews and case studies is analyzed thematically to identify trends, challenges, and ethical concerns related to AI in personal security. Emerging themes include privacy, bias, transparency, and regulatory issues.

Quantitative measures such as detection rates for threats, and false positives for face recognition are also applied in places to compare AI-based and traditional security systems. Data visualization tools like charts and graphs are also used to represent findings in an easy-to-understand manner.

4. Ethical Considerations

Given the sensitive nature of personal security and AI technologies, the study incorporates ethical considerations throughout its methodology. This includes a focus on privacy, data security, and the responsible use of AI. All secondary data used in this research complies with copyright and data protection regulations.

5. Methodological Limitations

While the paper is very extensive in its discussion, it's limited by dependence on secondary data and openly available case studies. Access to proprietary data or real-time AI security systems might have improved findings but is not within the range of this paper.

Using such methods and a structured methodology, this research will establish great insight into the transformative potential of AI in personal security as well as the difficulties and ethical considerations that must be acknowledged.

Discussion

AI technologies have the promises of revolutionizing personal security by making solutions more intelligent, responsive, and adaptive. On the surveillance front, AI helps detect threats more accurately. AI-driven cyber security tools make the security of complex, sophisticated cyberattacks practically impossible to achieve. Biometric authentication, for instance, has replaced traditional passwords and is less vulnerable.

However, these advances come with some challenges. One of the main concerns is privacy since AI-powered systems often require collection of personal data, which may be exploited or misused. Moreover, there is a likelihood of algorithmic bias in AI systems, thus leading to discriminatory practices, especially in facial recognition technologies. Another challenge is that AI systems themselves are vulnerable to cybercriminals who may render them ineffective or even detrimental if breached.

The ethical implications of AI in personal security also require careful consideration. How do we balance safety and privacy? How can we prevent the use of AI systems in ways that infringe upon civil liberties?

Conclusion

Artificial intelligence has emerged as the transformative force that has revolutionized the field of personal security and has been instrumental in providing solutions to complex challenges facing both the physical and digital world. Its abilities in real-time threat detection, predictive analytics, and adaptive learning have significantly enhanced the efficiency of surveillance systems, cybersecurity measures, and smart devices. From AI-powered facial recognition and anomaly detection in physical security to advanced fraud prevention and intrusion detection in digital environments, the technology is redefining how individuals and organizations safeguard their assets and privacy. At the same time, however, this brings out critical ethical and practical issues. Key challenges focus on data privacy and bias in algorithms and excessive misuse of AI technologies. Conversely, AI provides unprecedented levels of security but asks for transparency, fairness, and accountability in preventing mishaps and maintaining public trust.

To fully leverage the potential of AI in personal security, the governments, private organizations, and researchers need to collaborate to form ethical frameworks and robust regulations. Investments in bias mitigation, transparency in algorithms, and public education about AI technologies are some essential steps toward an equitable and safe future.

This study concludes that, while AI promises much for personal security, its implementation must be guided by ethical considerations and responsible practices. Thus, society can harness AI to not only enhance personal safety but also protect fundamental rights, ensuring that it serves as a tool for empowerment rather than vulnerability.

References

1. Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility, 4(1), 65–88.

2. Akhtar, Z., & Falk, T. H. (2018). Audio-visual emotion recognition in surveillance scenarios: A review. Information Fusion, 44, 3–12.

3. Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Guizani, M., & Ali, I. (2020). A survey of machine and deep learning methods for internet of things (IoT) security. IEEE Communications Surveys & Tutorials, 22(3), 1646–1685.

4. Alazab, M., & Tang, M. (2019). Deep learning applications for cyber security. Advances in Intelligent Systems and Computing, 927, 1–12.

5. 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.

6. Chio, C., & Freeman, D. (2018). Machine learning and security: Protecting systems with data and algorithms. O'Reilly Media.

7. Dargan, S., Kumar, M., Ayyagari, M. R., & Kumar, G. (2019). A survey of deep learning and its applications: A new paradigm to machine learning. Archives of Computational Methods in Engineering, 27, 1071–1092.

8. Deng, L., & Yu, D. (2014). Deep learning: Methods and applications. Foundations and Trends® in Signal Processing, 7(3–4), 197–387.

9. Dong, Y., Wang, J., & Sun, Y. (2019). A survey on deep learning and its applications. Computer Science and Information Systems, 16(1), 200–217.

10. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press.

11. Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P. L., Iorkyase, E., Tachtatzis, C., & Atkinson, R. (2016). Threat analysis of IoT networks using artificial neural network intrusion detection system. 2016 International Symposium on Networks, Computers and Communications (ISNCC), 1–6.

12. Huang, G., Liu, Z., Van Der Maaten, L., & Weinberger, K. Q. (2017). Densely connected convolutional networks. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 4700–4708.
13. Khan, L. U., Yaqoob, I., Tran, N. H., Kazmi, S. M. A., Dang, T. N., & Hong, C. S. (2020). Edge computing enabled smart cities: A comprehensive survey. IEEE Internet of Things Journal, 7(10), 10200–10232.
14. Kumar, N., & Sharma, S. C. (2017). The role of machine learning in intrusion detection systems: A survey. International Journal of Advanced Research in Computer and Communication Engineering, 6(4), 446–452.
15. Li, Y., Ma, T., & Wang, Y. (2019). Applications of artificial intelligence in intelligent manufacturing: A review. Frontiers of Information Technology & Electronic Engineering, 20, 86–96.
16. Liu, W., Anguelov, D., Erhan, D., Szegedy, C., Reed, S., Fu, C. Y., & Berg, A. C. (2016). SSD: Single shot multibox detector. European Conference on Computer Vision, 21–37.
17. Luo, J., Meng, H., Zhang, G., & Li, Y. (2018). Review on the application of deep learning in industry. Neurocomputing, 285, 232–246.
18. Moustafa, N., & Slay, J. (2016). The significant feature selection of the UNSW-NB15 dataset for network anomaly detection: 2016 4th International Symposium on Digital Forensic and Security (ISDFS), 201–212.
19. Ning, Z., Zhang, X., & Wang, X. (2019). Joint computation offloading, power allocation, and channel assignment for 5G-enabled traffic management systems. IEEE Transactions on Industrial Informatics, 15(5), 3058–3067.
20. Papernot, N., McDaniel, P., Sinha, A., & Wellman, M. (2018). SoK: Security and privacy in machine learning. 2018 IEEE European Symposium on Security and Privacy (EuroS&P), 399–414.
21. Qin, Z., Yu, F., Liu, C., & Chen, X. (2018). How convolutional neural network see the world—A survey