International Journal of Research Publication and Reviews

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

Enhancing Cyber Threat Detection Through Big Data Analytics and ChatGPT

Khushi Chahar[1], *Dr. Febin Prakash*[2]

[(1)]22MCAR0184 Department of CS & IT JAIN (Deemed-To-Be-University) Bangalore, India ,jpc222645@jainuniversity.ac.in
[(2)]ProfessorDepartment of CS & ITJAIN (Deemed-To-Be-University) Bangalore, India, febin.prakash@jainuniversity.ac.in

DOI : https://doi.org/10.55248/gengpi.5.0324.07100

ABSTRACT :

Cyber threats and network attacks are getting more sophisticated every day. Every day, there is an increase in the number of attacks occurring worldwide and a diversification of the strategies used to compromise personal devices and organizational systems. These attackers could be a single hacker or members of an organized organization or even the entire government. Attack options are steadily growing, and as of late, these attacks could have far-reaching, detrimental effects. These factors come together to present difficulties for security teams in keeping up the pace and developing more intelligently needed solutions. This study explores how cybersecurity issues can be avoided by utilizing artificial intelligence (AI) tools and platforms like ChatGPT and big data analytics. The study also addresses current artificial intelligence and data analytics technologies, as well as how they can strengthen the cybersecurity. This study also addresses the flaws of ChatGPT's forthcoming AI application, highlighting both its advantages and disadvantages in terms of managing cyber dangers. The study emphasizes security systems as a means of responding to more predictive and pre-emptive responses and monitoring. In addition, this could save time on repeated, manual security duties. Lastly, this study examines the obstacles preventing these adoptions and offers suggestions for how to get around them in the future.

Big Data Analytics is essential to cybersecurity by processing or analyse massive datasets to detect threats, irregularities, and patterns in real-time. The integration of BDA enables organizations to proactively identify and mitigate cyber risks, offering a dynamic and adaptive approach to safeguarding sensitive information. The paper delves into various applications of BDA in cybersecurity, including predictive analysis, behaviour analytics, and threat intelligence, illustrating how these contribute to the overall resilience of systems and networks.

In conclusion, cyber threat detection through Big Data Analytics and ChatGPT is transformative, providing organizations with advanced tools to fortify their defence mechanisms. As the cyber landscape continues to evolve, leveraging these technologies becomes imperative for staying ahead of sophisticated threats and ensuring the resilience of digital ecosystems. This research contributes to the ongoing discourse on the intersection of artificial intelligence and cybersecurity, offering insights into the promising future of proactive and intelligent cyber defence strategies.

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

Introduction :

Massive volumes of data must be processed by security analytics in order to identify the patterns and abnormalities that could set off alarms about possible attacks. Sources that provide such enormous volumes of data include networking technology, security technologies, personal user devices, and server logs. In this situation, evaluating various correlation and visualization tools required for swiftly and efficiently detecting is the responsibility of Security Operations Centers (SOCs) and Computer Security Incident Response Teams (CSIRTs) [1]. The CSIRTs and SOCs look for cutting-edge innovations in fields like big data, artificial intelligence, and data science. The concept of "cognitive security," which combines data science and cognitive science with security operations, is based on the application of cognitive sciences to information security processes. Modern times have seen the admission and availability of enormous volumes of data, which has led to proactive security measures. Prescriptive or predictive analyses may be able to foresee the possible consequences of an attack if the current security posture is preserved and the threats against it continue.

The Data Science Research Program was started by international organizations such as the National Institute of Standards and Technology (NIST) with the aim expediting the examination of analytical data methods. Within the realm of business, the function that Employment of cybersecurity data scientists is now quite profitable for both companies and workers.

