International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 2 Feb. 2023, pp: 813-821 www.ijaem.net ISSN: 2395-5252

Fundamental Study of Hacking Attacks Protection using Artificial intelligence (AI)

Mohd Shamshul Anuar Omar[1], Mohamad Fadli Zolkipli[2]

School of Computing, University Utara Malaysia, Sintok, Kedah, Malaysia[1]
School of Computing, University Utara Malaysia, Sintok, Kedah, Malaysia[2]

Date of Submission: 15-02-2023 Date of Acceptance: 25-02-2023

ABSTRACT : Nowadays, Internet is more vulnerable to cyberattacks that compromise critical information system attributes like confidentiality, integrity, or availability because of the tremendous development of information technology (IT). AI technologies, such as deep learning, have been integrated into cyber security to manage these cyber risks. The most frequent uses of AI are to identify attacks and threats. The mechanisms are created in a way that they must be capable of taking immediate action on their own[1]. These models will safeguard users from hackers by identifying malware, detecting intrusions, and sensing intelligence for any exploitable weaknesses. Various cyber concerns are also circulating at the same time, which will interfere with AI models' sampling, learning, and decision-making processes. Therefore, cyber security defence and protection solutions are required for AI models to counter adversarial machine learning, safeguard machine learning privacy, secure federated learning, etc. This article's main objective is to illustrate the vital role that AI plays in cybersecurity vulnerability identification and hacker protection.

Keywords: cyber security; hackers, Artificial Intelligence, malicious, vulnerability,

I. INTRODUCTION

The word "cyber" is thought to have sprung from the Greek verb "kybereo," which means to direct, control, or steer. Norbert Wiener, an American mathematician, coined the term "cybernetics" to describe computerised control systems at the end of the 1940s. According to Wiener's further explanation, cybernetics is a discipline of study that emphasises the management of machines and living things through feedback and communication [2].

Cybersecurity is defined as "technology, methods, and procedures developed to offer cover to computer network, equipment, programmes, and data from any illegal access"[3]. Information technology security is another name for cyber security.

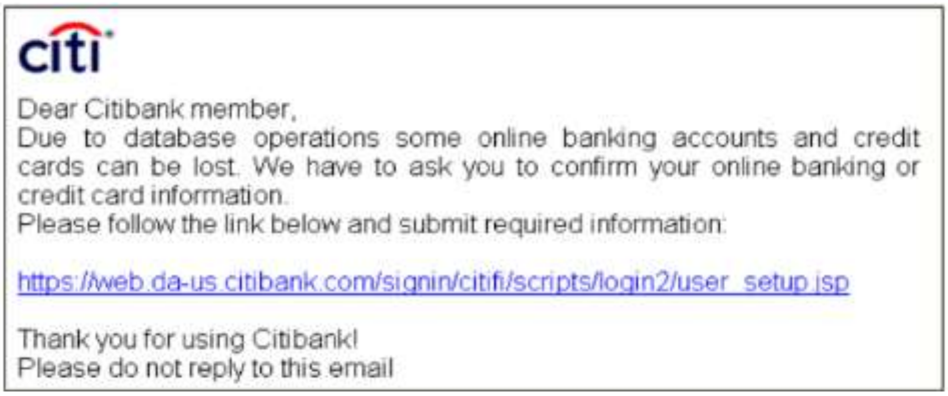
Worldwide spread of the Coronavirus disease 2019 (COVID-19) has made huge impact on almost everything. During the pandemic, people have experienced a major unprecedented and unexpected global public health crisis. It has presented us with changes in our daily behaviour. People have been spending more time on Internet and depending heavily on digital capabilities for work and personal means. As a result, cyber criminals or hackers have exploited the situation and divert the focus to the pandemic situation. Everyone, individually or group have and continue to fall victim to cyberattacks and threats[4]. This has a lot to do in relation to the new normof people working from home (WFH)[5]. Since then, the Internet usage has increased tremendously and At the beginning of 2022, there were 4.95 billion users worldwide, making internet penetration 62.5 percent of the world's population[6].

