Dr B. MANJULA -ARTIFICAL INTELLIGENCE FOR SUSTAINABLE DEVELOPMENT:- CHALLENGES AND OPPORTUNITIES (2022)

Proceedings of

2nd INTERNATIONAL VIRTUAL CONFERENCE

ON

ARTIFICIAL INTELLIGENCE FOR SUSTAINABLE DEVELOPMENT :- CHALLENGES AND OPPORTUNITIES

25th November 2022

Organized by

SCHOOL OF COMMERCE

VET Institute of Arts and Science
(Co-education) College
Affiliated to Bharathiar University
An Institution Run by Vellalar Educational Trust
Thindal, Erode – 638 012
Tamil Nadu, India.

Proceedings of

2nd INTERNATIONAL VIRTUAL CONFERENCE

ON

ARTIFICIAL INTELLIGENCE FOR SUSTAINABLE DEVELOPMENT:- CHALLENGES AND OPPORTUNITIES

25th November 2022

Organized by

SCHOOL OF COMMERCE

VET Institute of Arts and Science
(Co-education) College
Affiliated to Bharathiar University
An Institution Run by Vellalar Educational Trust
Thindal, Erode – 638 012
Tamil Nadu, India.

INSTITUTION'S INNOVATION COUNCIL

SHANLAX PUBLICATIONS

Title: "ARTIFICIAL INTELLIGENCE FOR SUSTAINABLE
DEVELOPMENT:- CHALLENGES AND
OPPORTUNITIES"

Editor's Name: Dr. L. Rajendran
Dr. P. Vellingiri
Dr. S. Arulraj
Dr. P. Murali

Published by: Shanlax Publications,
Vasantha Nagar, Madurai – 625003,
Tamil Nadu, India

Publisher's Address: 61, 66 T.P.K. Main Road,
Vasantha Nagar, Madurai – 625003,
Tamil Nadu, India

Printer's Details: Shanlax Press, 66 T.P.K. Main Road,
Vasantha Nagar,Madurai – 625003,
Tamil Nadu, India

Edition Details (I,II,III): I

ISBN: 978-93-95422-56-7

Month & Year: December, 2022

Pages: 259

Price: ₹850/-

THE ROLE OF ARTIFICIAL INTELLIGENCE IN CYBER SECURITY

Dr. B. Manjula
Islamiah Women's Arts and Science College
#10, Bypass Road, New town, Vaniyambadi,
Tirupattur District, Tamil Nadu

Abstract

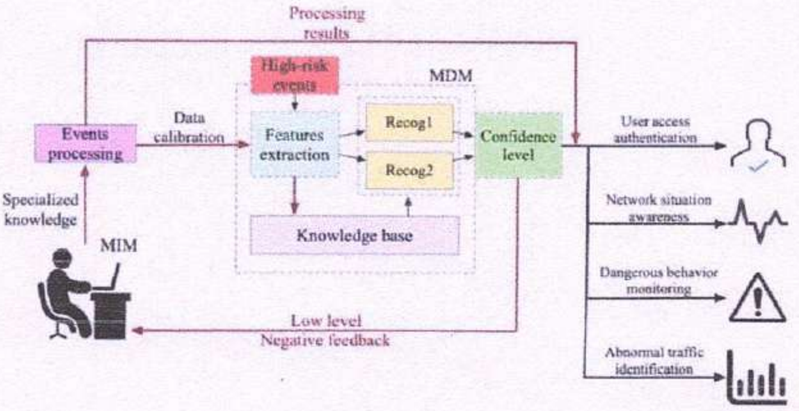
In the digital age, cyber security has grown to be a big concern. Data breaches, identity theft, captcha cracking, and other similar issues frequently harm millions of people as well as corporations. Inventing the proper rules and processes and putting them into practice with exacting perfection to combat cyber-attacks and crimes has always been a challenge. Recent advances in artificial intelligence have significantly increased the risk of cyber attacks and other crimes. It has been used in practically all branches of engineering and research. AI has sparked a revolution in fields like robotics and healthcare. Cybercriminals were unable to avoid this ball of fire, and as a result, "ordinary" cyber attacks have evolved into "intelligent" ones. This article talks about exact techniques in artificial intelligence, the applications of those techniques in cyber security and the competence of artificial intelligence and cyber security in future.

Keywords : *Artificial Intelligence, Cyber Security, Machine Learning, Technologies and Computer*

Introduction

Artificial Intelligence (AI) is a branch of science which transaction by means of helping machines find solutions to complex problems in a additional human being like Fashion. This typically entails taking traits of human intellect and implementing them as computer-friendly algorithms. Making a computer, a robot that is controlled by a computer, or a piece of software think intelligently like a human brain is known as artificial intelligence. Artificial intelligence is when a machine, particularly a computer system, stimulates human intelligence processes.

