ARTIFICIAL INTELLIGENCE AND CYBERSECURITY IMPLICATIONS FOR BUSINESS MANAGEMENT

Philippe Funk

SMC Business School, Pope Urbanus VIII Street, B'Kara BKR 1425, Malta

Structuralia, Engineering eLearning partnering with Universidad Isabel I, Av. de la Industria 4, Edificio 1 - Oficina 1-B Alcobendas (28108) Madrid

Abstract

The cybersecurity market is a fast-growing market due to cybersecurity's ever-changing nature of attacking and defending. Organizations need to find new ways to counter cybersecurity threats. Artificial Intelligence (A.I.) has the potential to create disruptive change, both for good and evil. To better manage cybersecurity within organizations, companies must look at how technology can be used with the people who use it daily. By implementing artificial intelligence, cybersecurity teams can make faster decisions, allowing them to move faster than attackers. Business management using artificial intelligence can help organizations make more informed business decisions about their products and services. Cybersecurity and artificial intelligence must work together to increase cybersecurity awareness within organizations. This paper discusses cybersecurity and artificial intelligence implications on business management using cybersecurity journals, websites, company information, and military information sites. It also uses artificial intelligence journals and the author's experience in cybersecurity training. It highlights that when it comes to artificial intelligence (A.I.) and cybersecurity, businesses need to be aware of the potential implications for their management and operations. With the ever-increasing sophistication of A.I. technology, cybercriminals find new ways to exploit vulnerabilities in systems and networks. As such, businesses need to understand the risks associated with A.I. and cybersecurity to take steps to mitigate them.

Keywords: *cybersecurity, artificial intelligence, implications, business management, implementation, decision making, cybersecurity awareness, management and operations, A.I. technology, vulnerabilities, risks associated with A.I., mitigation*

1. INTRODUCTION

The advancement of information technology has enabled organizations to operate faster than ever before, especially as far as the provision of customer services is concerned. Additionally, such advanced operational systems have made it possible to manage their resources effectively and efficiently. Most organizations, however, are yet to understand the potential benefits that accrue from the use of A.I. and related technologies. Many companies and governments are currently exploring these aspects of knowledge management to maximize the value they can derive from these new forms of computing power that are taking shape within our digital age. As such, there is a need for business executives to devise strategies that will enable them to leverage the advantages emerging from what is referred to as artificial intelligence. According to management experts, businesses can utilize artificial intelligence effectively in terms of cost reduction and increased business efficiency (Rosário and Raimundo, 2021).

The current state of affairs has led to the establishment several areas of interest and opportunities for businesses. Businesses have sought to capitalize on their opportunities by applying the latest advancements in intelligent manufacturing to the manufacturing sector. An excellent example of such a situation that has emerged in the last two years is the adoption of Smart Manufacturing instead of traditional manufacturing (Elsner & Hart, 2017). Instead, Smart Manufacturing focuses on leveraging and integrating intelligent equipment in manufacturing environments. In addition to having these integrated devices that connect to sensors and other elements, such systems can automatically collect relevant data sets in real-time to inform decision-making and planning. Such tools that come from A.I. are a clear indication that even if any business owner does not see any difference between the company's

current assets and the ones being used by the future generations, the implication of adopting A.I. is vast. Almost every modern organization has started using A.I. to save time and reduce the prices and costs of manufacturing products. Many banks prioritize strategic technology development by investing in artificial intelligence programs to serve their customers better, enhance productivity and increase revenue. Over the years, the global age has evolved; media have moved from television, radio, and newspapers to the Internet and are slowly and steadily adapting to artificial intelligence (Rana et al., 2021).

A.I. can reduce the time it takes to process facts, assesses customer threats, and decide on customers' ongoing control and fate. One of the most challenging situations that large organizations, banks, insurance companies, and financial institutions face when implementing A.I. is that large amounts of their past data are stored in paper files and not in digital areas. A quirk learning machine is necessarily trained in virtual reality, so financial institutions should make sure they digitize old documents long before hiring experts to develop A.I. solutions or buying A.I. software. Artificial Intelligence may be used in any phase of the business process, including the front, middle, and back offices. Artificial Intelligence may be used in any business. Regardless of the industry and any place, there are a lot of computer-to-computer connections. In terms of cyber security, humans might still be the weakest link. (Xu and Babaian, 2021). Although machine-to-machine data learning and Artificial Intelligence might assist deal with cyber-attacks, a careless user could harm the entire system, which is impossible to predict. I.T. security administrators should understand how to think about using the Internet before employing any new technology.