When Al was first developed, the objective was to replicate the human brain to solve issues effectively in the real world and to learn how to operate human-inspired components, make decisions, and experience emotional experiences. It demands the occurrence of a device that responds and functions like a human mind. AI is a machine-based intelligence, as opposed to human intelligence.Hackers are gaining more skilled and outpacing existing cybersecurity measures as technology develops rapidly. Experts are starting to use Artificial Intelligence (AI) to thwart emerging cyberattacks to stay one step ahead of cybercriminals.

This paper's literature review will concentrate on cyberattacks[7], which are related to information and operational systems[8], as well as their effects on cutting-edge technologies[9], including the Internet of Things (IoT) [22] and applications[10]. The following are various types of attacks that were intended to upset and interrupt the regular operation of computer systems:

a. **Phishing**

Phishing is described as an illegal conduct using methods of social engineering that allows scammers to endeavour illegitimately to obtain valuable information, such as passwords, credit card information, ID information, etc. by posing as a trusted individual or organization in a digital communication[11][12] as depicted in Figure 1.



citi

Dear Citibank member,
Due to database operations some online banking accounts and credit cards can be lost. We have to ask you to confirm your online banking or credit card information.
Please follow the link below and submit required information:

https://web.da-us.citibank.com/signin/citifi/scripts/login2/user_setup.jsp

Thank you for using Citibank!
Please do not reply to this email

Figure 1 : Email phishing that alleges tooriginate from Citibank [11].

b. **False Data Injection Attack (FDIA)**

FDIA is a cyberattack that has been extensively investigated and is well recognised for having a serious impact on transmission networks, and grids, among other systems. It is a form of cyber assault where the hacked sensors reflect fake occurrences. An effectively deployed FDIA will result in inappropriate decisions being made and relevant unintended behaviours, which may have serious consequences like mistreating patients, providing inaccurate diagnoses, and so on.[13]

c. **Ransomware**

Cryptographic ransomware and disruptive ransomware are two fundamental categories of attacks. The encryption method compiles an inventory of file systems before encrypting crucial assets. A screen with instructions on how to pay an anonymous ransom to unlock the data is displayed to victims.[14]

This article will discuss various types of cyberattacks from the traditional and AI eras, their effects on network security, and how to prevent them. The remainder of the essay is written as follows. The literature overview on cyberattacks and the impact of AI is introduced in Section 2. Section 3 covers the effects of AI and how to prevent cyberattacks. The use of AI technologies and approaches in cyber security is examined in Section 4. The challenges are analysed and discussed in sections 5 and 6. The article is finally concluded in Section 7, which is followed by an acknowledgement and a list of references.

1.1 HACKING DEFINITION

Unauthorized use of computer and system resources is known as hacking. The act of modifying computer hardware and software to achieve a goal other than that for which they were originally designed is known as computer hacking. Hackers are people who take part in computer hacking exercises. A hacker is a person who illegally gains access to another people's computer system or personal data.

1.2 TYPES OF HACKING

The following are the list of hacking techniques used by hackers for their attacks :

a. Non-technical attacks: These attacks take use of people as the weakest link in cyber security, according to [15]. Social engineering is defined as the use of people's trustworthiness as a means of obtaining information for nefarious purposes. Physical attacks against data frameworks are another common and effective form. Infrastructures, computer rooms, and other locations with fundamental data or property are broken into by hackers. Among physical assaults is dumpster diving (exploring bins for intellectual properties, passwords, network frameworks and other valuable data).
b. Attacks on network foundations: Given that many networks may be accessed from anywhere in the world via the Internet, hacker attacks against network foundations can be straightforward. A few examples of network foundation attacks are provided below:

- Using a firewall-protected computer and a rogue modem to access a network.

- Making use of TCP/IP and NetBIOS flaws in network transport components.
- Abundant solicitations that overwhelm a network, causing a denial of service (DoS) for legitimate requests.
- Network analyser deployment and monitoring every package passes through it, revealing sensitive information in plain text, and piggybacking on a network using an unstable 802.11b wireless design.

c. Operating-framework attacks: Hackers' preferred method of attack is to compromise operating systems (OSs). OSs include a significant amount of hacker attacks because each computer has one and because there are so many well-known exploits that may be used against them. Occasionally, attacks are made against several OSs that are more secured right fresh from the oven, such as Novell NetWare including some varieties of UNIX. In any case, given their popularity and reputation for flaws, operating systems like Windows and Linux are more frequently targeted by hackers. Here are a few instances of operating system attacks:

