WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Artificial Intelligence and Cybersecurity: Protecting Guests and Assets with Advance Technology

Ms. Rachana Hangirkar

(UG Student) D Y Patil School of Hospitality, Kolhapur
Constituent Unit of D.Y. Patil Education Society (Institution Deemed to be University),Kolhapur

ABSTRACT

The business process is changing now. We are already in digital era, and this is a constant challenge. Today the most valuable thing is not currency or gold, is data. How vulnerable are businesses to computerization? 100%. Internet is a virtual space available for everyone. Storing data on any device that can be connected to the internet can become vulnerable in any given second. This article comes to show how we can combine and use artificial intelligence and cyber security to protect our business against cyberattacks, presenting in the same time cases of risk management in Hospitality Industry.

AI and ML have made it possible to detect cyber-threats faster and with a higher accuracy than human teams and stop cyberattacks quickly. The Research Article aims to underline the benefits of using Artificial Intelligence to improve the business productivity, and in the same time to address awareness in order to overcome fear in exploring new technology, because of cyber-attacks.

Keywords: *Artificial Intelligence, Cyber security, Information security, Data breach, Hotel industry*

1. Introduction

‘Cybersecurity’: Many of us has already heard this term but not quite got the meaning of it. So in simple words Cybersecurity means the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this. Artificial Intelligence and security is a topic that explores how Artificial Intelligence is being used to improve security measures and protect against cyber threats. Artificial Intelligence can be used to analyze large amounts of data and identify patterns that may indicate a security breach or cyber attack.

This can help businesses and organizations respond to potential threats in a more effective and quick way. AI can also be used to automate certain security tasks, such as monitoring network traffic or detecting fraud behaviour. However, along with its advantages, the drawbacks of Artificial Intelligence are also present and can be used in a wrong way, such as in deep fake videos or other forms of cybercrime. It's important for businesses and organizations to stay up-to-date on the latest developments in Artificial Intelligence and security, and to implement appropriate steps to protect against potential security threats.

Cybersecurity is growing day by day in various sectors of the industries which also include our Hospitality Industry. In hospitality industry guest data is to be kept secured and private no matter the situation. Also the impact of Artificial Intelligence on the hospitality industry is gaining much and much importance as we as humans are starting to depend on AI on daily basis. So with the help of Artificial Intelligence and Cybersecurity organizations and hotels can store their guest data is a more effective and secure way.

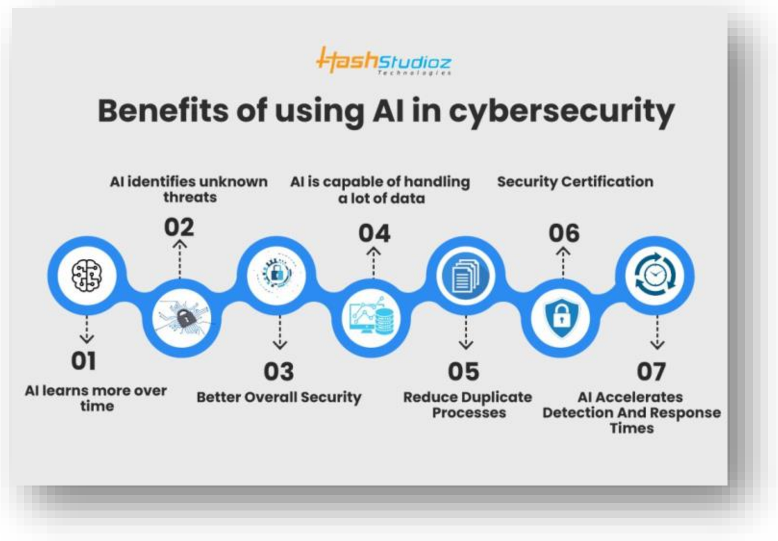
AI can also be used to train and test cybersecurity professionals, and to develop new security technologies. Hotels and organizations can hire such cybersecurity professionals for the security of the guest or customer data and information in a safer manner.

2. Methodology

Research methodology discusses and explains the data collection and analysis methods that are used in this research. A key part of this research paper, the methodology chapter explains what and how the research was conducted, allowing us to evaluate the reliability and validity of this research topic. The type of research conducted in this research paper is regarding the concept of Artificial Intelligence and Cybersecurity and how it is protecting guests and assets with advance technology.