Data analytics and artificial intelligence are not new disciplines. However, data science can greatly progress various socioeconomic areas thanks to emerging technology such as big data, cloud computing, machine learning, high-performance computing and other sources of information. This area includes benefits related to agriculture, public administration, cybersecurity, and health tourism, among many others. Data analytics can be used to create the necessary training for security analysts as well as the process of implementing cybersecurity operations. From the security analyst's point of view, an attack necessitates that they evaluate relevant data as soon as possible; this includes looking at structured data, like logs. Additionally, they need unstructured data from sources like news, security feeds, websites, and manufacturer bulletins [2]. The main objective of this research is to analyze the many cybersecurity risks that are now in existence and how to defend against them using Al and Big Data analytics in order to ascertain the future direction of cybersecurity. Intrusion detection and prevention solutions in computer security are designed to change and identify potential threats and deviant behaviour, Al techniques and data analytics were introduced.

Scale, velocity, and variance are the three main areas where traditional and big data differ from one another. Variance indicates the various forms of structured and unstructured data, while volume indicates the amount of data generated and the velocity rate which the data is generated. These days, big data is becoming a popular research topic in nearly every sector, especially cyber security. [3] The main sources of this information are smart devices and social networking sites. Data are being generated at this point. This enormous number of malware infections in a single industry highlights the annual threat to the world economy. Consequently, it is evident that the cyber-security of web apps, corporate networks, and IT systems may not be adequate to handle the swift advancement of cyberattacks.

Background Of the Study :

Cybersecurity has emerged as a highly researched domain. Approximately 45% of the world's population still needs to install anti-malware software, according to a Kagita et al. [3] analysis, but the rest must improve prepare for significant cyberattacks. Modern technologies, like cloud computing, Bring Your Own Device (BYOD), and the Internet of Things (IoT), have made data networks more complex, vast than security analysts can handle when it comes to connecting user-data system associations. By 2020, 5200 gigabytes for each person on the earth, or 40 trillion gigabytes of data, will exist., according to research by Zhao et al. [4]. Fagbemi, Wheeler, and Wheeler (2019), cybercriminals use Internet of Things (IoT) devices in their illicit activities [5]. A successful Mirai worm attack on European telecom home router providers in 2016 turned every infected device into an army of warm-bodied bots ready for massive DDO attacks. The FBI's Cyber Division then stated that, understanding priorities and potential dangers is crucial since players frequently modify and alter their strategies and methods. Modern technology is still among the most advanced Artificial Intelligence Algorithms, and Machine Learning to defeat the world's best Programmer [6]. Big data analytics is the process of mining both structured and unstructured data for insights using machine learning, data science, complex statistical functions, and visualization tools. Big data offers fresh options for spotting and preventing cyberattacks by comparing internal and external security data. Information can be gathered by Twitter feeds and events can be connected to security news from specialized blogs and websites thanks to big data. The NIST Information Access Division has promoted the generation of analytical data in order to improve comprehension and facilitate access to information contained in the diverse multimodal data. However, artificial intelligence gained a boost in 2015 when Google created AlphaGo, a computer program meant to play the game of Go. AlphaGo employed computation of neutral labor authority. The most recent advancements in artificial intelligence include speech and face recognition, smart speakers, and algorithms for advertisements. However, the Al instruments have not yet reached their full potential. Furthermore, data indicates that scaling up these Al tools will greatly reduce the amount of risk breaches and increase the efficacy of functions related to cyber security.

Attack Type	Description
Malware Attack[7]	It's the typical kind. When we talk about viruses, we're talking about trojans, worms, spyware, ransomware, and adware.
Phishing Attack [7]	These are very prominent in social engineeringattacks with fake emails and ads.
Password Attack[8]	Here, the hacker uses programs and tools like Aircrack, Cain, Abel, hashcat, etc. to crack the victim's password.
Man-in-the- Middle Attack (MITM) [7]	The term "eavesdropping attack" refers to MITM. By placing themselves between the client and a host connected to a wi-fi network, the attacker gains access to the data.
SQL InjectionAttack [8]	An SQL injection attack happens when a hacker uses a common SQL query to modify and steal data from a database-driven website.
Denial-of-Service Attack [9]	As part of a denial-of-service (DDoS) assault, hackers target computers, networks, or systems and flood them with data.

