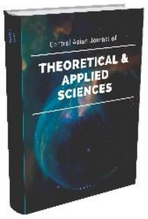

CENTRAL ASIAN JOURNAL OF THEORETICAL AND APPLIED SCIENCES

Volume: 03 Issue: 04 | Apr 2022 ISSN: 2660-5317

Artificial Intelligence and its Application in Information Security Management

O'rinov Nodirbek Toxirjonovich, Yunusov Odiljon Fozilovich
Teacher, Department of Information Technology, Andijan State University
nodirbekurinov1@gmail.com, odiljon.yunusov.71@mail.ru

Received 24th Feb 2022, Accepted 13th Mar 2022, Online 22th Apr 2022

Abstract: *Artificial intelligence (AI) is a technology that can learn, understand and act on the information it receives. AI identifies and prioritizes risks, giving IT professionals the ability to instantly identify malware on their networks and develop an incident response strategy. AI has many applications in information security management, in particular; incident response, disruption prediction, performance monitoring and inventory management. The problems faced by AI in its application for information security management can be divided into digital, physical and political, while the methods of applying AI are artificial narrow intelligence (ANI), artificial general intelligence (AGI) and artificial superintelligence (ASI).). The paper discusses the applications of artificial intelligence (AI) in information security management, discusses its benefits and challenges, and recommends areas for future research.*

Keywords: *artificial intelligence (AI); Computer security; Information security management.*

I. INTRODUCTION

In November 2018, Amazon experienced a data issue when the names and email addresses of its customers became public. In a news post, Amazon blamed the data disclosure on a technical error that occurred on one of its systems [1]. Users affected by data failures were sent a vague email reassuring themselves that the system was secure and that there was no need to change their passwords. However, many users assumed that the email was a phishing attempt, and this situation confused them. Although Amazon was able to seal any information about the leak, many experts argue that the data leak was legal. According to the Identity Management Institute (2020), when a company grants permissions that go beyond any user access needs, there is a high chance of error and more opportunities for hackers to gain access to systems and cause a leak, as happened with Amazon. Over the years, companies have tried to improve their systems with various technologies to protect themselves from the unlimited threats they face in their daily work. One such tool that has helped many firms is artificial intelligence (AI).

Artificial intelligence (AI) has improved a lot over the past few years. Its development has created a wide range of useful applications. However, with the growth of its use in areas such as healthcare and government, there is an ever-growing concern about its resistance to cyberattacks. Like any other technology, artificial intelligence (AI) has weaknesses that can be exploited and thereby threaten the overall security of data management systems in companies [2].

Companies are incorporating artificial intelligence (AI) into their information security systems to mitigate the threats of cyberattacks that have become commonplace in global business. The application has been scaled up by increasing the information gathering state, storage systems, and computing power of system organizations. Artificial intelligence (AI) works by learning the sequences and methods used by management firms and cyber attackers. According to Tolani M and Tolani H (2019), the technology is capable of detecting any form of anomaly that may occur in information management systems. Therefore, their most important task is to detect and prevent.

Interestingly, artificial intelligence (AI) assists in the machine learning process by improving access to specific data management systems by learning the information provided to it. Artificial intelligence (AI) is capable of detecting both present and future threats that organizations have yet to discover with human knowledge. At the same time, artificial intelligence (AI) improves the decision-making process [3]. It helps to create resistive systems that can cope with changes in the environment by providing several variables that improve the overall protection of the control system. (Pal, Tiwari &Maheshwari , 2018).

Contribution: The paper discusses the applications of artificial intelligence (AI) in information security management, discusses its benefits and challenges, and recommends areas for future research. Section II begins by defining the foundations of artificial intelligence and its early adopters. Section III defines and explores the various AI techniques used in information security management. Sections IV and V discuss the security framework of AI in information security management. Finally, section V provides an analysis of the application of AI in information security management.

II. AI BASICS AND FIRST RECEIVERS

Artificial intelligence (AI) is a technology that can learn, understand and act on the information it receives. In today's world, artificial intelligence (AI) works in three ways. The first approach is assisted analytics, which is the most common method used to improve what people and companies are already doing. Further, augmented intelligence is an emerging branch of artificial intelligence (AI) that enables firms and individuals to do things that they might not otherwise be able to do. Finally, autonomous intelligence is under development and will mainly be applied in the future [4]. However, some aspects of autonomous intelligence are already being applied in some countries. An example of autonomous intelligent technology is self-driving cars, which have increased in China and other developed countries.