2. MATERIAL AND METHODS

The keywords or terms considered relevant fall into two categories; with different meanings. Those related to intelligent systems "artificial intelligence, machine learning, and deep learning and its relation with business management" and those related to security "cyber security, record security, internet security, and network security. "Phrases from each category are combined to form search terms that include artificial intelligence and/ or cybersecurity, machine learning, and/ or cybersecurity. The search criteria have been changed to published studies from 2008 to 2021: this allows for interest in research methods over a more extended period. The IEEE and Association for Computing Mechanisms (ACM) Virtual Libraries were considered the most appropriate databases for data collection, as initial searches indicated a limited number of related studies in the region across several scientific databases. It can be said that the IEEE and ACM scholarly databases are considered to be the primary databases for the study of knowledge in the field of computer technology, and lots of searches were carried out.

Furthermore, numerous studies were taken from the IEEE search database. However, some inappropriate articles were moved to the ACM digital library. All studies met the inclusion and exclusion criteria. As per the inclusion and exclusion criteria, peer-reviewed journal articles, Textbooks, short articles, and conference reports were all included; however, websites were excluded. This ensures that each selected survey is continuously reviewed and/ or reviewed by two external stakeholders for first-class accuracy.

2.1 Research Method

This research has used a qualitative method while collecting data and determining results. There are two kinds of data, primary and secondary. In this research, the researcher has used secondary data to analyze.

2.2 Research Approach

The interpretivism research philosophy was chosen for the study. The researcher chose interpretivism because he intended to dig further into the research issues by examining the human views around the variables. The qualitative research design was chosen as the study approach since it aided the interpretivism philosophy and allowed the investigator to delve deeply into the issues. Interpretivism philosophy helps researchers obtain rich and vast knowledge about their study topics, making it superior to any other philosophy. Interpretivism is a study philosophy that focuses on human behavior by taking

personal interpretations from social activities into account. This concept is based on subjective, opinion, and perspective-based evidence and can be regarded as the polar opposite of positivism.

3. DATA ANALYSIS

For the data analysis of this research, the researcher used thematic analysis. The thematic analysis method is recognized as one of the few Green Record classification schemes widely used in qualitative research. Using thematic assessment, researchers create topics based on information collected during interviews (Braun et al., 2018). In this observation, thematic analysis is used to interpret the results of the secondary data. Research has found that thematic analysis is the most applicable method of interpreting the collected facts. Thus, the purpose of using the thematic analysis method in this study is to give a clearer picture of each of the factors that can be observed. In addition, this study depends entirely on the design of qualitative studies; this reflects a thematic analytical approach that is most suitable for assessing the facts.

The thematic analysis method is mainly used to analyze qualitative records, which may additionally include case studies, general qualitative, phenomenological, and narrative studies (Vaismoradi et al., 2016). Therefore, in considering the qualitative nature of this view, an objective analytical approach was used to ensure the validity of the study results. The following is the use of an objective inductive method to translate the collected data to deepen the understanding of the research subject. Conducting thematic analyses started with examining the data, generating raw code, researching, evaluating, identifying, and writing themes. Thus, incorporating most of these steps into the objective analysis method allowed the researcher to maintain the correct flow of facts and give the appropriate interpretation to draw a conclusion.

4. RESULTS

4.1. Artificial Intelligence as Technology Solution to Improve Important Areas of Business Management

Artificial intelligence (A.I.) is a technology solution to manage business and customer service. A.I. is the science and engineering discipline that focuses on developing technologies that can be used for intelligent, automated, or even self-learning systems (Sabillon et al., 2021). The fact that we live in the era of consumerism and personalized service has brought forth a new generation of consumers. They have a high preference for customized products and services offered by services companies. Today, almost all businesses have recognized that it is crucial to create tech solutions that are easy to consume, adaptable, seamless, and accurate. For instance, it is essential to develop platforms that deliver quick and transparent answers to queries that arise as a consequence of interactions with various systems (Lee, 2021).