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.
The act of cryptojacking [9]	This new kind of attack happens when hackers take control of someone else's device and mine cryptocurrency on it.
Zero-Day Exploit[9]	When a network vulnerability is found, a Zero-Day Exploit occurs; often, the issue cannot be fixed. Customers are consequently made aware of the vulnerability by the vendor, but the information also reaches the attackers.
Water HoleAttack [9]	Private information obtained from the government is frequently stolen these days. In such an assault, the attacker selects websites that the targeted group frequently accesses. Websites are found by estimating or by attentively observing the group.

TABLE I. TYPES OF CYBER ATTACKS :

Types Of Cybersecurity and Current Situation :

There are many distinct kinds of cybersecurity, as this article has shown, and each one has unique problems that need to be addressed. Several of the pertinent cybersecurity threats will be discussed in this section. The development of artificial intelligence and deepfake algorithms makes cyberattacks in the present era more worrying than ever. The top ten cyberattack categories of the present that people need to be informed of are listed below.

Endpoint security is the final area of cybersecurity that needs to be taken care of. By definition, end security is the process of implementing security at the network's point of entry where an attack is likely to occur. Entry points and ends are defined as smartwatches, computers, printers, mobile phones, and other smart devices that are reachable over a network. Endpoint security is not a new concept, but it has never received enough attention. The average quantity of antivirus software available nowadays might not be sufficient to combat the daily threats. Many corporations and businesses consider data to be a critical asset, thus having tools to safeguard it is essential [10]. In order to stay up with the pace and emerging trends, endpoint protection platforms (EPP) and automatic detection systems are the way of the future, given that a network with fifteen nodes can have thousands of entry points.

Cybercrime, cyberattacks, and the expansion of businesses, machines, and services all rise in tandem with the advancement of technology solutions in every other sphere of life. Fifteen billion data structures were exploited in 2016; this is a significant increase [11] over the number of exploited records in 2010, which was only 103 million. The deployment of a 5G technology infrastructure in the future will result in increasingly sophisticated IoT networks, which will greatly raise the possible number of devices that might be targeted for attack. Additionally, the bandwidth of 5G technology will allow for the transfer of more data at once. An excellent illustration of how hackers take advantage of negative situations is the recent coronavirus illness outbreak. Wang-et-al (2017) provided statistics on online and the number of Email frauds has risen over 400percent [12]. It is difficult to argue against the relationship between the fright function and people's emotions.

There have been a lot of cybersecurity challenges recently, and one of the problems is the geographic distance or links, which might reveal weak areas in a chain, if only temporarily. It is challenging to find adequate time to address all of the attack attempts because, as was previously said, many security systems still rely on manual detection work. Additionally, computers continue to adopt reactive recovery techniques rather than proactive ones [13]. Reactive methods seldom suffice in the long run, so they don't really stop the same issue from coming up repeatedly. Because cybersecurity research and data are readily available, and because the methodologies used are transparent, criminals can utilize this information to comprehend the applications and build exploits them being straightforward [14]. Additionally, in order to avoid detection, hackers may use Virtual Private Networks (VPN) and proxy services to charge IP addresses.

How AI and BIGDATA Improve Cybersecurity :

Evidently, there is a clear motivation to implement the solutions that Artificial Intelligence and Big Data analytics have brought about in the recent past to combat cybercrime [15] (see Fig 1). The real benefits of Artificial Intelligence techniques and Big Data analytics to cyber-security are thoroughly discussed in this segment, as is their merit. The diagram below illustrates addressing cyber-security issues systematically and step-by-step is the aim of the big data and analytics procedures.