Structure



Cyber Crime - Meaning

Any illicit activity directed through electronic means that compromises the security of computer systems and the data they handle is known as "cybercrime" or "computer crime." Cybercrime is essentially criminal activity carried out in a virtual environment where data about individuals, things, facts, events, phenomena, or processes are represented mathematically, symbolically, or in any other way and transmitted through local and international networks.

Who are involved in cyber crime

There are three sorts of people who participate in cybercrime:

The Idealists (Teenager)

They are typically not adults with advanced training or skills, but rather adolescents between the ages of 13 and 26 looking for social acceptance.

The Greed – Motivated (Career Criminals)

These cybercriminals are risky since they are frequently callous and willing to commit any crime as long as it results in financial gain.

The Cyber – Terrorist

They are the most recent and hazardous group. Their key motivations include a particular cause they support in addition to money. To make a point, they frequently threaten people by email and delete data from networks used mostly by the government. The threat posed by cyber terrorism is comparable to that posed by biological, chemical, or nuclear weapons.

Cyber Security

Cyber security is the application of technologies, processes, and controls to protect systems, networks, programs, devices and data from cyber-attacks. This aims to reduce the risk of cyber-attacks and protect against the unauthorized exploitation of systems, networks, and technologies.

Cyber Security Law

Cyber Laws give up legal recognition to electronic documents and a structure to support e-filing and e-commerce transactions and also afford a legal structure to reduce, ensure cybercrimes. significance of Cyber Law: It covers all transactions over the internet. Track all the activities on the interment. **Cybercrime, the** main law **on** cybercrime in India, **is** covered by the Information Technology Act, **2000** and the Indian Penal Code, 1860. It is the Information Technology **Act** of **2000 that addresses** issues related to **cybercrime** and electronic commerce.

Modern Challenges in Cyber security

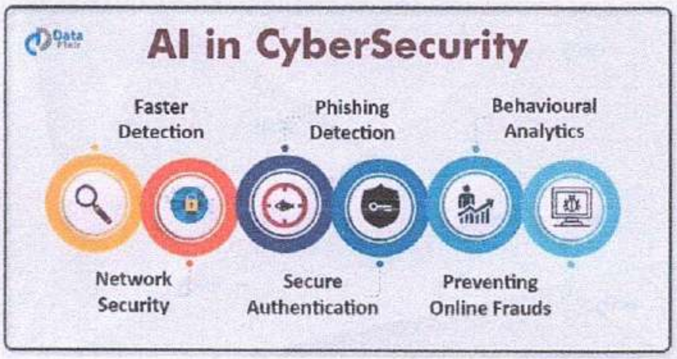
Cyber security is a shared responsibility, which boils down to:

The more systems we cyber security protect, the safer we are all. Now that you have a basic idea of how the cyber world affects all entities, from individual to organizational to national to international levels, let's dive into the complexities being created by technology. Let's see. .example: Artificial Intelligence, Machine Learning, Blockchain, Deep Learning, Big Data Analysis, Data Science, Internet of Things, etc.

1. **Technologies:** Technologies is distributes everywhere each single day and predators (cyber criminals) are continually spying in search of loopholes. Continually rising rate of cybercrimes is generating 3.5 million new jobs in the ground of cyber security, which will remain empty. Elevations in new technologies in half a decade have greater than before the security necessities about three hundred and fifty (350) times, an enormous rise.
2. **User:** Technologies are not only the challenges to cyber security, but user at huge scales are also one. The habit of users of doing things without opinion and occasionally unawareness of threats associated with the facilities they use are some general reasons following the same. We could also not ignore the participation of some user in malicious activities and negligent behavior of few people at higher authorities. Many a times, it is just one click of user, which makes all the disaster
3. **Financial Expenditure:** While considering the scenario of cyber security, enrichment in the technologies, goods and services are just one face of it and many a times we could not see the other one, the expenses in these enhancements. People and organizations only use up on cyber security when they become victim of cyber-attacks. Investment in cyber security considering future threats is an obsolete carry out giving invitations to predators (cyber criminals).

