Impact of Big Data Analytics and ChatGPT on Cybersecurity

Conference Paper · March 2023

CITATIONS
0

READS
147

2 authors:

Pawankumar Sharma
University of the Cumberlands
30 PUBLICATIONS **474** CITATIONS
SEE PROFILE

Bibhu Dash
University of the Cumberlands
39 PUBLICATIONS **622** CITATIONS
SEE PROFILE

Impact of Big Data Analytics and ChatGPT on Cybersecurity

Pawankumar Sharma
School of Computer and Information Sciences
University of the Cumberlands, Williamsburg, KY USA
psharma8877@ucumberlands.edu

Bibhu Dash
School of Computer and Information Sciences
University of the Cumberlands, Williamsburg, KY USA
bdash6007@ucumberlands.edu

***Abstract*—Network attacks and cyber threats are increasingly attaining sophistication every day. There is a rising global number of attacks daily and the diversification of the techniques and methods applied in infiltrating organizational systems and personal gadgets. Such attackers may comprise a whole government, organized groups, or even lone hackers. The alternatives of pursuing attacks are slowly increasing, and recently such attacks may result in widespread, severe consequences and results. Such reasons amalgamate to generate challenges for security teams to maintain the pace and create smarter required solutions. This research discusses how Big Data analytics and Artificial Intelligence (AI) tools or platforms like ChatGPT can be used to prevent cybersecurity challenges. The research also discusses the existing AI and data analytic technologies and how they can enhance cybersecurity. The incoming AI application in ChatGPT shortcomings is also discussed in this research focusing on its pros and cons in managing cyber threats. In order to respond to more preemptive and predictive reactions and monitoring, the paper places a strong emphasis on emphasizing security systems. This may further save time when performing manual, repetitive security tasks. Finally, this research looks at the challenges curbing such adoptions, thus providing future directions to overcome the challenges.**

Keywords— cyber threats, network attacks, Big Data analytics, Artificial Intelligence, cybersecurity, ChatGPT

I. Introduction

Security analytics must process huge amounts of data to reveal the anomalies and the patterns that might trigger alerts of potential attacks. Security tools, personal user devices, networking hardware, and logs on servers are sources that generate such massive amounts of data. In this context, Computer Incidents Response Teams (CSIRTs) and Security Operations Centers (SOCs) are in charge of analyzing various correlation and visualization solutions necessary for detecting very effectively and quickly [1]. The CSIRTs and SOCs search for novel technological breakthroughs, such as Data Science, Artificial Intelligence, and Big Data. Using cognitive sciences in information security procedures drives the notion of cognitive security, which constitutes the combination of security operations with data science and cognitive science. The admission and availability of massive amounts of information in the current age have resulted in proactive security approaches. Analyses that are either prescriptive or predictive may have a forecasting perception of the potential effects of an attack if the existing threats against the present state of security are maintained. International organizations like the National Institute of Standards and Technology (NIST) began the Data Science Research Program intending to hasten the progress of the investigation for the analytical data strategies. In the field of enterprise, the role played by cybersecurity data scientists has become very lucrative for employees and employers.

AI and data analytics are not brand-new fields. Nonetheless, newer technologies like the cloud, high-performance computing, machine learning, Big Data, and other information sources make it possible for data science to advance several societal areas significantly. Cybersecurity, public administration, health tourism, agriculture, and many more benefits fall under this category. Data analytics can produce the process of implementing cybersecurity operations and the essential training for the security analyst. From the viewpoint of the security analyst, an attack needs one to review necessary information within the shortest possible time - they have to analyze data in the form of a structured type like logs. They also need unstructured data like the ones coming from the manufacturer's bullets, security feeds, news, and websites [2]. The central aim of this research is to review the existing types of cybersecurity attacks and how to counter them through Al and Big Data analytics, thus giving the future direction of cybersecurity. By introducing Al methods and data analytics in computer security, detection, and intrusion systems developed to alter and detect possible attacks and deviating behavior.

