IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 1, January 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.118

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 1, January 2023 ||

| DOI:10.15680/IJIRSET.2023.1201109 |

A Study on Detecting and Preventing Threats by using Artificial Intelligence in Cybersecurity

Suresh B

Senior Scale Lecturer, Government Polytechnic, Koppal, Karnataka, India

ABSTRACT: This research assesses the impact of Artificial Intelligence (AI) on cybersecurity through an exhaustive review of the existing literature. The study depicts AI as a dual-faced entity, serving both as a potent defense against cyber threats and as a potential vulnerability. By harnessing machine learning algorithms, AI significantly enhances the efficiency of predicting, detecting, and responding to cyber-attacks. Nonetheless, it also highlights the significance of secure AI development and human oversight. Looking ahead, the role of AI in cybersecurity is expected to grow, opening new opportunities for preemptive defense mechanisms against cyber threats. Consequently, despite the challenges imposed by AI, its potential remains too promising to overlook. Artificial intelligence (AI) is considered one of the most promising methods for addressing cybersecurity threats and providing security. In this study, we present a systematic literature review (SLR) that categorize, map and survey the existing literature on AI methods used to detect cybersecurity attacks in the IoT environment. The scope of this SLR includes an in-depth investigation on most AI trending techniques in cybersecurity and state-of-art solutions. However, several studies have proposed smart intrusion detection systems (IDS) with intelligent architectural frameworks using AI to overcome the existing security and privacy challenges.

KEYWORDS: Artificial Intelligence (AI), cybersecurity, cyber-attacks, cyber threats, IoT environment, intrusion detection systems (IDS).

I. INTRODUCTION

A cyber security threat refers to malicious activities carried out by individuals with harmful intentions, aiming to cause disruption, damage, and chaos in cyberspace. Cybersecurity, on the other hand, encompasses the proactive actions taken to secure the vast realm of cyberspace, which includes information, data, and software, from all potential threats. As technology continues to advance, cybercriminals have become more creative and adept at evading traditional security measures. They constantly stay ahead of the game, making it increasingly challenging for individuals and organizations to effectively protect themselves from cyber threats. This has led to a serious increase in cybersecurity threats, and this requires unconventional and innovative solutions to maintain our safety and privacy. In the 21st century, humans have made multiple revolutions in the field of cybersecurity to safeguard systems and networks from unforeseen threats. However, it is becoming increasingly evident that relying solely on human efforts has its limitations. No matter how sophisticated the security measures are, there will always be vulnerabilities that cybercriminals can exploit. AI platforms assist enterprises in the development, management, and deployment of machine learning and deep learning models at scale. Decreasing software development tasks such as data management and deployment make AI technology more accessible and economical. With the increase in cyber risks, artificial intelligence (AI) is increasingly widely employed to monitor and restrict cybercrime. This is clear that only smart technologies can help defend against sophisticated cyber devices, with the sophistication of malware and cyber-arms increasing exponentially in the past two years.

II. LITERATURE REVIEW

Bibhu Dash (2022) Artificial intelligence is opening up new avenues for value generation in enterprises, industries, communities, and society as a whole. Technology has been researched to be relevant in many aspects of the world. This factor has made it to be included mainly in different businesses and industries. The applications of AI are endless to discuss. The research below examines the applications of artificial intelligence (AI) in cybersecurity. Cybersecurity has also been a growing concept in the technological industry. Many companies have included information technology in their businesses. This factor has required companies and organizations to demand more security measures. The attempt to protect the available data and information has resulted in the growth of cybersecurity, and AI has been seen to influence cybersecurity heavily on a large scale. This factor has made machine learning to be significantly induced in

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 1, January 2023 ||

| DOI:10.15680/IJIRSET.2023.1201109 |

recent technologies supporting cybersecurity. The research paper performs a literature review and examines the overall impacts of artificial intelligence on cybersecurity.

Carina Barbio (2022) Communication for the Internet of things (IoT) currently is predominantly narrowband and cannot always guarantee low latency and high reliability. Future IoT applications such as flexible manufacturing, augmented reality and self-driving vehicles rely on sophisticated real-time processing in the cloud to which mobile IoT devices are connected. High-capacity links that meet the requirements of the upcoming 6G systems cannot easily be provided by the current radio-based communication infrastructure. Light communication, which is also denoted as LiFi, offers huge amounts of spectrum, extra security and low-latency transmission free of interference even in dense reuse settings. We present the current state-of-the-art of LiFi systems and introduce new features needed for future IoT applications. We discuss results from a distributed multiple-input multiple-output topology with a fronthaul using plastic optical fibre.