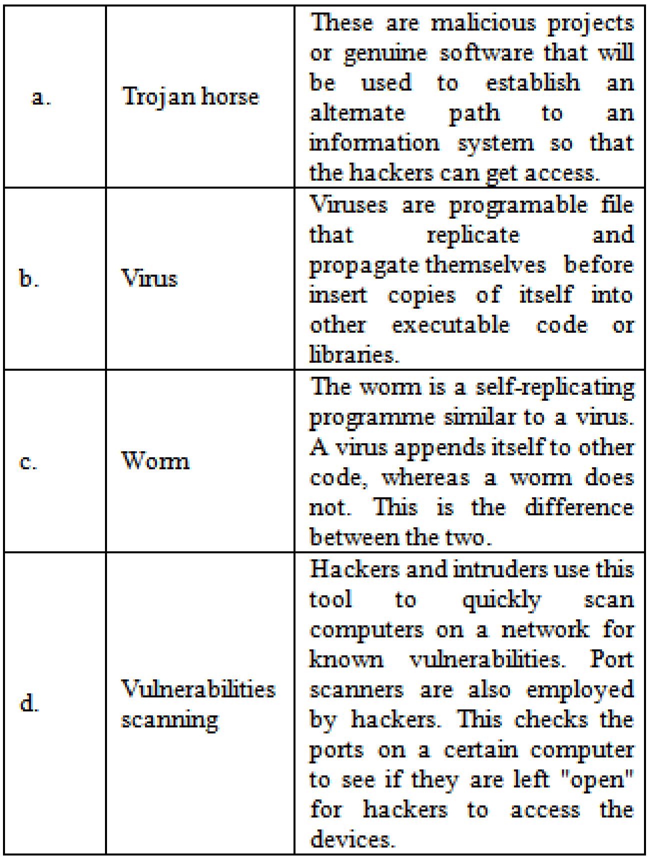
- Making use of protocol exploits
- Attacking in systems of confirmation.
- Breaking records framework security.
- Breaking encryption and password tools.

d. Applications are frequently attacked by hackers, among other forms of attack. Web applications and email server software frequently receive a beating:

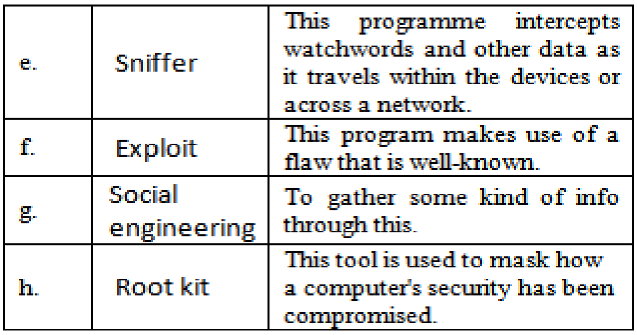
- Majority of firewalls and other security mechanisms are set up to provide total access to these assignments stored at Internet, HTTP and SMTP applications are frequently attacked.
- Infections, worms, Trojan horses, and spyware are all components of malicious software (or malware). Networks and systems are brought down by malware.
- Accessibility and storage space for the framework are being destroyed by spam (junk email). It can also spread malware. Such attacks on your computer systems are discovered by ethical hacking.

1.3 HACKING INSTRUMENTS

Table 1 listed a few tools that hackers frequently use to access networks[15]:



a.	Trojan horse	These are malicious projects or genuine software that will be used to establish an alternate path to an information system so that the hackers can get access.
b.	Virus	Viruses are programable file that replicate and propagate themselves before insert copies of itself into other executable code or libraries.
c.	Worm	The worm is a self-replicating programme similar to a virus. A virus appends itself to other code, whereas a worm does not. This is the difference between the two.
d.	Vulnerabilities scanning	Hackers and intruders use this tool to quickly scan computers on a network for known vulnerabilities. Port scanners are also employed by hackers. This checks the ports on a certain computer to see if they are left "open" for hackers to access the devices.



e.	Sniffer	This programme intercepts watchwords and other data as it travels within the devices or across a network.
f.	Exploit	This program makes use of a flaw that is well-known.
g.	Social engineering	To gather some kind of info through this.
h.	Root kit	This tool is used to mask how a computer's security has been compromised.