II. Background of the Study

Cybersecurity has been one of the most studied areas in recent years. Kagita et al. [3] report outlined that about 45% of the globe needs to be better equipped for serious cyberattacks, yet 30% still need to adopt anti-malware software. The application of current technologies, such as the Internet of Things (IoT), cloud, bring your device (BYOD), and others, have improved the complexity and the amount of data networks that are beyond the capabilities of the security analyst to connect the associations between users and data systems. Research by Zhao et al. (2020) predicted that by the year 2020, there would be 5,200 gigabytes for every other individual in the world or 40 trillion gigabytes of data [4]. Fagbemi, Wheeler, and Wheeler (2019) identified that IoT devices involved cybercriminals to be applied in their illegal activities [5]. In 2016 the providers of European telecom home routers had a successful attack from a Mirai worm, which changed all the devices compromised into army warm bots for huge attacks by DDOs. The Cyber Division of the FBI then declared that knowledge prioritization and upcoming threats are significant since the actors quickly alter and adapt their techniques and tactics.

Big data analytics concentrates on discovering knowledge in unstructured and structured data through visualization tools, machine learning algorithms, advanced statistical functions, and data science. Big data illustrates new substitutes for preventing and detecting cyber-attacks using the correlation of external and internal security data. Using Big Data, data can be gathered through Twitter feeds and correlated with the events detected with security news published on specialized

blogs or websites. NIST Information Access Division has encouraged analytic data development for more accurate and greater understanding and access to information found in the diversified multimodal data. On the other hand, Artificial Intelligence was developed in 2015 when Google developed AlphaGo – a designed computer program for playing the GO game. AlphaGo applied the power of computation of neutral works and machine learning to beat the highest-ranked world Go players, and up-to-date technology is still among the most sophisticated algorithms of Artificial Intelligence [6]. The most recent discoveries of Artificial Intelligence include smart speakers, advertisement algorithms, and face and speech recognition. Yet, the complete potential of the Al instruments has not been explored. Moreover, evidence demonstrates that upscaling these Al tools will significantly decrease the number of breaches of risk and improve the effectiveness of cyber-security-connected functions.

III. Types of Cybersecurity and Current Situation

As illustrated herein, there are varied cybersecurity types, and they all have different fields of challenges to tackle and resolve. Here there will be a discussion of several of the relevant cybersecurity threats. With the evolution of AI and deepfake algorithms, modern-day cyber attacks are more concerning than before. Below are the 10 types of cyber attacks the world should be aware of in current years.

Table I. Types of Cyber Attacks

Attack Type	Description
Malware Attack [7]	It's the common type. It refers to viruses including worms, spyware, ransomware, adware, and trojans.
Phishing Attack [7]	These are very prominent in social engineering attacks with fake emails and ads.
Password Attack [8]	Here hacker cracks victim passwords with programs and cracking tools like Aircrack, Cain, Abel, Hashcat, etc.
Man-in-the-Middle Attack (MITM) [7]	MITM is known as an eavesdropping attack. The attacker comes in between the client and a host with wi-fi networks and steals the information.
SQL Injection Attack [8]	SQL injection attack occurs on a database-driven website when the hacker manipulates and steals the data using a standard SQL query.
Denial-of-Service Attack [9]	Attackers target systems, computers, or networks in this case, and bombard them with data to deplete their bandwidth and resources (DDoS attack).
Insider Threat [8]	As the name suggests, it might be someone who works there and is intimately familiar with the business. The possible harm from insider threats is enormous.
Cryptojacking [9]	This new type of assault occurs when hackers gain access to another person's device to mine cryptocurrencies.
Zero-Day Exploit [9]	A Zero-Day Exploit happens after a network flaw is discovered; in most cases, there is no fix for the problem. The vendor informs customers of the vulnerability as a consequence, but the information also gets the attackers.
Watering Hole Attack [9]	Theft of private information from the government is very common these days. The perpetrator chooses websites that the targeted group commonly visits in such an attack. Websites are discovered either by closely watching the group or by estimating.

The last cybersecurity aspect that requires to be addressed is endpoint security. In the short definition, the concept of end security can be said to be a practice that involves putting security at the point of entry on the network under attack or exploitation. The meaning of entry points and ends means smartwatches, desktops, printers, mobile phones, mobile phones, and other smart devices accessible through a network. Endpoint security is not a novel aspect, yet has always been overlooked. Currently, the average amount of existing antivirus software may not be enough to tackle the attacks faced on a day-to-day basis. Data is a key vital asset in many companies and businesses, meaning that there is a need to have tools that can be used to protect it [10]. Since numerous thousands of entry points can be found in a 15 network, endpoint protection platforms (EPP) and automatic detection systems are the predictions of the future when keeping up with the pace and new trends.