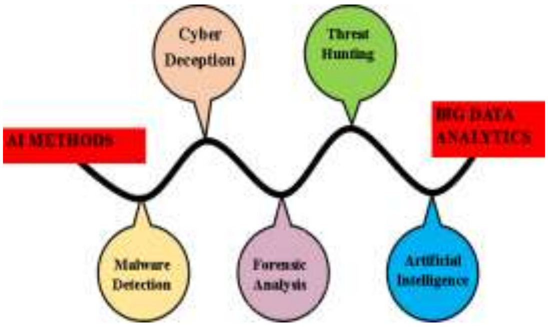

Fig. 1. Role of AI and Big Data in Cybersecurity

Artificial Intelligence-

Al infrastructure's calculation and analytical capacity are faster than human intelligence. Al is able to achieve a significantly faster detection speed than the latest techniques. In addition to being quicker at identifying risks, it is also capable of swiftly identifying undiscovered attacks, and it can carry out a superior response without requiring prior implementation [16]. The human fallibility of cybersecurity problems continues to be a major factor. Adopting AI technology can significantly minimize the amount of cybersecurity issues that humans cause, especially for routine tasks that are done every day. AI, though, can also be used to make decisions [17]. Unnoticed faults and hidden security concerns may be identified early enough in the decision-making process by employing algorithms to examine the program and data. Even in cases where AI's processing capacity surpasses that of humans, human creativity and innovation remain limited to humans [18]. Because AI infrastructures free up time for security people to improve protocol and focus on creative thinking, they should be implemented in repetitive and planned duties. The fact remains that these signature-based techniques are highly efficient, detecting up to 90% of threats [19]. AI cannot be the best option if signature-based techniques are completely replaced, as this would result in more than eighteen false positives. However, combining the two strategies yields better results.

Forensic Analysis-

The comprehension, evaluation, and demonstration of computer data are implied by the term "forensics." Forensics was once thought to be the primary source of information security gathered from a variety of network devices. Nieto, Rios, and Lopez (2018) presented forensics as a security information management solution [20]. According to literature, it is flexible enough to implement various security countermeasures to strengthen security overall. Security information on different devices is correlated and analyzed using a rule-based correlation technique [27, 30]. It presents a method of the customization of reports and alerts to enhance an organization's security information management process. By utilize

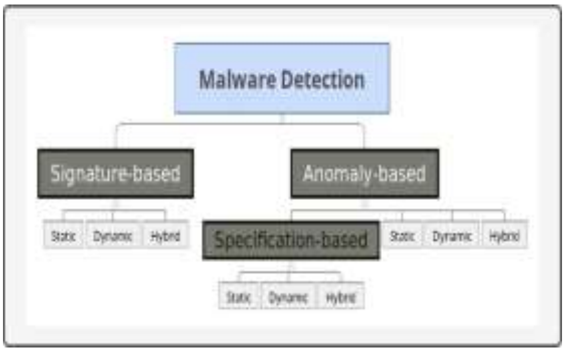

Fig. 2. Types of Malware Detection Techniques

ing a single framework for a variety of reporting and alerting services, net forensics helps to construct a basic policy compliance audit.

Malware Detection

Malware is often referred to by terms like malicious software, harmful code, and malcode. There are also other ways to define malware. According to Ogundokun-et-al (2021), a malware incidence is a computer program with a malevolent intent [21]. Malware, according to Denney et al. (2019), is software which has been added, altered, or uninstalled with the goal of intentionally damaging a system or subverting its regular operation [22]. In this particular situation, it is appropriate to employ Asamoah's (2020) definition of malware, which includes ransomware, adware, spyware, viruses, trojans, and other invasive codes [23]. Malware detection techniques fall into two categories: anomaly-based and signature-based (Fig. 2).

When determining the level of maliciousness in a program that is under suspicion, signature-based detection uses predetermined signatures. However, anomaly-based detection uses its prior understanding of what constitutes typical behavior to determine whether a suspicious software is harmful. A subset of anomaly-based detection is known as specification- or rule-based detection. This branch creates guidelines and standards to define appropriate legal conduct, then uses those guidelines to determine whether a suspicious application is malevolent.

Cyber Deception-

By executing a cyber deception, the main goal is to make it possible to detect attacks and develop an adaptive cyber defensive strategy aimed at confusing the adversary. Although the growing reasons in this study include Big Data, theory games, and Artificial Intelligence to better cybersecurity methods against attackers, the sorts of cyber deception utilized typically used honeynets and honeypots [24].