Table 1 : Common hacking tools.

1.4 CATEGORIES OF HACKING

The following are list of hacking's categories[15]:

a. Internal Jobs

Most security breaches start off on the victim network itself. Inside jobs include stealing passwords (which hackers then use or provide), performing automated secret operations, inflicting harm (as irate employees), or committing plain abuse. A large percentage of these security breaches can be avoided by employing smart personnel who protect their passwords and devices and sound arrangement authorisation.

b. Rogue Access Points (APs)

Rogue APs are unprotected wireless APs that are easy for outcasts to breach. (Nearby hackers frequently encourage one another to use unauthorised APs.) Rogue APs are frequently linked by amicable but ignorant representatives.

c. Back Doors

Hackers can get into a system by making use of back doors, easy access points, setup errors, easily cracked passwords, and unprotected dialups. Hackers might probably find any weakness in your network with the help of automated searchers (bots).

d. Denial of Service (b) (DOS)

Hackers can take down a network without gaining more internal access by using DOS attacks. Access is flooded with phoney movement in DOS attacks to gain entry via email or Transmission Control Protocol (TCP) ports.

e. Distribution of DOS (DDoS)

DoS attacks are assisted by DDoS from a various origin. A DDoS is highly challenging to counter because it uses several, varying origin IP addresses.

f. Crackers, kiddies, and anarchists:

People who like to destroy things is referred as an anarchist. Most of the time, they take advantage of any random objective. Crackers are specialists or professionals who construct Trojan horses or other software that can crack passwords. Normally it makes internally use of the software (for bragging rights) or sell it. Politicians, fear-based oppressors, disgruntled workers, or anyone else who felt degraded, abused, or taken advantage or hated are just a few examples of the various attackers.

g. Sniffing and spoofing,

The term "sniffing" refers to the act of sneaking a TCP packages. It is possible to capture this person by simply listening covertly. Sending a malicious package including a legitimate affirmation (ACK), which an attackers may determine, anticipate, or get, is known as spoofing by snooping.

II. LITERATURE REVIEW

Access control, antivirus software, cryptographic software, Intrusion detection system (IDS), Intrusion Prevention system (IPS), Sandbox, Security Information and Event management (SIEM), code review and patches are several types of conventional or traditional cybersecurity protection against hackers[1]

These usual well-known security solutions may not be as effective as they were in the early days of cybersecurity, according to [16][17]. The main issue with these conventional systems is that they are typically administered by a small number of knowledgeable security specialists, and data processing is done on an as-needed basis, making it impossible for them to function intelligently according to needs [18]. A more effective strategy utilising AI is necessary in context of current advanced attacks.

The odds of a breach exist even with complete cybersecurity preparation. According to research by [19] on 60 cybersecurity organisations that had experienced a major ransomware assault, 100% of assaults had avoided the antivirus and firewall solutions of the companies.Despite the staff of the organisations having comprehensive cybersecurity training, 77% of assaults evaded email filtering, 52% of intrusions evaded anti-malware solutions, and one third of attacks were succeeded.

The security of online banking can be hacked by phishers utilising cutting-edge tools like the Man-in-the-Middle Attack (MiTM). The hackers want to obtain the information of bank customers [12]. Hackers then utilise this banking information to steal funds or commit fraudulent activity for their own gain, such as sending money and making purchases. Hence, users of e-banking are exposed of being robbed. Deceptive, malicious, and DNS-based attacks are all possible types of phishing[11].

As a result, in recent years, researchers have been investigating ways to use AI to improve cyber-security. AI has been recognised as a flexible method for identifying bogus information and assessing vast amounts of data [20][21]. Dogus information might be coming from the act of hackers using the False Data injection Attacks (FDIA). This type of attacks are considered invisible to the naked eyes. The used of AI tools will surely help in tackling this type of attacks. According to [13], FDIA hackers stole tens of millions of records in 2015 and gained access to the personal data of 80 million patients. It is regarded as one of the biggest healthcare cybersecurity incidents. The hack is thought to have been carried out by Black Vine, a well-funded cyberespionage organisation. The attackers made use of specially created malware known as "Hurix," "Sakurel," and "Mivast."