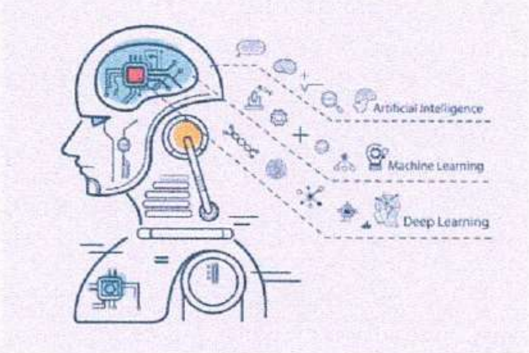
AI Comes To Release

AI and cyber security were not related at all. But as time went on, the boundaries blurred. CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is a very good example of the relationship between AI and cyber security.



Artificial Intelligence

The ability of machines to make decisions and perform tasks that simulate human intelligence and behavior.



Applications of AI In Cyber Security

1. **Improve network security**

   Network security deals with the protection against destruction, unauthorized access, and misuse of files and data in a system. It also protects the confidentiality of a network within an organization. AI can be utilized to automatically analyze the network traffic for any potential breaches or unauthorized access.

2. **Detect advanced malware**

   AI cyber security threat detection systems are mostly useful for finding malware applications that can keep changing themselves to avoid getting detected (e.g., polymorphic and metamorphic malware).

3. **RISING YOUR ORGANIZATION'S DATA PRIVACY**

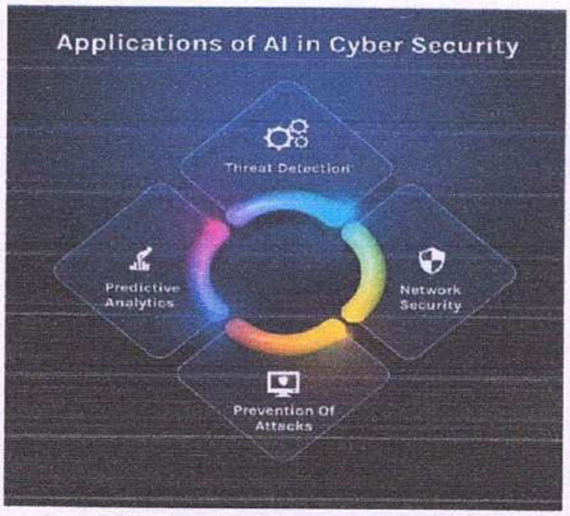
   AI cyber security systems can help avoid breaches of responsive organization and customer data.

4. **Taking Cloud Security to the Next Level**

   AI is a very important factor in preventing cyber-attacks against the cloud, as cyber-attacks against the cloud are occurring and evolving. Cloud service providers are actively using advanced AI to build more robust and resilient cyber security systems.

5. **Strengthen** IoT **security**

   The Internet of Things (IoT) is powering the world by connecting everything to the internet. Many companies are investing heavily in IoT, which has the potential to revolutionize nearly every industry. Managing the security of a human-scale mass of devices is impossible. Ultimately, AI will be the only option for automatically monitoring, detecting, and preventing cyber attack activity.



Malware Detection Using AI

Malware is a coined word combining the words "malicious" and "software". Malware can be viewed as a piece of code designed to harm computers, data/information and networks. Malware-related damages can appear only after these malicious codes are installed or implanted. The purpose behind this malware is to spy and steal sensitive data, provide system control to intruders, slow down or malfunction of infected system. Here are some malware.

1. **Virus:** Its full form is Vital Information Resources Under Seize. It is a computer program that can duplicate itself and infect a computer without consent or knowledge of the user.
2. **Worms:** Its major function is to self-replicate and infect other computers while remaining active on infected systems.
3. **Trojans:** A trojan horse (trojan) is a type of malware that disguises itself as legitimate code or software.
4. **Rootkits:** It is a software used by cybercriminals to increase control over a aim computer or network. It is the result of direct attack such as exploitation of known vulnerability or password. It conceals itself in the Operating System.
5. **Remote administration tools:** It is a software program that gives you the capability to control another device slightly.

6. **Botnets:** It is a network of computers infected by malware that are under the control of a single attacking party, known as the "bot-herder".
7. **Spyware:** Any software that installs itself on your computer and starts covertly monitoring your online behavior without your knowledge.

Signature Based Techniques

Traditional cyber-security techniques are primarily called "Signature-based techniques". Signature-based techniques are those approaches of information security that detect cyber-attacks or malware [section 7] by matching certain signatures (at least a byte sequence of code) of the instance of malware in question with the database of signatures of malware stored. The database has known malicious programs and they are called as "blacklists". The signature-based techniques assume that the malicious software can be described using the signatures (also called as malicious patterns).