Rammanohar Das (2021) Without substantial automation, individuals cannot manage the complexity of operations and the scale of information to be utilized to secure cyberspace. Nonetheless, technology and software with traditional fixed implementations are difficult to build (hardwired decision-making logic) in order to successfully safeguard against security threats. This condition can be dealt with using machine simplicity and learning methods in AI. This study provides a concise overview of AI implementations of various cybersecurity using artificial technologies and evaluates the prospects for expanding the cybersecurity capabilities by enhancing the defiance mechanism. We may infer that valuable applications already exist after the review of current artificial intelligence software on cybersecurity.

Erwin Adi (2020) Cybersecurity is a fast-evolving discipline that is always in the news over the last decade, as the number of threats rises and cybercriminals constantly endeavor to stay a step ahead of law enforcement. Over the years, although the original motives for carrying out cyberattacks largely remain unchanged, cybercriminals have become increasingly sophisticated with their techniques. Traditional cybersecurity solutions are becoming inadequate at detecting and mitigating emerging cyberattacks. Advances in cryptographic and Artificial Intelligence (AI) techniques (in particular, machine learning and deep learning) show promise in enabling cybersecurity experts to counter the ever-evolving threat posed by adversaries.

III. AI IN CYBER SECURITY: RISKS OF AI

Artificial intelligence (AI) has been enhancing cyber security tools for years. For example, machine learning tools have made network security, anti-malware, and fraud-detection software more potent by finding anomalies much faster than human beings. However, AI has also posed a risk to cyber security. Brute force, denial of service (DoS), and social engineering attacks are just some examples of threats utilizing AI. The risks of artificial intelligence to cyber security are expected to increase rapidly with AI tools becoming cheaper and more accessible. For example, you can trick ChatGPT into writing malicious code or a letter from Elon Musk requesting donations, you can also use a number of deepfake tools to create surprisingly convincing fake audio tracks or video clips with very little training data. There are also growing privacy concerns as more users grow comfortable sharing sensitive information with AI.

The risks of AI in cyber security
Like any technology, AI can be used for good or malicious purposes. Threat actors can use some of the same AI tools designed to help humanity to commit fraud, scams, and other cybercrimes.

Let's explore some risks of AI in cyber security:
1: Cyber attacks optimization
Experts say that attackers can use generative AI and large language models to scale attacks at an unseen level of speed and complexity. They may use generative AI to find fresh ways to undermine cloud complexity and take advantage of geopolitical tensions for advanced attacks. They can also optimize their ransomware and phishing attack techniques by polishing them with generative AI.

2: Automated malware
An AI like ChatGPT is excellent at accurately crunching numbers. According to Columbia Business School professor Oded Netzer, ChatGPT can already "write code quite well." Experts say that in the near future, it may help software developers, computer programmers, and coders or displace more of their work. While software like ChatGPT has some protections to prevent users from creating malicious code, experts can use clever techniques to bypass it and create

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 1, January 2023 ||

| DOI:10.15680/IJIRSET.2023.1201109 |

malware. For example, one researcher was able to find a loophole and create a nearly undetectable complex data-theft executable. The executable had the sophistication of malware created by a state-sponsored threat actor.

3: Physical safety

As more systems such as autonomous vehicles, manufacturing and construction equipment, and medical systems use AI, risks of artificial intelligence to physical safety can increase. For example, an AI-based true self-driving car that suffers a cyber security breach could result in risks to the physical safety of its passengers. Similarly, the dataset for maintenance tools at a construction site could be manipulated by an attacker into creating hazardous conditions.

AI privacy risks

In what was an embarrassing bug for OpenAI CEO Sam Altman,ChatGPT leaked bits of chat history of other users. Although the bug was fixed, there are other possible privacy risks due to the vast amount of data that AI crunches. For example, a hacker who breaches an AI system could access different kinds of sensitive information.

An AI system designed for marketing, advertising, profiling, or surveillance could also threaten privacy in ways George Orwell couldn't fathom. In some countries, AI-profiling technology is already helping states invade user privacy.

Advantages of AI in Cybersecurity

AI presents many advantages and applications in a variety of areas, cybersecurity being one of them. With fast-evolving cyberattacks and rapid multiplication of devices happening today, AI and machine learning can help to keep abreast with cybercriminals, automate threat detection, and respond more effectively than conventional software-driven or manual techniques.