Artificial intelligence (AI) pioneering companies that consistently use the technology in information security management are Google, IBM, Juniper Networks, and Balbix , among others . For example, Google Gmail uses artificial intelligence (AI) to filter emails and provide users with responses to suggestions. IBM has applied artificial intelligence (AI) to its cognitive learning platform to consolidate the data it uses to detect threats. Finally, Balbix , through its intrusion control platform, uses an artificial intelligence (AI) approach to observe and analyze real-time information that it uses to predict risks and manage vulnerabilities. Balbix has managed to create proactive control over some violations in their system. This technology allows her cybersecurity team to work more effectively with security systems, thereby preventing ransomware and other forms of external attacks [4].

III.METHODS FOR USING AI IN INFORMATION SECURITY MANAGEMENT

As a branch of computer science, artificial intelligence (AI) develops computers that are highly skilled at performing actions that can be described as intelligent. Currently, artificial intelligence (AI) can be divided into three categories applied in information security management: artificial narrow intelligence (ANI), artificial general intelligence (AGI) and artificial superintelligence (ASI).

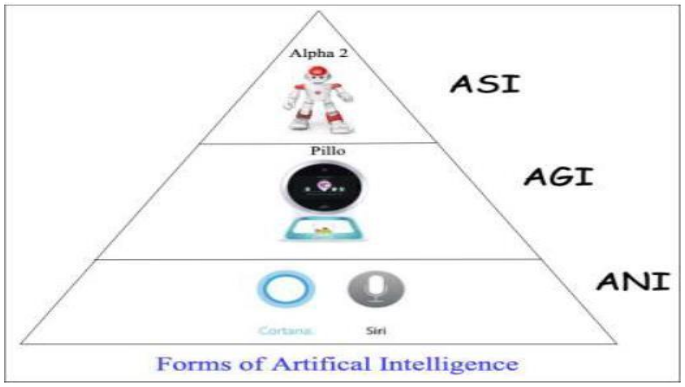

FIGURE 1: FORMSFROMARTIFICIALINTELLIGENCE

A. Artificial Narrow Intelligence (API)

this is the most common form of AI. It's narrow concentrated on the performance a One task and often works in predefined range. So ANI can be defined as a stream intelligence created to perform one task with uniqueness and quick wits. To achieve its goal, technology studies task using built-in savvy, and then moves on to perform it without errors [5]. in human life, especially in Respectfully to Information control, API comes in very convenient. Behind example, This is helps in Information reproduction in smartphones where it exists as Siri or Cortana. In accordance with Sundu and Özdemir (2020), it is also increasingly used in video, image, and audio treatment. Generally, API It has improved control and decision making by allowing companies to to execute One tasks more effectively how people [6].

B. Artificial General Intelligence (AGI)

It is a branch of artificial intelligence (AI) that can think at all. It's an adaptive form of artificial intelligence (AI) that improves based on past learning. In accordance with Baum (2017), he uses learning to make decisions without taking into account any previous impact. It was compared to the human brain, as it can learn and improve when performance specific tasks. Unlike API, AGI can fulfill various tasks. Thanks to the closeness to the person ability, it often mentioned to as strong Artificial Intelligence (AI). An A great example of AGI is the pillo robot , which is used in health care to answer questions about family health problems. the robot is designed and programmed with enough data to guide patients about their health and distribute their medicines [7]. As a data management tool, technology has become timely doctor to get real-time information and help people in performance convenient projects.

C. Artificial Super Intelligence (AS I)

This is is an a kit from intelligence and is an deliberate more dominant and complicated compared to Human intelligence. AS I is an in most effective the form from Artificial Intelligence (AI) as This is can surpass Human intelligence in daily scenarios. He has the ability to think and soften abstractions, a skill that no one else has. Compared to humans, ASI is perfect because it reduces errors by predicting them appearance and development of mitigation strategies. An example of an ASI is humanoid Robot, which was called Alpha 2. Alpha 2 was designed for the family. The robot is designed to control families by managing things in the house. He has a high technical ability and warns people of impending danger such as severe weather conditions before they leave the house in in the morning [2]. AT Information security systems, often used to navigate in system and isolate spaces on conducting penetration testing to improve them systems.