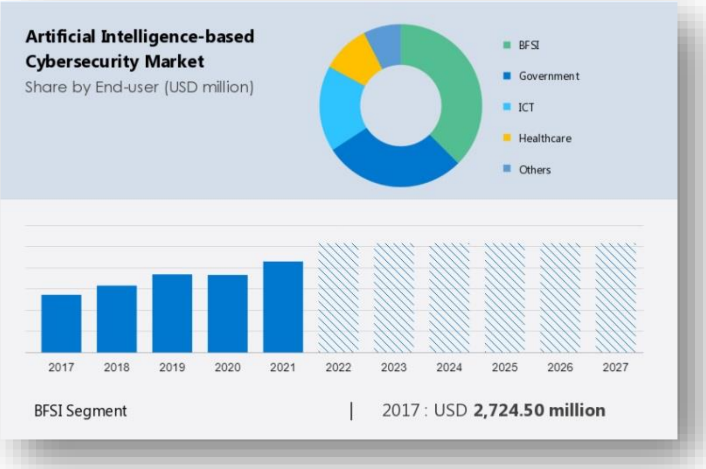
The Sampling data required for this Research Paper was collected and distinguished between qualitative and quantitative data and the required raw data was collected from various books on Artificial Intelligence and Cybersecurity as well as journals and online sources. Research limitations for this research paper was that as most on the technologies are still under development, the information obtained regarding the topic was not adequate.

As cyberattacks grow in volume and complexity, artificial intelligence (AI) is helping under-resourced security operations analysts stay ahead of threats. Curating threat intelligence from millions of research papers, blogs and news stories, AI technologies like machine learning and natural language processing provide rapid insights to cut through the noise of daily alerts, drastically reducing response times. Analyzing and improving cybersecurity posture is not a human-scale problem anymore. In response to this unprecedented challenge, Artificial Intelligence (AI) based tools for cybersecurity have emerged to help information security teams reduce breach risk and improve their security posture efficiently and effectively.AI and machine learning (ML) have become critical technologies in information security, as they are able to quickly analyze millions of events and identify many different types of threats – from malware exploiting zero-day vulnerabilities to identifying risky behavior that might lead to a phishing attack or download of malicious code. These technologies learn over time, drawing from the past to identify new types of attacks now. Histories of behavior build profiles on users, assets, and networks, allowing AI to detect and respond to deviations from established norms.AI is ideally suited to solve some of our most difficult problems, and cybersecurity certainly is growing in large number. With today's ever evolving cyber-attacks and proliferation of devices, machine learning and AI can be used to "keep up with the bad guys," automating threat detection and respond more efficiently than traditional software-driven approaches.These are some of the benefits of using Artificial Intelligence in cybersecurity (by Hash Studioz):


HashStudioz Technologies
Benefits of using AI in cybersecurity
01
AI learns more over time
02
AI identifies unknown threats
03
Better Overall Security
04
AI is capable of handling a lot of data
05
Reduce Duplicate Processes
06
Security Certification
07
AI Accelerates Detection And Response Times

Cybersecurity in the hospitality industry is an important consideration as hotels and other businesses in the industry handle a large amount of sensitive data, such as guest credit card information and personal details. Cybersecurity threats can come from a variety of sources, including hackers, malware, and phishing attacks. To protect against these threats, hotels and other businesses in the hospitality industry should implement a number of cybersecurity measures, such as using strong passwords, encrypting sensitive data, and regularly updating software and security systems. Additionally, it's important to train staff on cybersecurity best practices, such as how to identify phishing emails and how to handle guest data securely. Finally, hotels and other businesses in the hospitality industry should have a plan in place for responding to security incidents, including how to notify guests and authorities if a data breach occurs.In the hospitality industry, AI and cybersecurity can be used to protect guest data, prevent cyber attacks on the hotel's network, and detect fraudulent activity. AI can also be used to monitor online reviews and social media posts for any negative comments or threats, and to respond quickly to any issues that arise. Additionally, AI can be used to monitor physical security measures, such as surveillance cameras and access control systems, to ensure that the hotel is secure and safe for guests. However, it's important to ensure that any AI systems used in the hospitality industry are secure and protected against potential cyber threats, and that guest data is stored securely and in compliance with relevant regulations.AI and cybersecurity can be used in the hospitality industry to improve guest safety and protect sensitive guest data. AI can be used to monitor network traffic, detect potential security breaches, and identify patterns that may indicate a cyber attack. Artificial intelligence has advantages and disadvantages in cyber security. On one hand, it improves the analysis, understanding, and prevention of cybercrime, enhancing the safety of companies and customers. However, AI can be resource-intensive and not always practical, and it can also be used by cybercriminals to improve their attacks. One industry that benefits from AI is VPNs, as machine learning allows them to protect users from online threats posed by AI. The use of AI in cyber security has been a topic of discussion for some time, with the ability to analyze data quickly being a key advantage of AI technology.