AI is becoming increasingly popular as a tool for helping users fight crime and address issues in cyberspace. AI primarily aids in the identification of viruses, the design of solutions, and the deployment of solutions that aid in combating cybercrime. Businesses are embracing AI as well because it can improve the security of the internet of things (IoT) by anticipating or identifying criminal activity[22]

[23] claims that AI technologies have had a substantial impact on preventing most of these attacks. This element has been linked to the fact that many firms concentrate on AI-based cyber security to safeguard their organisations' systems. AI was also emphasised by [24][23] as the best strategy for guaranteeing that organizations can prevent intrusions within their enterprises. Additionally, the development of AI-based cyber security solutions has increased [23].

Cybersecurity has also benefited from the advancement of machine learning technology. Utilizing automated features with a quick response time, machine learning ensures safety. As a result, the systems can identify significant dangers and developing defences against such attacks. The key advantage of implementing AI in cyber security is the response time, which encourages this sort of security in comparison to humans. The ability of AI to learn more over time is the second major advantage. With machine learning, AI systems may now get better by learning from their mistakes. The systems are capable of comprehending attack patterns and the best strategies for mitigating these threats. The next benefit of AI-based cyber security is that it can identify novel attacks that people are unable to comprehend. Attackers frequently test out novel concepts [25]. It has been revealed that AI technology provides superior outcomes when detecting new threats and attacks. A vast amount of data can be handled by AI thanks to contemporary technology. This aspect has made it possible for this system to provide improved security and vulnerability control. The results of combining human and AI assistance in cyber security have been much better. This factor demonstrates that greater understanding of AI-based cyber security would successfully deter hacker attacks.

III. OVERVIEW OF ARTIFICIALINTELLIGENCE (AI) IN CYBERSECURITY

AI enormous processing powerenables it to intelligently handle and store significant volumes of data, is one of its key qualities. In a variety of fields, including the healthcare and defence sectors, it has been employed to create intelligent applications. For instance, it has been utilized in the healthcare industry for surgery, treatment, and diagnosis[26]. AI may be summed up as artificially created intelligence that offers tools for tackling challenging tasks on a computer or other equipment. Information technology and biological intelligence are combined to create artificial intelligence (AI), which may be employed computationally to accomplish tasks. Al can programme computers to act like people, but they can also be quicker and more compassionate [2]

3.1 TYPES OF AI-BASED ATTACKS

The following are types of AI-based attacks performed by hackers[1]:

a. The malicious practise of using chat bots to send random emails: Confidential reports can be put together using automation to carry out more sophisticated attacks. By implementing legal sources like help desks, external code depositories, and other internet sources for relevant data that can make the attacker's job easier, AI can be used for automated collection of pertinent intelligence about an organisation, its systems, and identities before this type of attacks.

b. Brute force attack is a technique for predicting passwords through high level programming by converting data into a code and is particularly useful for preventing unauthorised access like passwords. By utilising the new approaches, this can be accomplished through more intelligent attacks such as AI or machine language password guessing efforts.

c. By utilising outdated encryption techniques, a far more sophisticated method of model identification that is simple to make using modern AI technologies can be employed to solve the problem of predicting passwords without losing valuable time.

IV. TOOLS AND TECHNIQUES FOR AI HACKER PROTECTION

Researchers in the current paper are only concentrating on novel forms of AI-powered cyberattacks. The primary three forms of AI-related assaults being studied are[27][28] as illustrated in Figure 1

The above-mentioned types of attacks can be mitigate using different AI-powered techniques include evidence-based approaches, machine and deep learning, natural language processing (NLP), text mining, and prescriptive analytics.[27] studies identified spam filtering, virus protection, and intrusion detection on networks are three security-sensitive apps that increasingly make use of machine learning.