Threat Hunting-

In order to identify sophisticated threats before an assault occurs, Threat hunting is the iterative practice of actively researching defenses across a variety of networks and security information. Research on threat-hunting technique deployment using Google Rapid Response was conducted by Rasheed, Hadi, and Khader [24]. In response, as well as through two separate tests: one for remote code execution and the other for client-side vulnerabilities [25]. Ko (2020) looked at how threat hunting differed from other cybersecurity-promoting practices including IDS, Cyber Intelligence, Forensics, Penetration Testing, and Cyber Defense [26].

Threats to Cybersecurity from CHATGPT :

While cybersecurity is significantly suppressed by AI and Big Data Analytics, there is evidence that contrary may also be right. With recent release of ChatGPT, there are significant cybersecurity risks. ChatGPT is a chatbot platform that creates a conversational interface by fusing Artificial Intelligence (AI) with huge Natural Language Processing (NLP) algorithms. It intended to allow user to text in Natural Language and get comprehensible responses in the same Natural Language. Based on the context, ChatGPT determines the response by analyzing the user's input. The software interprets user input using machine learning and rules-based algorithms. After processing the data, the platform generates a response in accordance with the guidelines [17, 32]. After then, the reply is sent. return information in a way that the user can comprehend. The ability of ChatGPT to process Natural Language input and provide response that are customized to user unique needs and circumstances is one of its key advantages; this facilitates user interaction with the chatbot and lowers the possibility that they would receive an unsuitable response. Furthermore, the platform has the potential to generate more customized user experiences by offering tailored support or contextual recommendations.

It has been noted that ChatGPT is drawing in cybercriminals despite these expected advantages. The platform might potentially keep constructing a pathway that makes it simple for hackers to launch cyberattacks [29, 33]. Cybercriminals have found multiple instances, according to Check Point Researchers (CPR), where ChatGPT from OpenAI has aided them in their nefarious actions. According to a well-known hacker community, one instance in which the cybercriminals are utilizing ChatGPT is the creation of Infostealer.

Python-based malware is created via ChatGPT [16, 31, 32]. Criminals can also use ChatGPT to construct an encryption tool. It was verified by evidence provided by US DoD is tagged by the CPR that he had written in Python script using OpenAI. The Python script had the ability to decrypt data and routines for encryption [19, 24].

In addition to the two malware-focused practices already stated, there is a perception that ChatGPT encourages fraud. As one of the activities on the Dark Web is the sale of malware, an analysis by CPR indicates the potential for the Dark Web Marketplace to grow. This is demonstrated via a cybercriminals' code, where the API is the third party. This algorithm was designed to obtain real-time cryptocurrency, specifically Etherium, Monera, and Bitcoin [32, 33]. Even though ChatGPT is still in its early phases of development, there is a good chance that, if left unguarded, this platform might contribute to an increase in cybersecurity risks. In conclusion, AI may have a harmful effect on cybersecurity.

Upcoming Directions :

Understanding the future of cybersecurity requires identifying several key directions, as seen in Fig. 3, which centers on the challenges and requirements encountered by the field as well as issues that come from deployment of AI and Big Data Analytics.