With the increase in technological solutions in every other life aspect, there is a corresponding increase in cyber criminality, cyberattacks, and companies, machines, and services growth. In 2016, 15 billion data structures were exploited; compared to 2010, the number of exploited records massively rose to 103 million, which shows a big figure [11]. In the future, introducing a 5G technological infrastructure will lead to the creation of IoT networks that are more complex and massively increase the number of potential devices that may be attacked. Moreover, the 5G technology's bandwidth will enable more data transmission at a time. The outbreak of the new coronavirus disease is a good example of how cybercriminals profit from unfavorable circumstances. According to Wang et al., 2017, statistics on online and email scams have increased by approximately 400% [12]. The tactics of scare function and people's emotions are not easy to dispute the equation.

Recently, there have been numerous problems with cybersecurity, one of the issues being the connections or distance in terms of geography, which exposes the weak points found within a chain, at least in a single space. As discussed prior, several security systems are still using manual detection labor, making it difficult to find enough time to handle all the attempts of attacks. Moreover, instead of applying proactive recovery methods, computers still use reactive ones [13]. The reactive method is never enough in the end; thus, it does not essentially prevent a similar problem from occurring on multiple occasions. Due to the availability of data and research on cybersecurity and the transparency of its methods, criminals use such information to understand the applications and make exploiting them simple [14]. Also, on some occasions, hackers apply proxy servers and Virtual Private Networks (VPN) in charging IP addresses, thus keeping them safe from being caught.

IV. How AI and Bigdata Improve Cybersecurity

As can be noticed, one realizes a transparent incentive to install the solutions brought about by AI and Big Data analytics in the recent future in the fight against cyber criminality [15] (see Fig 1). In this segment, there is an in-depth discussion about the actual contributions of artificial intelligence methods and Big Data analytics to cyber security and their worthiness. The figure below shows how the

process of big data and analytics is trying to solve cyber security issues systematically in steps.

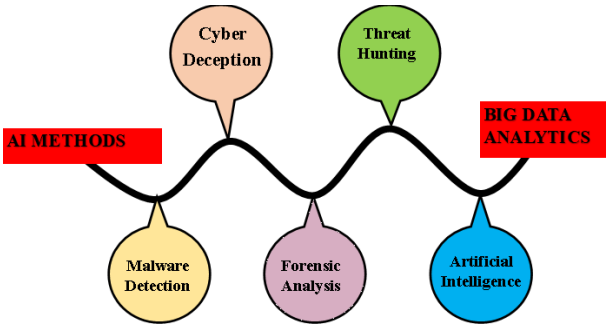

Fig. 1. Role of AI and Big Data in Cybersecurity

A. *Artificial Intelligence*

The analytic power of analytics and computation of the Al infrastructure is quicker than humans' brainpower. In comparison to the recent methods, Al can attain a much better detection speed. Apart from its ability to detect threats faster, it can also recognize unknown attacks quickly, and a better solution can be executed without a previous implementation [16]. The errors that humans bring about are still huge contributors to cybersecurity challenges. By adopting AI technology, the number of cybersecurity cases humans cause can be greatly reduced - this applies to daily repetitive functions. However, AI can also be exploited in decision-making [17]. During decision-making, a test can be conducted on the software and the data using algorithms; thus, hidden security threats and unnoticed errors may be detected early enough. When it is true that AI's computing power is bigger than human beings, innovation, and creative thinking are still aspects that humans can only do [18]. Thus, AI infrastructures should be adopted in repetitive and scheduled jobs - this creates additional time for the security personnel to enhance the procedure and concentrate on creative thinking. The other cybersecurity area where AI can accrue benefits is threat hunting. In traditional operations, the idea of threat hunting meant that the security software would be designed to look for threats and indicators. The difficulty with this strategy is that it requires prior knowledge of the threats to developing enough signatures for them. Such that the approach needs to be revised when faced with a completely novel danger. Although, these signature-based methods are very effective and can detect as huge as 90% of threats [19]. A total 100% replacement of signature-based methods by AI cannot be the best solution, as the results would generate more than eighteen false positives. Yet, an amalgamation of the two approaches is profitable.