It has become increasingly clear that organizations across every industry are making tremendous investments in cutting-edge technology in recent years. However, many companies see this investment as an essential means of leveraging their strengths, enhancing competition, and winning customers' hearts and minds. In other words, they seek out opportunities to create new capabilities while gaining market share (Duhigg et al., 2017).

A.I. is one such opportunity to capitalize on the human potential for knowledge and learning. Companies that understand how to use it in innovative ways will emerge ahead of competitors and gain a competitive advantage that leads to increased profits and more excellent long-term value to shareholders. Thus, using "artificial intelligence" (A.I.) at your company's core means understanding its advantages and disadvantages. A.I. applications have overgrown from simple models created by humans to complex algorithms that now take input from thousands of data sources daily and quickly churn through thousands of results. Consequently, there are several aspects of A.I. application at different levels. These include the following: A.I. at the product level – This includes everything from chatbots to virtual assistants that assist employees with tasks (Taeihagh, 2021). It also includes data analytics, machine learning, natural language processing, etc. This type of A.I. can create revenue streams for businesses

by selling their information, allowing consumers to find what they want, and enabling brands to sell products that meet the needs of both customers and employees within their reach (Razzaque, 2021). A.I. at the division level – A.I. is applied at most divisions using strategies that have been developed over decades or centuries through practice and observation. For example, if the marketing department uses advanced analytics to focus its efforts on creating customer relationships, then that branch would benefit from having a team of highly trained and experienced marketers. Similarly, if the accounting department implements A.I. to automate critical processes, then a key focus should be placed on automating repetitive work and reducing manual errors (Sarma et al., 2021).

When artificial intelligence is implemented at the function level, many functions that require intelligence, such as finance, administration, legal, health, and others, currently function on a limited amount of data. Nevertheless, much analysis needs to happen in-house because of a lack of available data. With AI, the organization could collect data rapidly. A.I.'s speed and accuracy could allow staff to do more work faster and effectively. Also, AI-enabled robots and bots could facilitate the collection of vast amounts of data.

On the other hand, artificial intelligence applications at the firm level (Mohammad Hosseini et al. 2021). Most companies now provide some degree of automation of tasks to achieve specific goals, such as cost-cutting initiatives, time-savers, etc. While some organizations already have established procedures and policies for how employees interact with computers and robots, A.I. is the next phase of automation that could ultimately lead to even greater efficiencies. An excellent way to get started with this process is to think about what tasks your company traditionally employs. Ask yourself if any of those tasks involve intelligence, whether or not they need to, and where they can be managed. If so, it makes sense to immediately put A.I. into action (Du and Xie, 2021).

As per the result, A.I. is an efficient resource for any organization because it is applied to various areas throughout the enterprise, such as Sales Support, Customer Service, Marketing, Advertising, Finance, H.R., and more. The research shows that A.I. could add value to any organization. An Artificial Vision and Natural Language Generation (A.I.) bot that automatically assists sales representatives in responding to questions posed to them by management. Sales support teams are often overwhelmed, and it can be difficult for managers to provide clear explanations of why specific actions need to be taken and the outcomes associated with those actions. An A.I. system can be designed to handle the repetitive tasks involved in doing this sort of work. By taking care of the tedious details, the human support reps can focus on providing expert guidance and feedback to prospects and clients. Moreover, the tool can analyze historical trends and identify changes in behavior that it believes were related to change efforts, thereby making smarter decisions (Cao, 2021).