Fundamental Concepts and Applications of AI in Cybersecurity

AI bears the potential to revolutionize cybersecurity methods by augmenting the capabilities of security systems through dynamic responses and predictive capabilities. At its core, AI operates on the ability to learn patterns, recognize anomalies, and adapt to changes through machine learning and neural networks. This aspect is of crucial importance in cyber threat detection and mitigation. AI powered antivirus software, intrusion detection systems, and predictive threat intelligence systems are prevalent examples of cybersecurity applications of artificial intelligence. AI enables these systems to identify, respond, and adapt to cyber threats in realtime, a benefit that significantly strengthens cybersecurity frameworks.

IV. RESEARCH METHODOLOGY

The approach to detect cybersecurity attacks in IoT using AI is widely developing. Due to this, there's need to explore in-depth analyses through examining previous studies. Our study goal is to identify what are the most effective AI methods to detect attacks, threats in IoT systems and investigate the available practice to reduce those attacks using effective techniques. To get an all-round impression of the junction between cybersecurity and AI, we used four databases: Scopus, Web of Science, ACM digital library also IEEE Xplore. Quality assessment was based on original research and a few review articles. To maintain the quality of the review, all duplicate records were thoroughly checked. In particular, the abstracts of all research articles included in the review process were checked in detail and filtered to ensure their quality and relevance. To improve our search results and to make them more accurate, the authors refined various keywords from the search machine to obtain the maximum coverage. In the additional step, obtained results were filtered. Last, the findings were categorized by the number of certifications. Besides those documents were selected, which had more than five citations. On the other side, newly published research study that had less than five citations/references but innovative methods/approaches were also selected. For this purpose, readers will have an idea about IoT security using AI especially those new in the area. Some studies focused on traditional methods, while some focused on DL techniques for IoT security. In our study, we explore both ML and DL techniques for IoT security with feature recommendations.

V. RESULTS AND DISCUSSIONS

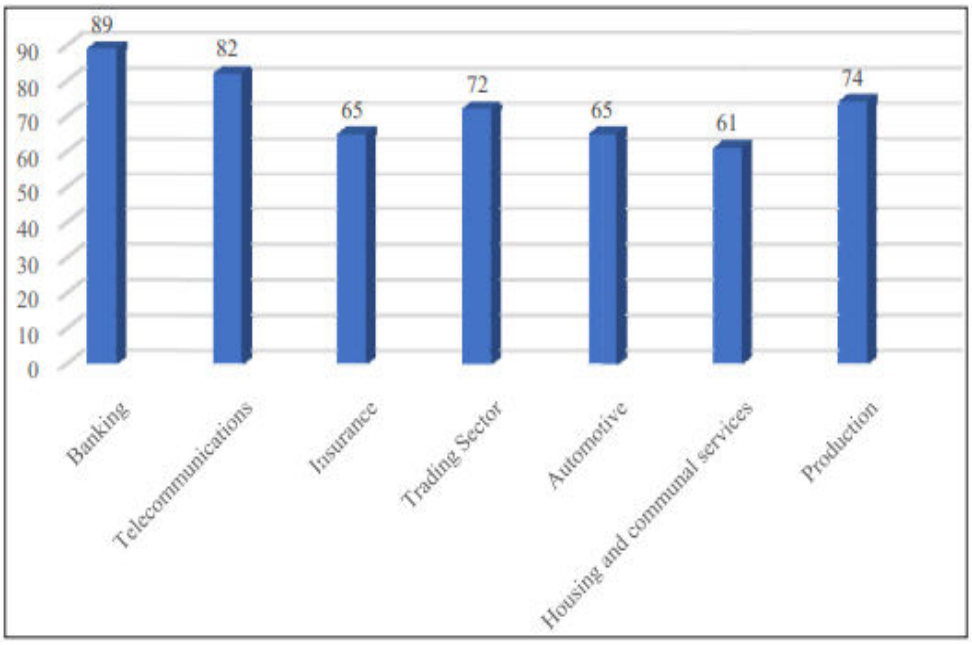
Secondly, only related literatures published within the last five years were considered because this paper aims to present an overview of recent developments of Artificial Intelligence applications in the area of cyber security. Manuscripts published later than five years but had novel approaches were selected. The introduction of artificial intelligence-based tools and methods in cybersecurity operations is now positioned as a relevant strategy. It is a