B. *Forensic Analysis*

Forensics implies the interpretation, analysis, and presentation of computer information. Nieto, Rios, & Lopez (2018) defined forensics as a solution for security information management that had been regarded as the principal point of information security collected through various network devices [20]. Literature has it that it has the flexibility of administering multiple security counter procedures to enhance the entire picture of security. It has a rule-based correlation tactic that correlates and analyzes security information on various devices [27, 30]. It offers a way of the report and alert customization to improve security information management flow in an organization. Net forensics assists in establishing a simple policy compliance audit by using one framework for various reporting and alarming services.

C. *Malware Detection*

Names like malcode, malicious code and malicious software have referred to malware. Malware has also had various definitions. Ogundokun et al. (2021) pointed out that a malware incident is a computer program with a nasty objective [21]. Denney et al. (2019) stated that malware is removed, changed, or added software systems geared to subvert the normal function or intentionally damage the system [22]. In this context, it is proper to use the definition of malware given by Asamoah (2020), who described it as a term that encompasses ransomware, adware, spyware, Trojans, viruses, and any other intrusive codes [23]. The approaches applied in detecting malware have two categories: anomaly-based and signature-based (see Fig.2).

Signature-based detection relies on signatures predefined in nature in decision-making concerning the maliciousness of a program under suspicion. Although, anomaly-based detection makes its own decision concerning the maliciousness of a program under suspicion regarding its past knowledge of what constitutes normal behavior. Anomaly-based detection has a branch referred to as ruled-based or specification-based detection. This branch constructs some set of regulations and specifications to represent normal legal behavior and applies such rules in making decisions concerning the maliciousness of a program under suspicion.

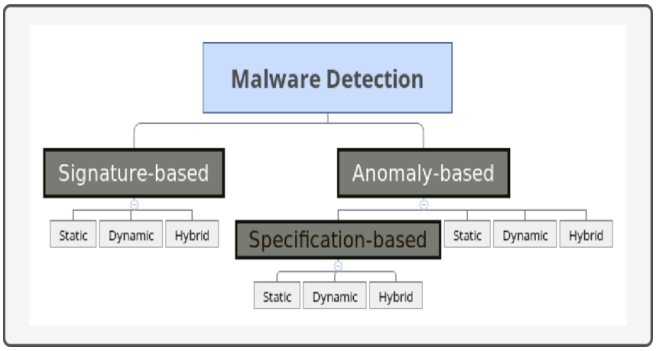

Fig. 2. Types of Malware Detection Techniques

D. *Cyber Deception*

The central aim of conducting a cyber deception is to enable the detection of attacks to create an adaptive cyber defense method that is objected towards bringing confusion to the attacker. The types of cyber deception used traditionally used honeynets and honeypots, although the developing motivations in this study include Big Data, theory games, and Artificial Intelligence to improve cybersecurity strategies against attackers [24].

E. *Threat Hunting*

Threat hunting involves an iterative work of active defense research across different networks and security data to detect advanced dangers without waiting for alerts upon attacks. Research by Rasheed, Hadi, & Khader [24] focused on threat-hunting procedure deployment by applying GRR Rapid

Response and through two distinct tests that include the test for the client-side exploits and that of remote code execution [25]. Ko (2020) examined the disparities between threat hunting against other activities that promote cybersecurity, such as Cyber Intelligence, IDS, Forensics, Penetration Testing, and Cyber Defense [26].

V. Cybersecurity threats from ChatGTP

Even though AI and big data analytics greatly suppress cybersecurity, there is evidence that the opposite can be true. Recently, the launch of ChatGPT (Chat-Based Generalized Turing Protocol) has posed high cybersecurity threats. ChatGTP is a chatbot platform that combines massive natural language processing (NLP) algorithms and artificial intelligence (AI) to create a conversational interface. It is designed to enable users to type in natural language and receive a response in natural language that they can understand. ChatGTP analyzes the user's input and generates a response based on the context. The platform uses rules-based algorithms and machine learning to interpret the user's input. The platform then processes the input and creates a response based on the rules [17, 32]. The response is then sent back to the user in a form they can understand. One of the main benefits of ChatGTP is that it can process natural language input and generate responses tailored to the user's specific needs and context - this makes it easier for users to interact with the chatbot and reduces the chances of them receiving an inappropriate response. Additionally, the platform can be used to create more personalized experiences for the users, such as providing contextual recommendations or personalized assistance (see Fig. 3).