IV. ARTIFICIAL INTELLIGENCE (AI) SECURITY THREATS

Cyber attacks can be divided into integrity, confidentiality, authenticity, and non-repudiation issues . Based on these concerns, AI security concerns can exist in three main ways;

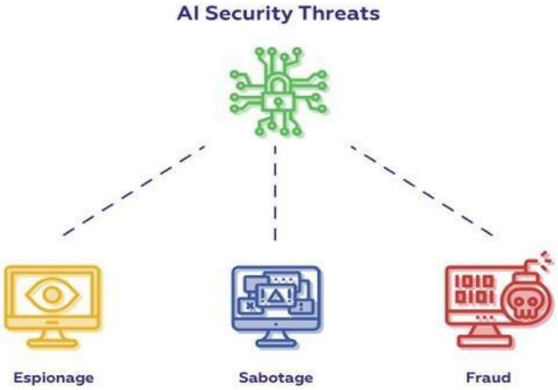

FIGURE 2: AI SECURITY THREATS

1) Espionage- AT computer security, espionage means en individual or the company collects information about information system of another company and uses Information They Receive to plot en advanced attack. Behind e.g. hacker can use AI- based on engine to dig the ground deep in en Information control system and to study more about This is using entrails Like in data sheet [eight].
2) Sabotage- This is means shutdown en Artificial Intelligence systems functionality through model modifications or technology pouring with Requests This is can not pen.
3) Fraud- This is means misclassification roles through data poisoning. Fraud can also involve introduction misinformation or interaction creation with system as a stage of learning to be able to influence in decision This is does [eight].

Malicious use of artificial intelligence (AI) threatens Information security control in many ways, secret under digital, physical, and political security.

A. Digital Security

The threat comes through social engineering and be secret as shown in in Figure 3

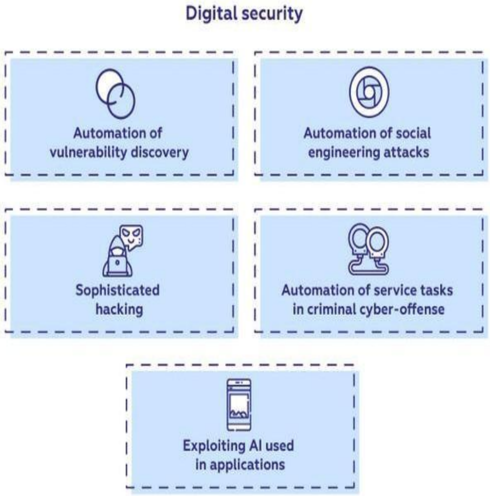
Digital security
Automation of vulnerability discovery
Automation of social engineering attacks
Sophisticated hacking
Automation of service tasks in criminal cyber-offense
Exploiting AI used in applications

Figure 3: Digital Security

1) **automated Social engineering attacks-** Through Easily mimic writing style with NLP tools a victim. This allows AI systems to collect online data about in individual, which can automatically generate malicious links, Email, and sites intended to harm in victim.
2) **Vulnerability discoveries-** AI uses story templates discover vulnerabilities that a hacker can use without knowing victim
3) **Complicated breaking into-** AI can automate goal victims choice on prioritization them vulnerabilities thereby allowing intruders to speed up them breaking into process.
4) **Service tasks for cybercrime -** AI can automate procedures that attack the data flow pipeline, for example, payment processing ("Artificial Intelligence behind Computer security," 2020).
5) **AI statement exploits-** AT Information security, data poisoning creates back door or cripple security protocols used in AI systems.

B. Physical Security

security risks take place on affecting in the car physical security, For example, using armed hard disks.

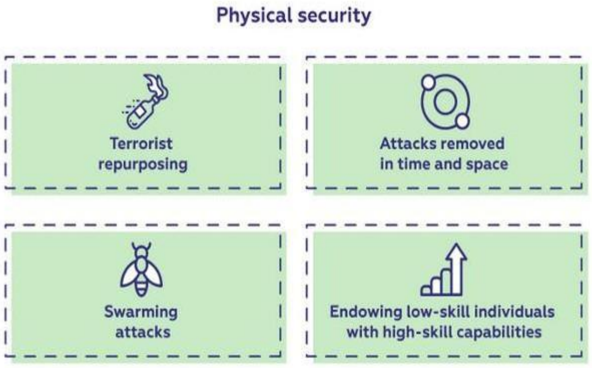
Physical security
Terrorist repurposing
Attacks removed in time and space
Swarming attacks
Endowing low-skill individuals with high-skill capabilities

Figure 4: Physical Security

1) **Terrorist repurposing** - Intruders can use commercial AI systems to violate on the in security rights of others. For example, they may use drones to deliver explosives to the data vault centers
2) **Boundless attacks** - Wireless connection and remote communication in AI systems allows continuous and automated attacks on the data centers
3) **Swarming / Coordination attacks** - Appendix from distributed networks in AI creates autonomous robotic systems that allow weight monitoring and performance from well-coordinated attacks.
4) **highly qualified opportunities-** AI gives alternatives behind attacks on exploitation in Best algorithms, navigation through the system and highlighting the weakest dot.