A.I. can be used to help deliver accurate and relevant content to consumers. Customers today expect instant replies to their queries and expectations regarding the information they receive. Brands must strive to improve customer experience by empowering customers by delivering fast, personalized experiences without compromising the quality of services. Today's customers expect quick response times and high-quality communications via email, text message, social media, mobile apps, web chat, and push notifications. Unfortunately, some organizations have found it challenging trying to balance competing priorities. For example, banks and credit card providers are often under pressure to maintain a competitive edge over their rivals because they serve millions of customers daily, and they want their customers to feel satisfied (Griffin & Moorhead, 2014). On the other side, some organizations have been unable to keep pace with an evolving consumer market, which means they need new approaches to give them that necessary edge. In the recent past, there have been identified three ways in which the company built a seamless digital relationship. One was to use A.I. to boost personalization and relevance while continuing to offer real-world expertise so that the bank could meet the changing needs of diverse populations. According to research conducted by (PwC, 2017), 60% of corporate executives believe that A.I. will play a positive role in their future business plans.

If Artificial intelligence is implemented correctly, A.I. could be a valuable solution to managing business strategy and performance. Here are some benefits of implementing A.I. at your company: many large corporations already conduct some analysis for their customers to understand their behavior better. Having access to these reports, experts at B2B marketers could better design campaigns, create targeted

messaging or follow up with sales leads, and more. Automation could further streamline the process, offering insights into customer behaviors that make it easier to plan and execute marketing campaigns (Cihon et al., 2021). A.I. allows companies to respond quickly to unforeseen events and challenges, including weather conditions, economic downturns, and unexpected disasters. It can increase the flexibility of your business model and allow you to deploy resources at your optimal efficiency and scale. Implementing A.I. as part of a larger initiative can help ensure and continue to grow the bottom line while increasing employee productivity and satisfaction (Khan et al., 2022).

Most importantly, An A.I. platform that helps employees communicate across channels, such as email, calendar, Slack, Google Hangouts, Zoom, Whatsapp, etc., allows employees to exchange ideas and express thoughts in real-time, especially during stressful or vulnerable moments. That aspect of collaboration and conversation empowers employees to work together regardless of geography, location, or language, giving them a chance to improve productivity and drive innovations. An A.I. platform that creates visibility into the process of generating data critical to the company can help in empowering the audience to make educated decisions about how brands and services can best contribute to their success by helping them make informed decisions about products and services. It generates leads and builds trust by enabling them to easily connect with the team via various communication platforms, such as Slack Rooms, to engage with colleagues in real-time (Duhigg et al., 2015).

4.2. Artificial Intelligence and Cybersecurity help keep Employees and the System Safe in the organization.

The adoption of artificial intelligence systems has resulted in changes and transformations in employee safety. From workplace accidents to sexual harassment, a myriad of concerns have surfaced regarding protecting workers employed by companies. However, unlike in previous decades when only human beings were allowed to take care of their jobs, there is now ample evidence that machine learning solutions can be used to avoid instances where workers are exposed to harm. Based on the existing literature, employers now have an imperative responsibility to educate their workers concerning the risks, especially when exposure is higher. This directly relates to preventing injuries and accidents within places of work (Mullions, 2011).

According to (Bain & Company, 2016), addressing the issue of worker safety requires a combination of different activities that ensure adequate preparation of the workforce, including training, awareness campaigns, improved working conditions, and effective communication channels to reduce cases of injury. At the same time, these efforts need to be supported with appropriate measures that will help mitigate burnout in staff members who may succumb to fatigue because of long hours spent indoors and the development of healthy habits and physical fitness to reduce occupational complications. Consequently, focusing on workplace health can only happen once the entire workforce understands and works towards addressing these issues (Du and Xie, 2021).

In today's business world, where day-to-day operations are highly intergenerational, online data and structures have become a company's most valuable asset. Violation of the protection of unmarried couples can bring an organization to the brink of bankruptcy or completely tarnish its reputation. Therefore, it is crucial to have an authorized cybersecurity team. I.T. outsourcing tasks are getting more popular these days, but you have to be more careful with the people who trust the agency for security when it comes to security. Cybersecurity professionals must respond to the idea that business is under constant siege. This happens regularly as hackers use various methods 24/7 to gain unauthorized access to a device or break into a network. The A.I. revolution has led to several significant developments related to social firewalls. Previously, organizations had to manually configure their firewall and decide which I.P. addresses to allow and which to block. Nevertheless, A.I.'s intelligent firewall can instantly detect security threats and update them to receive instructions on how to take them on the go (Bonfanti et al., 2021).