Fig 3. Example of how a malicious code was created by an info stealer using ChatGPT. Source [17]

Despite these anticipated benefits of ChatGPT, it has been identified that the platform is attracting cybercriminals. The platform might even continue creating a passway through which cybercriminals can easily mount cyber-attacks [29, 33]. According to Check Point Researchers (CPR), several instances have been identified where cybercriminals have identified that ChatGPT from OpenAI has helped them in their malicious activities. One incident through which the cybercriminals are using ChatGPT is creating Infostealer, as identified by a popular hacking forum experimenting with using ChatGPT to create Python-based malware [16, 31, 32]. Criminals can also create an Encryption Tool using ChatGTP. Evidence presented by USDoD, as tagged by the CPR, confirmed that he had created his first Python script from OpenAI. The script was capable of performing decryption and encryption functions [19, 24].

Apart from the two mentioned malware-oriented practices, there comes a sense of ChatGPT facilitating fraud activities. An analysis by CPR shows the potential for growth of the Dark Web Marketplace since selling malware is one of the activities in the Dark Web. Evidence of this emanates from a code from cyber criminals, with the API as the third party. This code was made for getting instant and current cryptocurrency, especially Bitcoin, Monera, and Etherium [32, 33]. Whereas ChatGPT is in its initial stages of growth, there is a high potential that, if not well-guarded, this platform might lead elevation of cybersecurity threats. Conclusively, AI can impact cybersecurity negatively.

VI. Future Directions

Basing this discussion on the challenges and requirements faced by cybersecurity and the issues that arise from the adoption of AI and Big Data analytics, there is a need to identify some significant directions needed to understand the future of cybersecurity (see Fig. 4).

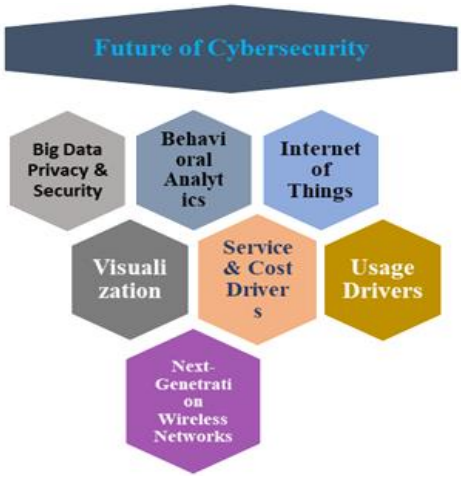

Fig. 4. Future of cybersecurity

A. *Big Data Privacy and Security*

As illustrated in the challenges that face Big Data analytics, offering protection for Big Data is a massive challenge that should be addressed. Multiple authentication schemes are required for data trustworthiness gathered from different sources to ascertain data provenance [27]. Also, Big Data should have adequate enhancements to the existing anomaly detection techniques successfully deployed in traditional security systems to protect data correctness in a real-time and automated form and detect any harmful events inside. [31]. Concerning privacy, further schemes that allow privacy preservation should be developed for Big Data analytics as far as the context of cybersecurity is concerned. Further guidelines and rules should be monitored and introduced by government agencies to keep data pieces that are connected to individual identities and their private issues hidden.

B. Behavioral Analytics

The other area that may improve as far as cybersecurity is concerned is behavioral analytics, which implies context information consideration to enhance the potentiality of abnormal behaviors and detect patterns that demonstrate thefts, frauds, and any other cybersecurity threats. The cyber solutions that were used traditionally achieved success with external intrusions, and they did not detect internal incidents [33]. Through behavior monitoring of legitimate and normal users, Big Data analytics solutions can be applied in forecasting unanticipated behaviors and detecting internal dangers through anomaly detection [28]. For instance, in association behavior, the number of times a file gets downloaded or the number of times a database is accessed. Although, other types of internal hazards will be unable to be detected except through modeling abnormal and normal behaviors of users.

C. Visualization

The advancement of visualization tools is an area that is anticipated to be addressed shortly to ensure the provision of security analytics by using insights that can help them save time in the context of detecting cybersecurity hazards. Some visualization dashboards that connect to security are already in the application, for instance, Keylines. Although, there is a requirement for improved development, especially due to the increased number of data sources that complicate data visualization and the mandate of data streaming and real-time processing [29].