C. political Security

Threats make an impact society through profiling, surveillance, and automated disinformation campaigns.

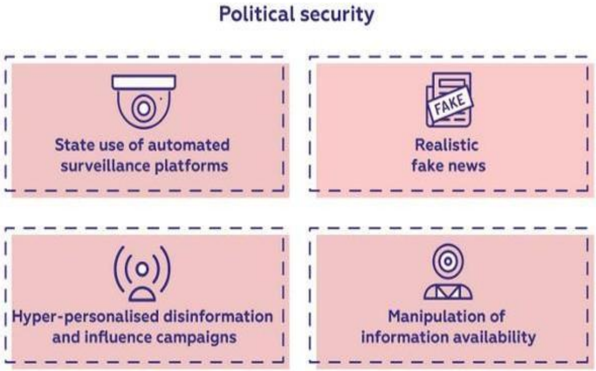
Political security
State use of automated surveillance platforms
FAKE
Realistic fake news
Hyper-personalised disinformation and influence campaigns
Manipulation of information availability

Figure 5: political Security

1) **Fake news** - AI allows behind image and video Generation using natural language methods. This is may also include information about inflammation, since This is is an not easy to check source
2) **automated observation** - State or federal governments can use AI platforms in video and audio treatment to collect and use information from companies and people without them OK.
3) **Personalized Disinformation** - AI in Social Media can to find key negative influencers or faces who offer target disinformation using in Social platforms
4) **Data Manipulation and Controlled Behavior** - AI smart algorithms can manipulate data drive users in taking a detail direction. Behind example, bot-controlled large scale negation- information attacks can be used by companies or people clog their information channels, thereby creating gaps in process acquisitions real data.

V. BENEFITS/APPLICATIONS OF AI IN INFORMATION SECURITY MANAGEMENT

A. Information Technology (IT) Asset Inventory Artificial intelligence (AI) is used to obtain a complete and accurate inventory of the users, devices, and applications that companies or individuals use to access their information systems. AI also helps measure and classify organizations to make inventory management easier [4].

B. Threat Impact

based on AI systems give until now Information on the global and corporate threats. Organizations can use This Information to prioritize them solutions on the which can expose them to attacks and make the necessary adjustments to them systems.

C. Efficiency The control

Organizations need to understand how various security systems instruments and processes O neither have busy can influence them general security and support a stable security pose. Artificial intelligence (AI) can help with this by creating InfoSec program that works stably and warns about existing spaces

D. Forecast from Violation Risks

Except from THIS assets inventory control, threat impact and control effectiveness, AI can also predict how, when and where the company is likely to experience violation. Thanks to this prediction, artificial intelligence (AI) helps organizations plan distribution of tools and resources overcome weakness when is it happening or prevent it before This is happening. Generally, according to "Using Artificial Intelligence in Cybersecurity, (n d), Directive Ideas that AI analysis generates can help en THIS security department to customize and improve their controls and processes. In long run, in Company governs to improve This general cyber sustainability.

E. Answer to Incidents

Artificial intelligence (AI) systems are capable of give it is better contexts behind response or prioritization to security alerts. They are Create a fast response system to dangerous cases and help person or organizations determine in root cause from in incident to avoid future rehearsal.

F. Explainability

Artificial Intelligence (AI) Scanning System seat belt keys that can be used to increase Human Information Security, which is an applicable in explanation analysis and recommendations. According to "The use of artificial intelligence in cybersecurity" (d) the process is essential. It allows management explain to other stakeholders, various programs and staff involved in data control and security.

VI. ANALYSIS

Traditional security protocols are increasingly failing to detect and protect information systems from security threats. AT in recent past, many organizations have recorded situations where they security firewalls were bypassed on cybercriminals who are constantly seeking behind new opportunities for exploitation. Therefore, the best way for companies protect themselves from hackers must accept a cleverer and planned Technics.

Artificial Intelligence (AI) suggestions a wide range from security technologies that have proven effective in detecting security networks unusual behavior in data control systems. Artificial intelligence (AI) systems can detect and report any anomalies present in the datasets with the concept from the car education. The car education is an en aspect from Artificial Intelligence (AI) that includes recognizing data patterns and manufacturing predictions about in effects from these patterns using past education or experience (Tolani M & Tolani H, 2019). Artificial intelligence (AI) systems have the ability to generate results that are considered human related reasoning and functioning.