Another practical, real-world example of mobile A.I. is email filtering systems. The amount of spam sent daily is enormous. While top-notch promotional emails include state-of-the-art spam filters, and 45% of all emails sent on any given day are spam, even the most sophisticated previous-generation artificial intelligence has a hard time saving them. Machine learning tools can be trained to immediately

detect and report suspicious content. As? It is all about the templates. The device exploration method thoroughly and quickly demonstrates a mobile application using many years of logs and allows algorithms to analyze functions and movements. This allows the A.I. engine to find problems more often than the old method — it feeds a list of blacklisted words to the application and mercilessly prints any message containing it (Bonfanti et al., 2021). A.I. helps maintain compliance and security when dealing with sensitive data. When working with government agencies, you must comply with numerous regulations to operate in the international marketplace. A smart idea would be to combine A.I. with data governance to provide the proper controls and oversight for the integrity of all data assets.

Moreover finally, A.I. can help prevent the loss of files, documents, backups, and software. Consequently, implementing A.I. is an easy road to take, but the reward is substantial for anyone who takes advantage. Through education, engagement, and practical application of A.I., consumers will be more receptive to the future of commerce and the jobs of tomorrow (Choi, 2021).

4.3. Artificial Intelligence Improves the Productivity at Workplaces

Cognitive computing systems such as A.I. are bound to improve modern workplaces' productivity. According to (Wisskirchen et al. 2015), advances in computing capacity have increased the speed of performing repetitive tasks, leading to a decrease in the cost of investing in hardware. Nevertheless, this improvement is not limited to the performance of employees in the workforce but also extends into the management of those functions outside the organization. As mentioned earlier, the ability of A.I. to automate repetitive workloads is very beneficial because it improves the quality of services provided to clients since the results obtained through AI-assisted research and analysis result in superior outcomes.

Research from McKinsey shows that 52% of organizations are already using cognitive computing solutions at some point or another. In 2017, 73% of businesses were expected to implement Cognitive Computing platforms by 2019 (Hassanein et al., 2020). These statistics indicate that businesses are looking forward to leveraging cognitive computing solutions, which will offer opportunities to enhance their competitiveness in the market. Cognitive Computing solutions enable business leaders to focus on matters and make decisions based on facts rather than emotional factors. Consequently, they are bound to improve productivity in business environments and an overall enhanced customer experience. In turn, the result is an overall better chance for business expansion. Therefore, cognitive computing is bound to positively influence business growth despite being disruptive (Alhayani et al., 2021).

According to experts, global executives view using A.I. as part of how their organization becomes more competitive in market environments. Organizations that fail to seize these lucrative opportunities by incorporating smarter and interactive systems that make it easier for employees to communicate and collaborate with stakeholders in real-time become increasingly vulnerable. It is important to note that while organizations would like to think that embracing these concepts means embracing smart technologies instead of outsourcing them, the reality is quite the opposite. Owing to widespread demand from customers, the industry expects to continue seeing strong demands from startups. As a result, implementing robust artificial intelligence frameworks that incorporate intelligent products, processes, and approaches is critical in ensuring modern organizations' continued success in meeting the growing needs of customers (Alomari et al., 2021).

5. DISCUSSION

Data integrity (especially confidential or personal statistics) is now more critical than ever. Hackers are getting smarter every day and can be more resourceful when exploiting the partial data of individuals, corporations, and governments. With new cyber-attacks, statistical bridges, gaps, information poisoning, hacks, and crashes are exposed daily. Cybercriminals threaten businesses, corporations, governments, and customers using computer networks (Chehri et al., 2021). Network attacks are getting more sophisticated, and cybercriminals are getting more sophisticated every day. This forces agencies and other computer network customers to pay for a service that approaches their network security. Cybersecurity refers to technologies and practices designed to protect networks and statistics from

damage or unauthorized access. This is vital as governments, corporations, and military establishments maintain and store many facts and how they work (Cihon et al., 2021).