D. Internet of Things (IoT)

The applications of IoT are Big Data applications, examples like habitat monitoring, ITS, smart cities, and many more, which imply the real-time processing and the production of streaming data. All the applications have different demands and requirements in privacy and security; thus, appropriate design improvement and augmentation are needed to achieve such requirements. There is, therefore, the necessity of embracing Big Data analytics in issues involving the security of IoT applications [30].

E. Next-Generation Wireless Networks

In the future self-driven network, a single infrastructure will require flexibly and effectively offering heterogeneous services, such as improved machine-type communications, low-latency and ultra-reliable communications, and mobile broadband. Such a network also will have an obligation to support existing accesses, like the 5G (fifth generation), WIFI, and LTE (long-term evolution). Additionally, they will be required to coordinate a diverse network with several base stations (BSs), for instance, heterogeneous operator devices, pico BSs, Femto, micro, and macro applications. The problem of effectively operating a network that can enable such flexibility and satisfy the requirements of diversified services is challenging for a mobile network operator [31]. Additionally, mobile network operators undergo massive problems keeping track of the ever-developing capacity demands and increasing their coverages with scarce resources and a limited pool of assets such as spectrum. Configuration of manuals for optimization, control, and network planning will make issues even more difficult. Also, human-machine relations can, at particular times, be expensive, susceptible to error, and time-consuming. Conversely, the cellular network's purposes and the automation of varied entities are currently the central issues for MNO in deliberating the reduction of expenses involved in the operation. From the perception of the operational expenses, the system should be self-adaptive, self-aware, and smart. It can run the services sparingly, administer, and be involved in the operation of the networks autonomously. Conservative reactive maintenance is not effective anymore. By applying big data analytics, the factors' proactive and predictive network maintenance can be achieved [32]. Considering the type of data sources, range, and speed of the flowing data, the network can go beyond anticipation; for instance, it can prescribe and/or assist the unit of maintenance and operation with options regarding decisions and the effects of the actions [33]. Artificial intelligence and machine learning are significant in revealing the hidden properties of wireless networks, detecting irregularities and associations that are not visible through manual inspection, and proposing new techniques necessary for network operations and deployments.

F. Service and Cost Drivers

Generally, subscribers have lots of demand, yet the majority still need to have the will to raise the wireless payout. Such a setting demands fast optimization of the network resources application. Moreover, there is a transformation from the network-centric to the user-centric model of the QoE. Due to that, the mobile network operators need to acquire knowledge about the QoE broadly and it is related to networks of KPIs. Moreover, mobile network operators aim to retain their clients [33]. Therefore, mobile network operators need to enhance the performance of the network and QoE without interfering with the cost, enhance efficiency to retain the profit margin, manage its traffic based on application and service, and maintain churn at the lowest possible standards.

G. Usage Drivers

The analytics in a user-oriented service model regulate and maintain wireless devices, traffic types, and subscribers varyingly based on each's needs and mobile network operator's strategies. The subscribers' profiles, subscriber equipment, and traffic patterns are all diversified in nature. Moreover, the traffic load of wireless applications is under faster development than the capacity; also, mobile network operators are undergoing difficult problems in cost-effectively enhancing network capacity. Thus, increasing resource utilization is significant [30]. Analytics is responsible for understanding the challenges faced due to the network load necessary for the MNOs to manage network traffic in real-time effectively.

VII. Recommendations and Conclusion

The concept of encountering future cyberattacks through applying Big Data analytics and ChatGPT is a double-edged sword. As the malicious actors and the attackers continuously develop their attacking strategies, urgency is needed in setting up reactions. Moreover, there is much misconception regarding the cybersecurity challenges that can be handled by Big Data analytics and ChatGPT. AI and Big Data analytics have been promoted as the responses to several cybersecurity challenges, yet, the industry still needs to catch up. Multiple existing technologies such as Cyber Intelligence, Intrusion

Detection Systems (IDS), Forensics, Security Orchestration, Automation and Response (SOAR), Network Detection and Response (NDR), Penetration Testing, Cyber Defense, and many others still require the intervention of human beings.