Artificial intelligence (AI) can isolate compromised data. isolation are important as They help individuals or companies fix deficiencies in their systems and prevent further malware attacks in them networks. AI It has improved the work of security specialists by removing unwanted information noise in the system. Technology learns from provided Information and uses This intelligence to discover abnormal activities insofar as This is can understand in cyber environment [9]. Thus, organizations have the opportunity able to apply artificial intelligence (AI) at three levels in their information security management in an attempt to improve computer security systems and practices that They use;

A. Level one: Prevention and Mitigation

Artificial intelligence (AI) systems are smart can have hidden protection that allow them to prevent data errors, loss or access by unauthorized persons. Systems hire flexible algorithms that to help in control in decision-making to improve them Information security general welfare of the leadership. Prevention and detection happen when the system is new and has not been compromised way (Tolani M & Tolani HOUR, 2019).

B. Level 2: Discovery

AI systems are applied as a basis for understanding normal system activity. Detection is often based on signatures because they depend on the system under study. Everyone the system has a set of rules that depend on recognition and signature update. Everitt , Herzel & Potapov, 2017) claims that AI systems provide internal and external sensors that allow them to discover anomalies in data storage and Transmission. The monitoring software monitors the flow of packets and evaluates digital traffic to guarantee No Confidentiality violation, honesty, confidentiality, and authenticity rights.

C. Level 3: Answer

This is is an in scene with in elementary load insofar as This is determines how effectively AI is used to overcome the dangers he faces. Artificial intelligence (AI) can intelligently change manual tasks such as searching for data using log files to automated tasks. AI can easy to redirect Human efforts and Create value activity based on on the general education and knowledge. Thanks to this, it can facilitate the intelligence response to attacks from or en interior or external perimeter.

An excellent statement from AI in response is an in creation from reasonable traps honey potters that creates a duplicate the environment to lure intruders, reveal gaps in system and reprogram to close this gap. Through artificial Intelligence (AI), some networks can be dynamically split into help redirect attackers from vulnerabilities. Briefly speaking, Artificial intelligence (AI) systems improve skills

Information security control on investigation high- probability signals and focus on sealing the weakest points within in system.

According to Everitt , Goertzel and Potapov (2017), Artificial intelligence (AI) is increasingly being used in education, healthcare and manufacturing due to its adaptability to data control and security. AT in future, This is May be it is possible to create error-free cyber centers with the help of artificial Intelligence (AI) as in technology controlled through the car education.

VII. CONCLUSIONS

Artificial intelligence (AI) has become essential technology behind increase Human efforts in Information security management in recent years. Because individuals and companies can no longer protect their dynamic information systems using firewalls and Other traditional technology, Artificial intelligence (AI) provides an excellent foundation for analyze, protect, soften, discover, and respond to spaces in security protocols that organizations use. AI identifies and prioritizes risk, giving IT the ability to instantly to identify malware within them networks and to generate incident response strategy. As discussed AI It has many Applications in Information security control, especially; incident response, violation prediction, efficiency inventory control and management. However, AI allows cybersecurity teams to develop a powerful and human-like a machine that pushes the boundaries of their data knowledge control and security protocols, thereby stabilizing Information security control.

REFERENCES

1. Identity Management Institute. (2020). Artificial intelligence in information security. Identity Management Center. Retrieved from https://www.identitymanagementinstitute.org/artificial-intelligence-in-information-security/

2. Tolani, M.G., and Tolani, H.G. (2019). The use of artificial intelligence in cyber defense. *International Studies Journal of Engineering and Technology (IRJET),* 6(7), 3084-3087.

3. Pal, TO., Tiwari, R., & Maheshwari , WITH. (2018). Implementation from artificial intelligence methods to deterrence of cyberattacks: an overview. *International Studies Magazine from Engineering and Technology* , 1466-1469.

4. The use of artificial intelligence in cybersecurity. (th). Balbix . Retrieved from https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/

5. Singh, WITH. P. (2019). *Artificial narrow intelligence adaptive sound processing* (PhD thesis, Dublin Business School).

6. Sundu , M., & Özdemir, WITH. (2020). Effect from Artificial Intelligent information about the control process: calls and Opportunities. AT *Problems and Opportunities behind SME in Industry 4.0* (pp. 22-41). IGI Global.

7. Everitt T., Herzel B. & Potapov A. (2017). Artificial general intelligence. *Art Lecture Notes Intelligence. Heidelberg: Springer* .

8. Artificial intelligence for cybersecurity: a double-edged sword. (2020). The science . Retrieved from https://medium.com/sciforce/artificial-intelligence-for-cyber-security-a-double-edge-sword-6724e7a31425.

9. Baum, S. (2017). Examination of an artificial general intelligence projects on ethics, risk and politics. *Global Catastrophic Risk institute Working Paper* , 17-1.