Cybersecurity takes on unique forms, including military, law enforcement, judicial, commercial, infrastructure, domestic systems, intelligence, and statistics. Cybersecurity is a dynamic and interdisciplinary subject related to statistical foundations, computer science, and criminology. The security goals were availability, authentication, confidentiality, non-repudiation, and integrity. It includes more than one problem related to people, processes, and technologies (Du and Xie, 2021). Cyber-attacks threaten the work of business organizations. They range from crimes committed by citizens (hacker attacks) to corporate actions (terrorists). Cyber-attacks or threats include malware, phishing, carrier denial attacks, social engineering attacks, and man-in-the-middle attacks. Cyber security involves reducing the risk of cyber-attacks. Cyber risks need to be actively managed through controls. Cybersecurity technologies are widely used along with firewalls (Barta and Görcsi, 2021).

There are many interdisciplinary intersections between artificial intelligence and cybersecurity. Artificial intelligence mechanisms (such as expert systems, computational intelligence, neural networks, intelligent providers, artificial immune systems, system domain, information mining, template reputation, ambiguous judgment, heuristics, etc.) allow security professionals to learn about the cyber environment counteract prejudice. The use of A.I. can help expand the horizons of existing cybersecurity solutions. To improve existing cybersecurity systems, organizations can monitor A.I. in four areas: automatic protection, cognitive security, intruder analysis, and dynamic parallel monitoring. Automated protection. There are two types of cybersecurity architecture: expert (analytics-driven) and automated (systems-driven) (Khan et al., 2022). Specialized structures are designed and managed by humans, even in the case of mechanical structures with smart A.I. tools. Most AI-based frameworks are self-contained and independent vendors. An example of a computerized system is CAPTCHA (Turing's fully automated public test to distinguish between computers and humans). Without automation, humans cannot handle the speed and volume of security-critical datasets in cyberspace. As networks look more extensive and complex, artificial intelligence can be a massive asset to an organization's cybersecurity. Ideal electronic security screens for fully protected users, all functions retained. Automated A.I. systems can be integrated into existing cybersecurity functions. These capabilities include: Creating more accurate biometrics-based login technologies, detecting threats and malicious activity with predictive analytics, improving learning and analysis with natural language processing, and securing conditional authentication and access (Alhayani et al., 2021).

6. CONCLUSIONS

In the practice of modern companies, artificial intelligence plays an essential role in the operation and management of companies. Thus, A.I. can be used to process, manipulate, or support the day-to-day aspects and functions of a business. There are many benefits to using A.I. in managing operations and overall business data. A.I. algorithms are already helping more agencies manipulate their data through in-depth analysis, and many unique industries are already using A.I. in their operations. Businesses have found that using A.I. strategies allows them to identify environmentally friendly driving patterns based on the ability of A.I. to get data. H.R. departments of the businesses are also using artificial intelligence techniques to help them find the best talent on their resumes. A.I. can generate the best candidates with positions based primarily on keywords, and the ability of A.I. helps verify the candidate's data. Thus, artificial intelligence is highly effective in carryout the human resource operations of the company. A.I. enables companies to reduce business costs, increase productivity, and enable last-minute shopping experiences (Raimundo and Rosário, 2021).

Artificial intelligence is one of those systems that is changing the company. However, many agencies are reluctant to integrate and use A.I. and new technologies, mainly due to a lack of knowledge and/ or loss of resources (Marketingcharts, 2017). For companies just starting to implement artificial intelligence, the functionality and financial systems improved. This new technology helped them. However, at the same time, artificial intelligence implies a central customer database for personal and business information with the same attributes. This is useful on the one hand but can also be an excellent

advertisement for a cyber-attack. In this context, organizations need to implement and use cybersecurity equipment and artificial intelligence (Cao, 2021). Cyber-attacks are often aimed at accessing, modifying, or destroying sensitive records, extorting money from clients, or abandoning the standard business approach. In other words, risk control is no longer another category: a cyber-attack that can be covered by cybersecurity. The antidote to this form of randomness is cybersecurity, which is the practice of protecting systems, networks, and packages from digital attacks within the business organization. Artificial intelligence is at the top of the list when defining fraud protection. In addition to buying behavior, the buying and selling of unique devices can be used to combat abnormal behavior and use a card in another country just a few hours after using it elsewhere or trying to withdraw. Another benefit of A.I. fraud detection is that the device does not doubt its superiority (Mohammad Hosseini et al., 2021).