What will be the size of the Artificial Intelligence-based Cybersecurity Market during the Forecast Period? Take a look at this graph.



Artificial intelligence is really a kind of computerized version of human intelligence. The way artificial intelligence works is like learning iteratively again and again, just like humans. In this generation, the threat of landscape is unquestionably evolving. The cyber attackers are entirely focused on financial rewards. But the department has found a new way to prevent attacks before they occur, as the old traditional way can no longer be relied upon. In the field of Cyber Security there has been a transition from the stage of Cyber Criminality to the stage of Cyber War over the last few years. According to the new challenges, the expert community has two main approaches: to adopt the philosophy and methods of Military Intelligence, and to use Artificial Intelligence methods for counteraction of Cyber Attacks.Cyber security is not only a problem related to a person. It is even for an organization and for a government also. Not necessary that each time one can protect data or information on social networking sites but also the information related to bank transactions must have enough security measures. There are several techniques available to protect information on net naming a few are password security, authentication of data, malware scanners, firewalls, antivirus software etc. By implementing proper cyber ethics, majority of cyber attacks can be prevented. In a nut shell, computer security is a very broad area which is becoming significantly important as the world itself turning into digital mode with networks being used to carry out vital transactions.The benefits of AI cybersecurity in the hospitality industry include increased protection of sensitive guest data, improved guest safety, and more efficient security operations. AI can help detect potential security breaches and cyber attacks, allowing hotels and other businesses in the hospitality industry to respond quickly and prevent damage. Additionally, AI can help automate certain security tasks, freeing up staff to focus on other important tasks. AI can also help improve physical security measures, such as surveillance cameras and access control systems, ensuring that hotels are safe and secure for guests. Finally, AI can help train and test cybersecurity professionals, ensuring that they are up-to-date on the latest threats and best practices.

3. Results

Artificial Intelligence (AI) is being increasingly used in the hospitality industry to improve customer experience, streamline operations, and increase efficiency. AI-powered chatbots, for example, can provide guests with instant answers to their queries, while AI-powered booking systems can help hotels optimize their room rates and occupancy levels.However, with the increasing use of AI comes the risk of cybersecurity threats. The hospitality industry is particularly vulnerable to cyber attacks because of the large amounts of personal data that hotels collect from guests, such as credit card information and passport details. To combat these threats, hotels are turning to cybersecurity solutions that use AI and machine learning to detect and prevent cyber attacks. One such solution is the use of blockchain technology, which can provide a secure and transparent way of storing and sharing data. Blockchain technology can also be used to create a secure digital identity for guests, which can help prevent identity theft and other cyber threats. By using these solutions, hotels can provide a secure and seamless experience for their guests, while also increasing their operational efficiency and profitability.

4. Conclusion

In conclusion, Artificial Intelligence (AI) has the potential to revolutionize the hospitality industry, but it also poses cybersecurity risks. The hospitality industry is particularly vulnerable to cyber attacks because of the large amounts of personal data that hotels collect from guests. To combat these threats, hotels are turning to cybersecurity solutions that use AI and machine learning to detect and prevent cyber attacks. Artificial Intelligence (AI) and Machine Learning (ML) have both negative and positive effects on cybersecurity.

AI algorithms use training data to learn how to respond to different situations. They learn by copying and adding additional information as they go along. This article reviews the positive and the negative impacts of AI on cybersecurity.Blockchain technology is another solution that can provide a secure and transparent way of storing and sharing data, and can help prevent identity theft and other cyber threats. By using AI-powered cybersecurity solutions, hotels can provide a secure and seamless experience for their guests, while also increasing their operational efficiency and profitability.

REFERENCES

Nam, K., Dutt, C. S., Chatbot, P., Daghfous, A., & Khan, M. S. (2021). The adoption of artificial intelligence and robotics in the hotel industry: Prospects and challenges. Electronic Markets, 31, 553-574.

Zhang, L. (2022). Artificial intelligence assisted cyber threat assessment and applications for the tourism industry. Journal of Computer Virology and Hacking Techniques, 1-17.

Millauer, T., & Vellekoop, M. (2019). Artificial intelligence in today's hotel revenue management: opportunities and risks. *Research in Hospitality Management*, *9*(2), 121-124.

Alawadhi, S. A., Zowayed, A., Abdulla, H., Khder, M. A., & Ali, B. J. (2022, June). Impact of Artificial Intelligence on Information Security in Business. In *2022 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS)* (pp. 437-442). IEEE.

Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., ... & Choo, K. K. R. (2022). Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artificial Intelligence Review*, 1-25.

Sedjelmaci, H., Guenab, F., Senouci, S. M., Moustafa, H., Liu, J., & Han, S. (2020). Cyber security based on artificial intelligence for cyber-physical systems. *IEEE Network*, *34*(3), 6-7.

Li, J. H. (2018). Cyber security meets artificial intelligence: a survey. *Frontiers of Information Technology & Electronic Engineering*, *19*(12), 1462-1474.

Abbas, N. N., Ahmed, T., Shah, S. H. U., Omar, M., & Park, H. W. (2019). Investigating the applications of artificial intelligence in cyber security. *Scientometrics*, *121*, 1189-1211.

Prasad, R., Rohokale, V., Prasad, R., & Rohokale, V. (2020). Artificial intelligence and machine learning in cyber security. *Cyber security: the lifeline of information and communication technology*, 231-247.

Bhatele, K. R., Shrivastava, H., & Kumari, N. (2019). The role of artificial intelligence in cyber security. In *Countering cyber attacks and preserving the integrity and availability of critical systems* (pp. 170-192). IGI Global.

Alhayani, B., Mohammed, H. J., Chaloob, I. Z., & Ahmed, J. S. (2021). Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry. *Materials Today: Proceedings*, *531*.

Thuraisingham, B. (2020, May). The role of artificial intelligence and cyber security for social media. In *2020 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW)* (pp. 1-3). IEEE.

Mosteanu, N. R. (2020). Artificial Intelligence and Cyber Security–A Shield against Cyberattack as a Risk Business Management Tool–Case of European Countries. *Quality-Access to Success*, *21*(175).

de Azambuja, A. J. G., Plesker, C., Schützer, K., Anderl, R., Schleich, B., & Almeida, V. R. (2023). Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey. *Electronics*, *12*(8), 1920.

Mosteanu, N. R. (2020). Artificial intelligence and cyber security–face to face with cyber attack–a maltese case of risk management approach. *Ecoforum Journal*, *9*(2).

Shamiulla, A. M. (2019). Role of artificial intelligence in cyber security. *International Journal of Innovative Technology and Exploring Engineering*, *9*(1), 4628-4630.

Welukar, J. N., & Bajoria, G. P. (2021). Artificial Intelligence in Cyber Security-A Review. *International Journal of Scientific Research in Science and Technology 2021*.

Das, R., & Sandhane, R. (2021, July). Artificial intelligence in cyber security. In *Journal of Physics: Conference Series* (Vol. 1964, No. 4, p. 042072). IOP Publishing.

Vähäkainu, P., & Lehto, M. (2019, February). Artificial intelligence in the cyber security environment. In *ICCWS 2019 14th International Conference on Cyber Warfare and Security: ICCWS 2019* (p. 431). Oxford: Academic Conferences and publishing limited.

Atiku, S. B., Aaron, A. U., Job, G. K., Shittu, F., & Yakubu, I. Z. (2020). Survey on the applications of artificial intelligence in cyber security. *International Journal of Scientistic and Technology Research*, *9*(10), 165-170.

Sadiku, M. N., Fagbohungbe, O. I., & Musa, S. M. (2020). Artificial intelligence in cyber security. *International Journal of Engineering Research and Advanced Technology*, *6*(05), 01-07.

Sagar, B. S., Niranjan, S., Kashyap, N., & Sachin, D. N. (2019, March). Providing cyber security using artificial intelligence–A survey. In *2019 3rd international conference on computing methodologies and communication (ICCMC)* (pp. 717-720). IEEE.

Trifonov, R., Nakov, O., & Mladenov, V. (2018, December). Artificial intelligence in cyber threats intelligence. In *2018 international conference on intelligent and innovative computing applications (ICONIC)* (pp. 1-4). IEEE.

Zhang, Z., Al Hamadi, H., Damiani, E., Yeun, C. Y., & Taher, F. (2022). Explainable artificial intelligence applications in cyber security: State-of-the-art in research. *IEEE Access*.

Sivasankar, G. A. (2022). The Review of Artificial Intelligence in Cyber Security. *International Journal for Research in Applied Science & Engineering Technology, 10*(01), 61-68.

Bonfanti, M. E., Cavelty, M. D., & Wenger, A. (2021). Artificial intelligence and cyber-security. In *The Routledge Social Science Handbook of AI* (pp. 222-236). Routledge.

Ghillani, D. (2022). Deep Learning and Artificial Intelligence Framework to Improve the Cyber Security. *Authorea Preprints*.