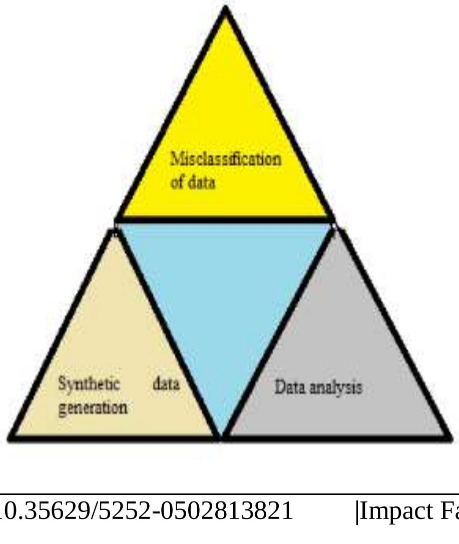


Figure 2 : Three Primary forms AI-related assaults

4.1 AI SECURITY OPERATIONS AND INCIDENT RESPONSE

The following are several examples on AI implementation in various Security Operation Centre and incident response and mitigation processes.

a. A12

An AI platform called A12 has been developed by the Massachusetts Institute of Technology (MIT) and PatternEx to anticipate cyberattacks. This platform detected cyberattacks with an accuracy rate of 86%, which is nearly three times higher than results from earlier investigations. 3.6 billion data elements (log lines) were used in a series of experiments that were run over the course of a three-month study period by millions of people. A12 recognises unusual activity and avoid attacks by using clustering techniques on the input data and optimising unsupervised machine learning algorithms. To establish which occurrences are really attacks, the results will be submitted to analysts. Analysts provide additional learning by incorporating the findings into platform models for the subsequent data set. The system's ability to keep creating new models in just a few hours can significantly improve the system's ability to identify cyberattacks.

b. CylanceProtect

CylanceProtect is a comprehensive data security threat prevention application that employs the advantages of artificial intelligence and information security policy to stop malware infections. Information security mitigation are employed to stop script-based, memory-targeted, or attacks that take advantage of external devices. CylanceProtect optimises AI to detect and avoid any malicious software executed on terminal devices, in contrast to typical security technologies that rely on the study of signatures and user behaviour to detect security vulnerabilities in the environment. Also prevented are any zero-day assaults.

c. Darktrace

Darktrace is a solution for information security that can help to identify the most recent cyberthreats that can elude typical information security measures. To identify anomalies in an organization's information network, Darktrace makes use of machine learning methods, mathematical concepts, and Enterprise Immune System (EIS) technology. EIS uses mathematical techniques, showing that it can recognise previously undisclosed cyber security assaults and does not need to use signatures or laws. EIS is skilled at spotting and countering the majority of skilfully implemented cyber threats, including insider threats that are concealed within information networks. To identify behaviours that point to actual cyber risks, EIS can automatically learn on patterns of user, device, and information network behaviour. Mathematics and machine learning are used to achieve this. Organizations may have a thorough understanding of the information network thanks to Darktrace's self-learning technology, which also enables them to act proactively to attacks and lower risk.

d. Deep Instinct

The implementation of deep learning methods is used to allowed for the detection of harmful software-related structures. Deep Instinct can spot and stop the harmful software. These neural networks were trained using databases containing tens of millions of malicious and benign files. A prediction-based model was the result, and it could be sent to a device to give real-time detection and stop harmful software. The objective is to teach the system to recognise trends in requests and behaviours that indicate malicious software. A GPU cluster processes information significantly more quickly than a CPU cluster. The result is a statistical neural network that can quickly and efficiently identify harmful software.

More than 16 000 dangerous software specimens assembled by Siemens CERT, Bit-Defender, McAfee, AVG, Kaspersky, Sophos, etc. were subjected to a malicious software identification test by the University of Göttingen. All those organizations had their own antivirus software, which had an average detection rate for malicious software of up to 61%, as opposed to Deep Instinct's 98.86% detection rate. While samples of dangerous programs had undergone mutations, their behaviour had not been irreversibly changed. More than 99.7% of hazardous PDF files and 99.2% of malicious executable files might be found using Deep Instinct.

e. SparkCognition DeepArmor

Using mathematical techniques like machine learning and natural language processing (NLP), SparkCognition DeepArmor can identify and stop the danger of malware, viruses, worms, Trojan horses, and ransomware programmes . Its design comprises of a platform for analysing threats and a tiny endpoint agent incorporated with a cloud-based cognitive engine. Regardless of signatures, the terminal agent detects and stops dangerous software and various sophisticated threats. The agent is made to safeguard integrated information security for an enterprise as well as the client, server, mobile, and loT devices. Additionally, an agent can be set up to operate independently without a human interface, offering a security option for loT devices.