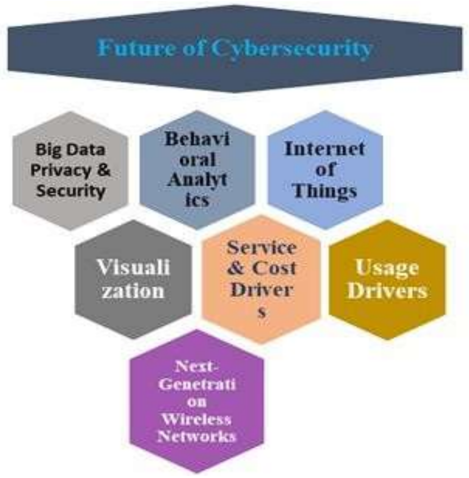

Fig. 3. Cybersecurity Future

Big Data Privacy and Security-

A demonstrated by difficulties in using Big Data Analytics, providing security to Big Data is significant issue that need to be resolved. In order to determine the provenance of data, several authentication systems must be used to ensure the trustworthiness of the data collected from various sources [27]. Additionally, Big Data needs sufficient improvements to the current anomaly detection methods that have been effectively implemented in conventional security systems in order to safeguard data accuracy in an automated, real-time manner and identify any potentially dangerous events within. [31]. In terms of privacy, more privacy-preserving Big Data analytics schemes should be created. This is especially important in the context of cybersecurity. Government organizations should monitor and implement additional regulations to protect the privacy of data fragments linked to individual identities issues hidden.

Behavioral Analytics-

Behavioral analytics is another area where cybersecurity may be improved. This involves taking context information into account to increase the likelihood of anomalous actions and identify trends that point to theft, fraud, and other cybersecurity concerns. Traditionally, cyber solutions were only effective against external incursions and were unable to identify internal breaches [33]. Big Data analytics systems can be used for internal threat identification through anomaly detection and for predicting unexpected behaviors by tracking the actions of both authorized and normal users [28]. The frequency with which a file is downloaded or a database is viewed are two examples of association behavior. But other internal dangers won't be possible to be found other than by modeling aberrant and typical user behaviors.

Visualization-

In order to guarantee the provision of Security Analytics by utilizing knowledge that will enable them to identify cybersecurity threats more quickly, it is anticipated that the advancement of visualization tools will be addressed in the near future. Keylines is one example of an application that already has certain visualization dashboards connected to security. However, there is a need for better development, particularly in light of the necessity for real-time processing and data streaming as well as the growing number of Data Sources that make Data Visualization more difficult [29].

Internet of Things (IoT)-

Internet of Things (IoT) has application that include big data, such as ITS, smart cities, habitat monitoring, and many more. These applications require the processing and generation of streaming data in real-time. Since every application has various needs and specifications when it comes to security and privacy, suitable design augmentation and enhancement are required to meet these needs. As a result, it is imperative to use big data analytics for addressing problems related to IoT application security [30].

Wireless Networks-

A single infrastructure will be needed to provide diverse services, including mobile broadband, incredibly dependable and low-latency communications and enhanced machine-type communications, in the future self-drive network in flexible and effective manner. Additionally, such a network will be required to support current access points, such as LTE (long-term evolution), Wi-Fi, and 5G (fifth generation). Furthermore, they will have to manage a heterogeneous network comprising many base stations (BSs), Femto, micro, and macro applications, as well as pico-BSs. It is difficult for a mobile network operator to efficiently run a network that can allow for flexibility and meet the needs of diverse services [31]. Furthermore, mobile network operators struggle greatly to meet the constantly rising capacity demands and expand their coverage areas while working with limited resources as well as a restricted stock of resources like spectrum. The configuration of optimization, control, and network planning manuals will exacerbate the problems.

Furthermore, human-machine interactions can occasionally be costly, error-prone, and time-consuming. On the other hand, the goals of both the cellular network and the widespread automation of various entities are currently MNO's main concerns when discussing how to lower operating costs. The system ought to be intelligent, self-aware, and capable of self-adaptation based on its sense of operating costs. It is capable of managing and participating in the independent operation of the networks, as well as sporadically running the services. Reactive maintenance that is cautious is no longer effective. Predictive and proactive network maintenance for the factors can be accomplished by using big data analytics [32]. The network can do more than anticipated; for example, it can advise and/or support the unit. It does this by taking into account the kind of a Data Source range, the pace of the flowing data of upkeep and operation with choices concerning choices and the results of activities [33]. In addition to identifying associations and abnormalities that are not apparent through manual inspection, artificial intelligence and machine learning play a vital role in uncovering the hidden characteristics of wireless networks and in suggesting novel strategies required for Network Operations , installations.