This method fails completely in case of new attacks or malware, for which known patterns or signatures are not available. Unfortunately, the current scenario is against these techniques of signature detection. Still, it can be used at the beginning level. Nonetheless, signature-based techniques have once been one of the most common malware detection techniques.

Significant Role of AI In Cyber Security

1. Detecting New Threats

AI can be used to spot cyber threats and possibly malicious activities Conventional software systems can't keep up with the sheer number of new malwares created every week, so this is an area where AI can help.

AI systems are being trained to detect malware, run pattern recognition, and detect even the smallest behaviours of malware or ransomware attacks before they enter the system using sophisticated algorithms.

AI enables superior predictive intelligence through natural language processing, which curates data on its own by scraping articles, news, and cyber threat studies.

This can provide new anomalies, cyberattacks, and prevention strategies.

After all, cybercriminals, like everyone else, follow trends, so what's popular with them changes all the time. AI-based cyber security systems can provide the most up-to-date knowledge of global and industry-specific threats, allowing you to make more informed prioritisation decisions based not just on what could be used to attack your systems, but also on what is most likely to be used to attack your systems.

2. Battle Bots:

Bots account for a significant portion of internet traffic today, and they can be dangerous. Bots can be a real threat, from account takeovers using stolen credentials to bogus account creation and data fraud.

Manual responses will not suffice to combat automated threats. AI and machine learning assist in developing a comprehensive understanding of website traffic and distinguishing between good bots (such as search engine crawlers), bad bots, and humans.

AI allows us to analyse massive amounts of data and allows cyber security teams to adapt their strategy to an ever-changing landscape.

3. Breach Risk Prediction:

AI systems assist in determining the IT asset inventory, which is an accurate and detailed record of all devices, users, and applications with varying levels of access to various systems.

AI-powered systems can predict how and where you are most likely to be compromised, allowing you to plan and allocate resources to the most vulnerable areas. AI-based analysis provides predictive insights that allow you to configure and improve controls and processes to strengthen your cyber resilience.

Future Aspects And Scope

Cyber Physical Systems (CPS), which are on the rise as a result of the exponential development of technologies like the Internet of Things (IoT), artificial intelligence (AI), cloud computing, robots, drones, sensors, etc., are assisting manufacturers in increasing productivity, efficiency, and the autonomous operation of production lines. Businesses are investing a lot of money in automation and artificial intelligence, and by 2025, the Industrial IoT (IoT) industry alone is expected to reach $500 billion in revenue.

Given the high demand, it is difficult to recruit a workforce with the necessary skills and experience to establish effective defenses against cyber-attacks in a business. People are becoming more and more interested in pursuing cybersecurity courses. Given that there is a considerably greater demand than there is supply, this trend is anticipated to continue.

Cyber attacks will continue to grow and become more dangerous if ignored. By consistently making a sizable investment in people, this can be avoided. This can be accomplished either by recruiting cybersecurity specialists or by instructing staff members on the use of AI in cybersecurity systems.

Lack of Talents (Demand Versus Availability of Cyber Security Experts)

Many studies have discovered that due to lack of talents there is a misbalance in the require and availability of cyber security experts. With the exponential development of cyber threats, demand for skillful and qualified cyber security experts has also exponentially increased but their availability is a big question.

According to a survey by Leviathan Security Group it has been found that:

1. **16%** of the organizations felt only half of their applicants are experienced
2. **53%** of them said finding a qualified aspirant can take at least six months, in case they find one.
3. **32%** of them find it hard to fill the positions of cyber experts.
4. Reasons behind this lack of cyber experts can be the under-investments on cyber instruction, growth in cyber-attacks, demand of qualified experts and less involvement of women in cyber security ground.

Conclusion:

Artificial intelligence, undoubtedly, has unmatched potential for accuracy, speed, and scale in cybersecurity. Larger amounts of data are being generated by new technological developments like IoT, and with all of that data comes a growing number of analysis that need to be performed. Big data analysis in real time with tolerable accuracy has become too difficult for human intelligence to handle. We require a method for rapidly, efficiently, and intelligently sifting through the data "noise" in order to use it to strengthen our defences and reduce security risks. AI will be required in cybersecurity both now and in the future to create robust and resilient systems that are adaptable, scalable, and automated.