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 1, January 2023 ||

| DOI:10.15680/IJIRSET.2023.1201109 |

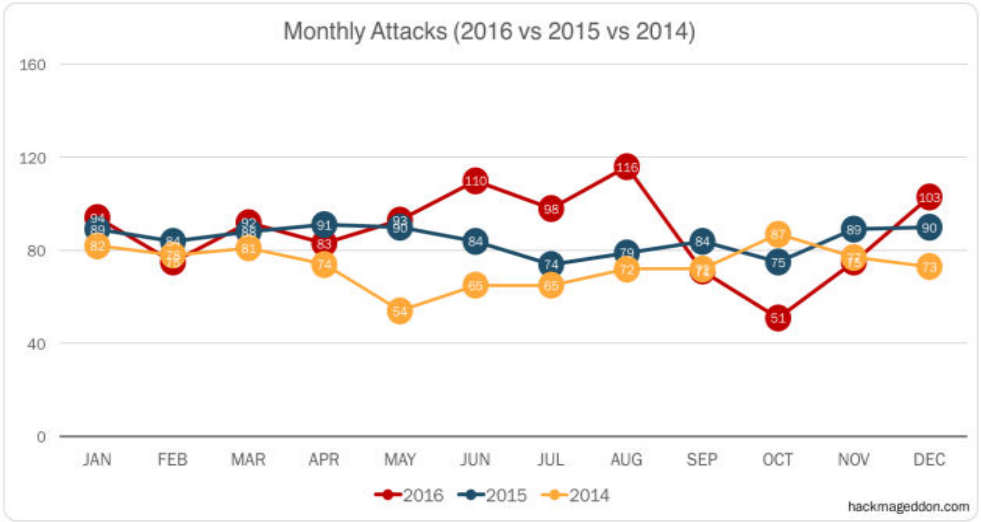
compulsory necessity to counter cyberattacks that are becoming even more unpredictable. This trend is confirmed by statistics that show that by 2025, 63% of organizations plan to integrate AI. Moreover, 69% of them believe that it is only possible to respond effectively to cyber threats with the help of AI.



Graph 1: Share of organizations in the global community that use AI capabilities to protect cyber security

The latest area of AI application is to improve the cybersecurity of cloud providers by automating the analysis and detection of potential threats, tracking anomalies in information data and traffic patterns, and predictive security based on the analysis of data from previous security incidents. Such prerequisites enable cloud providers to take preventive measures to prevent and mitigate risks.

The statistics are not inclusive, but the purpose is to outline the cyber threat landscape. During 2016, the level of attacks was quite similar to the last year. However, a peak was experienced in the central months. Starting from September 2015, it registered a more steady activity until December, when 2016 experienced a new tail of events.



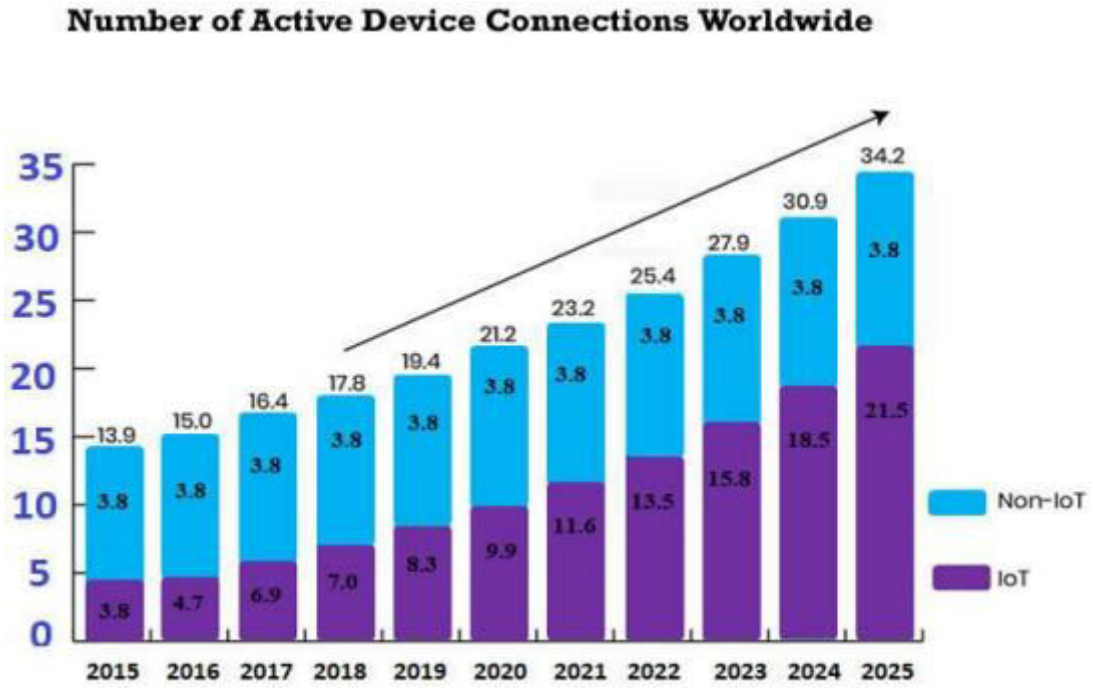
Graph 2: Graphic Representation showing comparative analysis in monthly attacks of (2016 vs. 2015 vs. 2014)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 1, January 2023 ||