Consequently, artificial intelligence is now part of almost every business organization; it activates business processes, improves productivity, and offers various approaches to speed up verbal exchange methods. A.I. software and automation by A.I. systems perform many tasks previously performed by employees and personnel. The transition to an automated operating environment has resulted in many wasted costs for companies, significant time savings, and slow profit recovery (Razzaque, 2021). AI-assisted automation for different ways of working has taken many companies and organizations to the next level in terms of production and control, so this article explains the role of A.I., tool adoption, and cloud computing in the enterprise. A.I. in the cloud turns them into a discovery hub and also opens up the clouds for reporting and changing technical information. Enterprises can manipulate raw memory structures or databases as important facts in fully AI-driven packages. However, the opposite of A.I. is that it can be deployed to applications using hardware programming configuration devices, and the infrastructure supports software dialects. These packages use absolute survivability to run all A.I. Threshold scanning can quickly diagnose fraudulent preset cases and identify issues with new frames for troubleshooting and reapplying. As a result, the implementation of artificial intelligence has become essential for managing several vital business areas because it provides better technology to overcome management issues of the organizations (Cihon et al., 2021).

REFERENCES

1. Alhayani, et al. 2021 *Intelligent of face cyber-attacks*. Materials Today: Proceedings.
2. Ahmad, T., Zhang, D., Huang, C., Zhang, H., Dai, N., Song, Y., and Chen, H., 2021. *Artificial intelligence in sustainable energy industry: Status Quo, challenges and opportunities*. Journal of Cleaner Production, 289, p.125834.
3. Abioye, S.O., Oyedele, L.O., Akanbi, L., Ajayi, A., Delgado, J.M.D., Bilal, M., Akinade, O.O. and Ahmed, A., 2021. *Artificial intelligence in the construction industry: A review of present status, opportunities and future challenges*. Journal of Building Engineering, 44, p.103299.
4. Alhayani, B., Abbas, S.T., Khutar, D.Z. and Mohammed, H.J., 2021. *Best ways computation intelligent of face cyber-attacks*. Materials Today: Proceedings.
5. Alhayani, B., Mohammed, H.J., Chaloob, I.Z. and Ahmed, J.S., 2021. *Effectiveness of artificial intelligence techniques against cyber security risks apply of I.T. industry*. Materials Today: Proceedings.
6. Alomari, M.K., Khan, H.U., Khan, S., Al-Maadid, A.A., Abu-Shawish, Z.K. and Hammami, H., 2021. *Systematic Analysis of Artificial Intelligence-Based Platforms for Identifying Governance and Access Control*. Security and Communication Networks, 2021.
7. Barta, G. and Görcsi, G., 2021. *Risk management considerations for artificial intelligence business applications*. International Journal of Economics and Business Research, 21(1), pp.87-106.
8. Bag, S., Gupta, S., Kumar, A. and Sivarajah, U., 2021. *An integrated artificial intelligence framework for knowledge creation and B2B marketing rational decision making for improving firm performance*. Industrial Marketing Management, 92, pp.178-189.