Although adopting Big Data analytic techniques and AI tools is a partial solution to the traditional reactive, more than the prevention tricks based on rules will be needed to handle massive attacks. Recently, ChatGPT is attracting more attention from hackers globally than any other algorithms because of its human-like engagement. As ChatGPT usage grows, it is important to be aware of its possible benefits and drawbacks. While ChatGPT can handle business support tasks or more quickly and correctly deliver information to clients, it also raises concerns as a potential hacking tool. To safeguard themselves from ChatGPT-related cybercrime, individuals and organizations must exercise caution and take the necessary precautions. Users need to be trained to recognize and prevent such attacks, appropriate security controls and protocols need to be implemented, and countermeasure technology needs to be regularly updated. To safeguard ourselves, we'll need to wait and watch how the states and business community respond to the use of ChatGPT in the future.

ACKNOWLEDGMENT

The authors would like to thank Dr. Azad Ali of the University of the Cumberlands, KY for his invaluable assistance and feedback on this project.

REFERENCES

[1] Andrade, Roberto O., and Sang Guun Yoo. "Cognitive security: A comprehensive study of cognitive science in cybersecurity." Journal of Information Security and Applications 48 (2019): 102352.

[2] Kagita, Mohan Krishna, Navod Thilakarathne, Thippa Reddy Gadekallu, Praveen Kumar Reddy Maddikunta, and Saurabh Singh. "A review on cyber crimes on the internet of things." Deep Learning for Security and Privacy Preservation in IoT (2022): 83-98.

[3] Fagbemi, Damilare D., David M. Wheeler, and J. C. Wheeler. The IoT architect's guide to attainable security and privacy. CRC Press, 2019.

[4] Holcomb, Sean D., William K. Porter, Shaun V. Ault, Guifen Mao, and Jin Wang. "Overview on deepmind and its alphago zero ai." In Proceedings of the 2018 international conference on big data and education, pp. 67-71. 2018.

[5] Ricci, Joseph, Frank Breitinger, and Ibrahim Baggili. "Survey results on adults and cybersecurity education." Education and Information Technologies 24 (2019): 231-249.

[6] Sharma, Pratima, Rajni Jindal, and Malaya Dutta Borah. "Blockchain technology for cloud storage: A systematic literature review." ACM Computing Surveys (CSUR) 53, no. 4 (2020): 1-32.

[7] Tabrizchi, H., & Rafsanjani, M. K. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. The journal of supercomputing, 76(12), 9493-9532.

[8] Annarelli, Alessandro, Fabio Nonino, and Giulia Palombi. "Understanding the management of cyber resilient systems." Computers & industrial engineering 149 (2020): 106829.

[9] Wang, Jingguo, Yuan Li, and H. Raghav Rao. "Coping responses in phishing detection: an investigation of antecedents and consequences." Information Systems Research 28, no. 2 (2017): 378-396.

[10] Sun, Nan, Jun Zhang, Paul Rimba, Shang Gao, Leo Yu Zhang, and Yang Xiang. "Data-driven cybersecurity incident prediction: A survey." IEEE communications surveys & tutorials 21, no. 2 (2018): 1744-1772.

[11] Kiru, Muhammad Ubale, and Sulaiman Isyaku Muhammad. "A situation analysis on cybercrime and its economic impact in Nigeria." International Journal of Computer Applications 975 (2017): 8887.

[12] Carroll, Fiona, Ana Calderon, and Mohamed Mostafa. "Ethics and the Internet of Everything: A Glimpse into People's Perceptions of IoT Privacy and Security." In Privacy, Security And Forensics in The Internet of Things (IoT), pp. 3-29. Cham: Springer International Publishing, 2012.

[13] Muheidat, Fadi, and Lo'ai Tawalbeh. "Artificial intelligence and blockchain for cybersecurity applications." In Artificial Intelligence and Blockchain for Future Cybersecurity Applications, pp. 3-29. Cham: Springer International Publishing, 2021.

[14] Mariani, Marcello M., and Satish Nambisan. "Innovation analytics and digital innovation experimentation: the rise of research-driven online review platforms." Technological Forecasting and Social Change 172 (2021): 121009.

[15] Dash, Bibhu, and Pawankumar Sharma. "Role of Artificial Intelligence in Smart Cities for Information Gathering and Dissemination (A Review)." Academic Journal of Research and Scientific Publishing 4, no. 39 (2022).