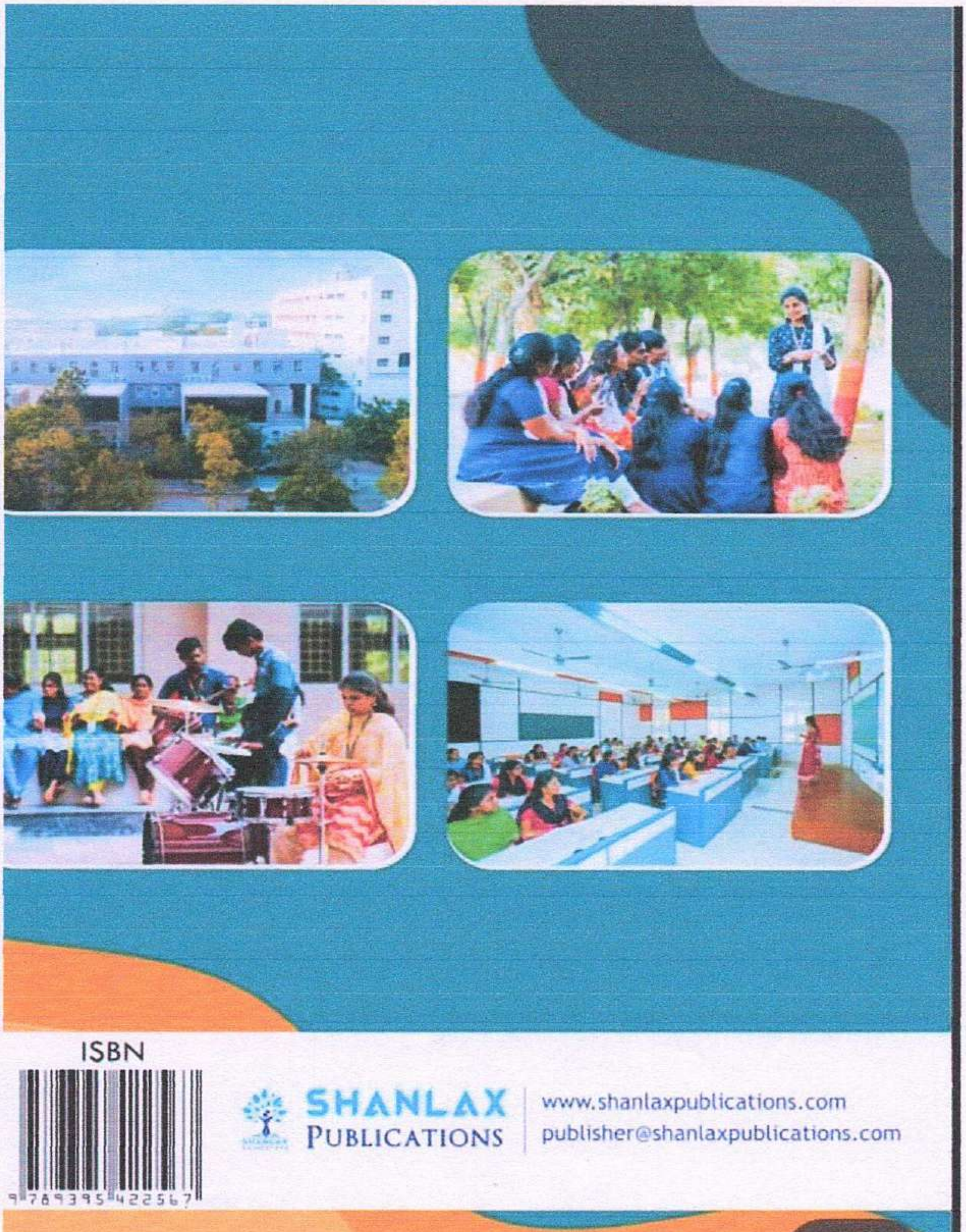
Instead of constantly monitoring the environment for suspicious activity, cybersecurity experts can utilise AI to reinforce best practices and reduce the attack surface. On the other hand, fraudsters can misuse those same AI systems.

Reference:

1. https://www.researchgate.net/publication/330569376
2. www.geeksforseeks.org
3. https://blog.ipleaders.in
4. https://www.researchgate.net/publication/330569376
5. http://csrc.nist.gov
6. www.techtarget.com
7. www.crowdstrike.com
8. www.kasperskey.com
9. www.dameware.com
10. www.paaltonetworks.com

11. www.thesslstore.com
12. www.simplilearn.com link.springer.com
13. www.veracode.com
14. towardsdatascience.com
15. www.thesslstore.com

Dr B. MANJULA - ARTIFICAL INTELLIGENCE FOR SUSTAINABLE DEVELOPMENT:- CHALLENGES AND OPPORTUNITIES (2022)



ISBN
9 789395 422567

SHANLAX
PUBLICATIONS

www.shanlaxpublications.com
publisher@shanlaxpublications.com