V. ISSUES AND CHALLENGES

The following are issues and challenges of AI in cybersecurity protection against hackers[1]:

a. Ransomware rapid evolution:

Ransomware is the horror of cybersecurity. It freezes its victim information and documents. According to [13], in February 2016, Presbyterian Medical Centre's information systems were hijacked by hackers using ransomware. To get their operation back up and running, they sought a $17,000 ransom. Investigation reveals that a worker's opening of a malicious email or download from a pop-up advertisement allowed the malware to be planted in the network.

b. Expansion of AI

Automation could help provide protection from approaching cyberattacks. One benefit of this technological advancement is that you do not have to pay for automated methods that use potent algorithms. Once you have them, they are free to use. They can work around the clock, which is the main benefit.

c. IoT Threats

At the end of 2020, there will be 21 billion connected IoT devices, forecasts Gartner Inc. Meanwhile Forbes predicted there will be 75.4 billion IoT devices worldwide in 2025[12].The younger generation is constantly hooked in. The issue is that because all the component elements are interconnected or connected, users are far more vulnerable to cyber-attacks.[22]

d. Serverless Applications Vulnerability

Cyberattacks are welcome on serverless apps. When users access your application off-server, i.e., from their own devices, they pose a specific risk to user data. You have complete control over the data you saved, whether it is on a server or in the cloud, and the service providers will put in place the necessary security measures [1]

VI. DISCUSSION

The study's overall findings suggested that AI has emerged as one of the key resources for businesses looking to boost their performance in terms of cyber security. Because there is a potential that enormous amounts of data and sensitive information may be targeted by online hackers, the current situation has demonstrated that cyber security is one of the crucial elements that any organisation must assure. The personal and financial information of businesses is saved on the cloud because of fast globalisation and technological advancement, and because of this greater reliance on digital technology, cyberattacks have increased in frequency. The study's conclusions showed that, apart from the expert system, all independent variables exhibited meaningful and favourable relationships. Although many other researchers agree that expert systems are important, this study's substantial results were not attained since the majority view did not agree.

VII. CONCLUSION

Enterprises and technology users must be equipped with practical defence techniques to protect themselves from the constantly growing and increasingly complicated cyber threat scenario. Organizations will effectively protect themselves from danger and potential financial loss by employing technical and human resources like AI to protect the network and linked devices, but they will also contribute to making the internet a more secure and safe place for online users. In conclusion, organizations will become more effective at safeguarding themselves the more they learn about the most recent threat avoidance, detection, and response tactics.

Acknowledgements

The authors would like to thank to all School of Computing members who involved in this study. This study was conducted for the purpose of Ethical Hacking & Penetration Testing Research Project. This work was supported by Universiti Utara Malaysia.

REFERENCES

[1]. B. Geluvaraj, P. M. Satwik and T. A. Ashok Kumar, “ (2018). The Future of Cybersecurity: Major Role of Artificial Intelligence, Machine Learning, and Deep Learning in Cyberspace.,” Data Engineering and Communications Technologies, , p. 739–747, 2018.

[2]. M. Lehto, “Phenomena in the Cyber World. Intelligent Systems, Control and Automation,” Science and Engineering, pp. 3-29, 2015.

[3]. P. Vähäkainu and M. Lehto, “Artificial intelligence in the cyber security environment,” in ICCWS 2019 14th International Conference on Cyber Warfare and Security: ICCWS 2019, Oxford, 2019.

[4]. WHO, “ACCESS TO MEDICINES AND HEALTH PRODUCTS PROGRAMME : ANNUAL REPORT 2020,” WHO, 2020.

[5]. B. &. A. A. Pranggono, “COVID-19 pandemic cybersecurity issues,” Internet Technology Letters, 2021.

[6]. S. Kemp, “DIGITAL 2022: GLOBAL OVERVIEW REPORT,” Kepios, 2022.

[7]. J. Beavers and S. Pournouri, “Recent cyber attacks and vulnerabilities in medical devices and healthcare institutions,” Advanced Sciences and Technologies for Security Applications,, pp. 249-267, 2019.

[8]. D. Dogaru and I. Dumitrache, “Cyber security in healthcare networks,” 2017 E-Health and Bioengineering Conference, EHB 2017, , pp. 414-417, 2017.