Cost and Service Factors-

Although there is always a lot of demand from subscribers, most nonetheless need to have the desire to increase the wireless payout. An application of network resources must be optimized quickly in such a context. Furthermore, the QoE paradigm is evolving from a network-centric to a user-centric one. Owing to this, mobile network operators must become knowledgeable about QoE in general as it relates to KPI networks. Mobile network providers also want to keep their customers [33]. As a result, mobile network operators must maintain the lowest levels of churn, improve efficiency to preserve profit margin, manage traffic depending on application and service, and improve network performance and quality of experience without compromising costs.

Usage Drivers-

User-oriented service model's analytics control and maintain the wireless devices, different kinds of traffic and subscribers in different ways according to their requirements and the plans of mobile network operators. The traffic patterns, subscriber equipment, and subscriber profiles are all varied. Furthermore, the traffic loader associated with wireless application that growing faster than the capacity and mobile network operators are facing challenging issues related to efficiently and economically increasing network capacity that increasing resource use therefore important [30]. In order for MNOs to properly manage the network traffic in real-time, they must have a thorough awareness of the problems posed by network load. This is where analytics comes in.

Recommendations & Conclusion :

- The idea of preventing future Cyber-attacks by using ChatGPT and Big Data analytics is not without risk. It's critical to set up responses quickly since attackers and malicious actors are always refining their attack tactics. Furthermore, there are a lot of misconceptions about the cybersecurity problems that ChatGPT and Big Data analytics can solve. Though the industry is currently lagging behind, AI and Big Data Analytics have been positioned as a solution to many Cyber Security issues. A variety of current technologies, including intrusion detection and cyber intelligence Human interaction is still needed in several areas, including intrusion detection and response (NDR), cyber defense, Security Orchestration, Automation and Response (SOAR), Intrusion Detection Systems (IDS) and forensics.

- While implementing AI technologies and Big Data Analytics is step toward replacing the conventional reactive approach, handling large-scale threats will require more than just rule-based preventative measures. Because of ChatGPT's human-like involvement, hackers from all over the world are becoming more interested in it than in any other algorithm. It's critical to understand the potential advantages and disadvantages of ChatGPT as its use increases. Although ChatGPT can perform business support duties and provide information to clients more rapidly and accurately, there are worries that it could be used as a hacking tool. In order to protect themselves against cybercrime related to ChatGPT, people and organizations need to be cautious and take the appropriate care. In order to identify and stop these kinds of assaults, users must have the necessary security controls and procedures must be put into practice, and technology for countermeasures must be upgraded frequently. In order to protect ourselves we'll have to wait and see how the states and business community react to ChatGPT in the future.

- To sum up, there is no denying the combined influence of ChatGPT and Big Data Analytics on cybersecurity. When these technologies are used wisely and responsibly, the cybersecurity environment becomes more proactive, robust, and adaptable. The future of cybersecurity in a dynamic and interconnected digital world is expected to be shaped by the further advancement of these technologies as well as a dedication to addressing issues and ethical considerations.

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 cybercrimes 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 IoTarchitect's guide to attainable security and privacy. CRC Press, 2019.
4. Holcomb, Sean D., William K. Porter, Shaun V. Ault, Guifen Mao, andJin 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. 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.
9. 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.
10. 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.
11. 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.
12. 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).
13. Zappone, Alessio, Marco Di Renzo, and Mérouane Debbah. "Wirelessnetworks design in the era of deep learning: Model-based, AI-based, or both?." IEEE Transactions on Communications 67, no. 10 (2019): 7331-7376.
14. 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.
15. Nieto, Ana, Ruben Rios, and Javier Lopez. "IoT-forensics meets privacy: towards cooperative digital investigations." Sensors 18, no. 2 (2018): 492.
16. 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.
17. Asamoah, Harrison. "Antivirus software versus malware." Архів кваліфікаційних робіт (2020).
18. 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.
19. 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.
20. 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 preprintarXiv:2012.04405 (2020).
21. 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).
22. 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.