[16] Dash, Bibhu, and Pawankumar Sharma. "Are ChatGPT and Deepfake Algorithms Endangering the Cybersecurity Industry? A Review." International Journal of Engineering and Applied Sciences, 2023, 10(1).

[17] Zappone, Alessio, Marco Di Renzo, and Mérouane Debbah. "Wireless networks design in the era of deep learning: Model-based, AI-based, or both?." IEEE Transactions on Communications 67, no. 10 (2019): 7331-7376.

[18] Alshamrani, Adel, Sowmya Myneni, Ankur Chowdhary, and Dijiang Huang. "A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities." IEEE Communications Surveys & Tutorials 21, no. 2 (2019): 1851-1877.

[19] Nieto, Ana, Ruben Rios, and Javier Lopez. "IoT-forensics meets privacy: towards cooperative digital investigations." Sensors 18, no. 2 (2018): 492.

[20] Ogundokun, Roseline Oluwaseun, Joseph Bamidele Awotunde, Sanjay Misra, Oluwakemi Christiana Abikoye, and Oluwafemi Folarin. "Application of machine learning for ransomware detection in IoT devices." In Artificial intelligence for cyber security: methods, issues and possible horizons or opportunities, pp. 393-420. Cham: Springer International Publishing, 2021.

[21] Denney, Kyle, Enes Erdin, Leonardo Babun, Michael Vai, and Selcuk Uluagac. "Usb-watch: a dynamic hardware-assisted usb threat detection framework." In Security and Privacy in Communication Networks: 15th EAI International Conference, SecureComm 2019, Orlando, FL, USA, October 23-25, 2019, Proceedings, Part I 15, pp. 126-146. Springer International Publishing, 2019.

[22] Asamoah, Harrison. "Antivirus software versus malware." Архів кваліфікаційних робіт (2020).

[23] Zhu, Mu, Ahmed H. Anwar, Zelin Wan, Jin-Hee Cho, Charles A. Kamhoua, and Munindar P. Singh. "A survey of defensive deception: Approaches using game theory and machine learning." IEEE Communications Surveys & Tutorials 23, no. 4 (2021): 2460-2493.

[24] Rasheed, Hussein, Ali Hadi, and Mariam Khader. "Threat hunting using grr rapid response." In 2017 International Conference on New Trends in Computing Sciences (ICTCS), pp. 155-160. IEEE, 2017.

[25] Ko, Ryan KL. "Cyber autonomy: Automating the hacker-self-healing, self-adaptive, automatic cyber defense systems and their impact to the industry, society and national security." arXiv preprint arXiv:2012.04405 (2020).

[26] Sharma, Pawankumar, and Bibhu Dash. "Smart SCM Using AI and Microsoft 365." International Journal of Advanced Research in Computer and Communication Engineering 12, no. 1 (2023).

[27] Rassam, Murad A., Mohd Maarof, and Anazida Zainal. "Big Data Analytics Adoption for Cybersecurity: A Review of Current Solutions, Requirements, Challenges and Trends." Journal of Information Assurance & Security 12, no. 4 (2017).

[28] Roy, Mousumi, and Abhijit Roy. "Nexus of internet of things (IoT) and big data: roadmap for smart management systems (SMgS)." IEEE Engineering Management Review 47, no. 2 (2019): 53-65.

[29] Trestian, Ramona, Ioan-Sorin Comsa, and Mehmet Fatih Tuysuz. "Seamless multimedia delivery within a heterogeneous wireless networks environment: Are we there yet?." IEEE Communications Surveys & Tutorials 20, no. 2 (2018): 945-977.

[30] Al-Turjman, Fadi, Enver Ever, and Hadi Zahmatkesh. "Small cells in the forthcoming 5G/IoT: Traffic modelling and deployment overview." IEEE Communications Surveys & Tutorials 21, no. 1 (2018): 28-65.

[31] A. Azaria, "CHATGPT usage and limitations," 2022.

[32] J. Robinson, "The cost of science a look at the ethical implications of chatgpt," 2023.

[33] Dash, Bibhu, Pawankumar Sharma, and Azad Ali. "Federated Learning for Privacy-Preserving: A Review of PII Data Analysis in Fintech." International Journal of Software Engineering & Applications (IJSEA) 13, no. 4 (2022).