[9]. K. Saleem, Z. Tan and W. Buchanan, “Security for cyber-physical systems in healthcare,” health 4.0: how virtualization and big data are revolutionizing healthcare, pp. 233-251, 2017.

[10]. A.Alharam and W. El-Madany, “Complexity of cyber security architecture for IoT healthcare industry: a comparative study,” in 2017 5th International Conference on Future Internet of Things and Cloud Workshops, W-FiCloud 2017, 2017.

[11]. Alsayed and A. Bilgrami, “E-Banking Security: Internet Hacking, Phishing Attacks, Analysis and Prevention of Fraudulent Activities,” International Journal of Emerging Technology and Advanced Engineering, pp. 109-115, 2017.

[12]. J. Saleem, B. Adebisi, R. Ande and M. Hammoudeh, “A state of the art survey - Impact of cyber attacks on SME’s,” in International Conference on Future Networks and Distributed Systems (ICFNDS 2017), Cambridge, UK, 2017.

[13]. M. Ahmed and A. S. Barkat Ullah, “False data injection attacks in healthcare,” in 15th Australasian Conference, AusDM 2017, Melbourne, VIC, Australia, August

19-20, 2017, Revised Selected Papers 15 (pp., Singapore., 2018.

[14]. D. Westerman, P. R. Spence and B. & Van Der Heide, "A social network as information: The effect of system generated reports of connectedness on credibility on Twitter," Computers in Human Behavior, pp. 199-206, 2012.

[15]. Sunil.K, "Hacking Attacks, Methods, Techniques And Their Protection Measures.," International Journal of Advance Research in Computer Science and Management. , pp. 2353-2358, 2018.

[16]. S. Anwar, J. Mohamad Zain, M. Zolkipli, Z. Inayat, S. Khan, B. Anthony and V. Chang, "Intrusion detection to an intrusion response system: fundamentals, requirements, and future directions.," Algorithms, p. 201, 2017.

[17]. S. Mohammadi, H. Mirvaziri, M. Ghazizadeh-Ahsaee and H. Karimipour, "Cyber intrusion detection by combined feature selection algorithm.," Journal of information security and applications, pp. 80-88, 2019.

[18]. D. Berman, A. Buczak, J. Chavis and C. Corbett, "A survey of deep learning methods for cyber security.," Information, p. 122, 2019.

[19]. J. West, "A Prediction Model Framework for Cyber-Attacks to Precision Agriculture Technologies.," Journal of Agricultural & Food Information,, p. 1–24., 2018.

[20]. S. Zeadally, E. Adi, Z. Baig and I. Khan, "Harnessing artificial intelligence capabilities to improve cybersecurity," IEEE Access 8, p. 23817–23837, 2020.

[21]. Chaloob, R. Ramli and M. Nawawi, "A new multi-interval weights approach in fuzzy goal programming for a multi-criteria problem," Int. J. Math. Oper. Res.9, p. 214–229, 2016.

[22]. M. Kuzlu, C. Fair and O. Guler, "Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity.," Discov Internet Things 1, 2021.

[23]. S. Purkait, "Examining the effectiveness of phishing filters against DNS based phishing attacks," Information &amp; Computer Security,, pp. 333-346, 2015.

[24]. M. Ansari, "A Quantitative Study of Risk Scores and the Effectiveness of AI-Based Cybersecurity Awareness Training Programs," International Journal of Smart Sensor and Adhoc Network, pp. 1-8, 2022.

[25]. R. Sabillon, J. Serra-Ruiz, V. Cavaller, J. J. and C. M., "An Effective Cyber security Training Model to Support an Organizational Awareness Program," Journal of Cases on Information Technology, pp. 26-39, 2019.

[26]. S. Kannan, K. Subbaram, S. Ali and H. Kannan, "The role of artificial intelligence and machine learning techniques: Race for covid-19 vaccine," Clinical Infectious Diseases, 2020.

[27]. A.Battista, C. Igino, M. Davide, N. Blaine, S. Nedim and L. Pavel, "Evasion attacks against machine learning at test time.," in european conference on machine learning and knowledge discovery in databases. , 2013.

[28]. Y. Mirsky, T. Mahler, I. Shelef and Y. Elovici, "CT-GAN: Malicious tampering of 3D medical imagery using deep learning.," in 28th USENIX Security Symposium (USENIX Security 2019, 2019.