| DOI:10.15680/IJIRSET.2023.1201109 |

There has been an increase in connectivity worldwide over the last decade. It has become mandatory to carry a device to stay linked all the time. The internet remains evolving in terms of the number of users, its size, heterogeneity of devices, and the type of applications that are developed for the ease of mankind. Today, similar to electricity, water, and gas, the Internet has become a significant utility in the daily lives of people around the world. As more devices connect to the internet, it is susceptible to more attacks by cybercriminals.



Graph 3: Graphic representation showing an increase in IoT over the years

Although AI's role in cracking cybersecurity issues continues to be inspected some fundamental apprehensions surround where AI deployment can become regulated. For example, as machines become imperative solutions for humanity, these will consume fundamental resources for life increasingly. When humans and machines strive for scarce resources, a new form of domination will propagate. This, in turn, will provoke a new research avenue.

VI. CONCLUSION

This study makes recommendations to address some of the challenges through research and identifies key areas to guide stakeholders driving cybersecurity research and development on AI and cybersecurity. In a scenario where malicious intelligence and cyber threats are rising exponentially, sophisticated cybersecurity strategies cannot be ignored. Also, security against large-scale threats, with very minimal resources, has been demonstrated from experience in DDoS prevention if smart approaches are used. Publications reviews indicate that studies into artificial neural networks offer the findings of AI most widely relevant to cybersecurity. Neural network implementations continue on cybersecurity. For many fields where neural networks weren't the most appropriate technologies, sophisticated cybersecurity approaches are still desperately needed. Such fields include decision support, understanding of the situation, and control of information. Too fast general artificial intelligence has advanced cannot be known, but a possibility remains that the perpetrators will exploit a new form of artificial intelligence as long as it is accessible. The research highlights the significance of maintaining regular surveillance and modifying cybersecurity measures to tackle the constantly evolving AI-driven threats effectively. Organizations must balance utilizing AI for defensive purposes and allocating resources toward skilled human personnel. This approach guarantees the effective management of potential risks that may emerge in the field of AI-powered cybersecurity.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 1, January 2023 ||

| DOI:10.15680/IJIRSET.2023.1201109 |

REFERENCES

1. Bibhu Dash (2022), "The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review",Ijarcce,ISSNno:2278-1021,Vol.11(9), Pages.81-90.DOI:10.17148/IJARCCE.2022.11912
2. Carina Barbio (2022), "ELIoT: enhancing LiFi for next-generation Internet of things",EURASIP Journal on Wireless Communications and Networking, Vol.(1),DOI:10.1186/s13638-022-02168-6
3. Erwin Adi (2020), "Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity",IEEE Access ISSNno:2169-3536,Vol.(99),Pages.1-1.DOI:10.1 109/ACCESS.2020.2968045
4. Mohammad Alshehri (2022), "Secure framework against cyber attacks on cyber-physical robotic systems",Journal of Electronic Imaging,ISSNno:1560-229X,Vol.31(6),DOI:10.1117/1.JEI.31.6.061802.
5. Naveed Naeem Abbas (2019), "Investigating the applications of artificial intelligence in cyber security",Scientometrics,ISSNno:0138-9130,DOI:10.100 7/s11192-019-03222-9.
6. Rammanohar Das (2021), "Artificial Intelligence in Cyber Security",Journal of Physics: Conference Series,ISSNno:1742-6596,Vol.1964,doi:10.1088/1742 -6596/1964/4/042072
7. Sadiku, M. N. O. (2020), "Artificial Intelligence in Cyber Security", International Journal of Engineering Research and Advanced Technology, ISSNno:2454-6135,Vol.06(05),Pages.01–07.https://doi.org/10.31695/ijerat.2020.3612.
8. Tyugu, E. (2011) "Artificial intelligence in cyber defense", 2011 3rd International Conference on Cyber Conflict, ICCC 2011 - Proceedings,ISSN no:2278-1021,Pages.95–105.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details