9. Bonfanti, M.E., Cavelty, M.D. and Wenger, A., 2021. *Artificial intelligence and cyber-security*. In The Routledge Social Science Handbook of A.I. (pp. 222-236). Routledge.
10. Choi, J., 2021. *Current and future considerations for the use of Artificial Intelligence by the United States Department of Defense*. Robotics & A.I. Ethics, 6(1), pp.1-6.
11. Chehri, A., Fofana, I. and Yang, X., 2021. *Security risk modeling in smart grid critical infrastructures in the era of big data and artificial intelligence*. Sustainability, 13(6), p.3196.
12. Cao, G., Duan, Y., Edwards, J.S. and Dwivedi, Y.K., 2021. *Understanding managers' attitudes and behavioral intentions towards using artificial intelligence for organizational decision-making*. Technovation, 106, p.102312.
13. Cihon, P., Schuett, J. and Baum, S.D., 2021. *Corporate governance of Artificial Intelligence in the public interest*. Information, 12(7), p.275.
14. Cao, L., 2021. *Artificial intelligence in retail: applications and value creation logic*. International Journal of Retail & Distribution Management.
15. Du, S. and Xie, C., 2021. *Paradoxes of artificial intelligence in consumer markets: Ethical challenges and opportunities*. Journal of Business Research, 129, pp.961-974.
16. Hassanein, R.A.A., Al-Qassas, S.A., Tir, F.N.A. and Abu-Naser, S.S., 2020. *Artificial neural network for predicting workplace absenteeism*. International Journal of Academic Engineering Research (IJAER), 4(9).
17. Khan, H.U., Malik, M.Z., Alomari, M.K.B., Khan, S., Al-Maadid, A.A.S., Hassan, M.K. and Khan, K., 2022. *Transforming the Capabilities of Artificial Intelligence in GCC Financial Sector: A Systematic Literature Review*. Wireless Communications and Mobile Computing, 2022.
18. Lee, I., 2021. *Cybersecurity: Risk management framework and investment cost analysis*. Business Horizons, 64(5), pp.659-671.
19. Mohammad hosseini, B., Hadizadeh, M. and Ghafelebashi, S.F., 2021. *The Drivers of Sustainable Cyber Service Offer in the Government with an Emphasis on Maintaining Security Using Artificial Intelligence*. Iran Future Studies, 5(2), pp.35-65.
20. Mendhurwar, S. and Mishra, R., 2021. *Integration of social and IoT technologies: architectural framework for digital transformation and cyber security challenges*. Enterprise Information Systems, 15(4), pp.565-584.
21. Raimundo, R. and Rosário, A., 2021. *The Impact of Artificial Intelligence on Data System Security: A Literature Review*. Sensors, 21(21), p.7029.
22. Rana, N.P., Chatterjee, S., Dwivedi, Y.K. and Akter, S., 2021. *Understanding dark side of artificial intelligence (A.I.) integrated business analytics: assessing firm's operational inefficiency and competitiveness*. European Journal of Information Systems, pp.1-24.
23. Razzaque, A., 2021. *Artificial intelligence and I.T. governance: a literature review*. The Big Data-Driven Digital Economy: Artificial and Computational Intelligence, pp.85-97.
24. Rosário, A.T. and Raimundo, R., 2021. *The impact of Artificial Intelligence on Data System Security: A Literature Review*.
25. Sabillon, R., Serra-Ruiz, J. and Cavaller, V., 2021. *An effective cybersecurity training model to support an organizational awareness program: The Cybersecurity Awareness Training Model (RAM).* A Case Study in Canada. In Research Anthology on Artificial Intelligence Applications in Security (pp. 174-188). IGI Global.
26. Taeihagh, A., 2021. *Governance of artificial intelligence*. Policy and Society, 40(2), pp.137-157.

27. Sarma, M., Matheus, T. and Senaratne, C., 2021. *Artificial Intelligence and Cyber Security: A New Pathway for Growth in Emerging Economies via the Knowledge Economy?* In Business Practices, Growth and Economic Policy in Emerging Markets (pp. 51-67).

28. Xu, J.J. and Babaian, T., 2021. *Artificial intelligence in business curriculum: The pedagogy and learning outcomes*. The International Journal of Management Education, 19(3), p.100550.

29. Wisskirchen, G., Biacabe, B.T., Bormann, U., Muntz, A., Niehaus, G., Soler, G.J. and von Brauchitsch, B., 2017. *Artificial intelligence and robotics and their impact on the workplace*. IBA Global Employment Institute, 11(5), pp.49-67.

30. Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., Zhang, F. and Choo, K.K.R., 2021. *Artificial intelligence in cyber security: research advances, challenges, and opportunities*. Artificial Intelligence Review, pp.1-25.