iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** X **Month of publication:** October 2022

DOI: https://doi.org/10.22214/ijraset.2022.47155

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue X Oct 2022- Available at www.ijraset.com

Artificial Intelligence in the Field of Cyber Security

Ms. Jayabalaji K[1], Harini R[2], Vengadesh S[3]
[1]*Assistant Professor Department of Computer Science,* [2] *Student IV MSc Software Systems,* [3]*Student IV MSc Software Systems, Sri Krishna Arts and Science College*

Abstract: ***The cyber security industry's financial resources and human abilities to assess and battle every new type of cyber danger have been overwhelmed by the surge in cyber assaults. With the rise of the digital world, there is a rising quantity of personal and financial data that has to be secured against cyber-attacks. In reality, cyber assaults may devastate an organization's reputation or cause it to fail totally.***

This study investigates the use of artificial intelligence (AI) to improve cyber security. Artificial intelligence has advanced to the point that it has surpassed human capability in activities like data analytics. The analysis indicated that using AI to regulate cyber attacks has both benefits and drawbacks the benefits exceed the drawbacks. This study discovers that AI systems are likely to increase the safety of customers and enterprises in cyberspace due to the fast and efficient technology necessary to operate them[2].

Keywords: Artificial intelligence, cyber security, AI, Artificial, expert system

I. INTRODUCTION

As exponential growth of computer networks has led to a tremendous growth in number of cyberattacks. As attackers are continually looking for new ways to breach data, cyber or online attacks are becoming a greater threat to your sensitive digital data. In reality, they employ artificial intelligence and social engineering to circumvent established internet security protocols.

Cybersecurity can prevent any form of data from being harmed or stolen. Personal identifiable information, sensitive data, protected health information, industrial and governmental data, personal and intellectual property, and a variety of other items fall into this category.

Artificial intelligence (AI) is a critical aspect that employs automation to increase an organization's production and efficiency. AI has become one of the most important strategies for defending against cyberattacks as a result of digital transformation. Cyber AI can spot trends in data and enable security systems to learn from their mistakes.

Furthermore, enterprises may cut quick reaction times and improve security measures by utilizing AI and machine learning approaches[1].

II. AI AN OVERVIEW

All artificial intelligence computer systems are built on a knowledge base and an ability to infer, or draw conclusions based on logic and prior knowledge. A knowledge base is composed of a large number of discrete information items that reflect facts, concepts, theories, processes, and linkages that are all crucial to a particular activity or aspect of the universe.

To manipulate this data and reason, judge, draw conclusions, and select solutions to the issue at hand—such as determining if a string of credit-card transactions is fake or guiding an automated rover through a rocky Martian landscape programs are created. Pattern matching can still be algorithmic, which means the computer needs to be told what to look for and how to identify matches in its knowledge base. The computer searches its knowledge base for specific instances or patterns that fit the requirements of the challenge. Because of advancements in microchip technology, AI algorithms can now quickly scan huge volumes of data.

III. AI FOR CYBERSECURITY

In the hands of specialists, AI can detect and protect against these dangers automatically. It may be thought of as anti-virus protection for our PCs. Because malware changes too fast to be detected or analyzed manually, AI approaches can reduce the period between attack and discovery.

With automation to detect risks in every area and scale of business, AI and machine learning have become vital in the defensive process. For example, Google utilizes deep learning, a machine-learning technology that allows algorithms to make more autonomous modifications and self-regulation as they train and grow, in practically all of its services[1].

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue X Oct 2022- Available at www.ijraset.com

Fig 3.1 Ai for cybersecurity [7]

IV. EXPERT SYSTEM

An expert system is computer software that can handle complicated issues and make decisions in the same way as a human expert can. It accomplishes this by retrieving knowledge from its knowledge base depending on the user's queries, using reasoning and inference techniques.

The expert system is a type of AI, and the first ES was created in 1970, making it the first successful artificial intelligence technique. As an expert, it solves the most difficult problems by pulling knowledge from its knowledge base .An expert system's performance is determined on the knowledge stored in its knowledge base by the expert. The more knowledge that is stored in the KB, the better the system operates. When entering in the Google search box, one of the most typical examples of an ES is a recommendation of spelling problems.[3]

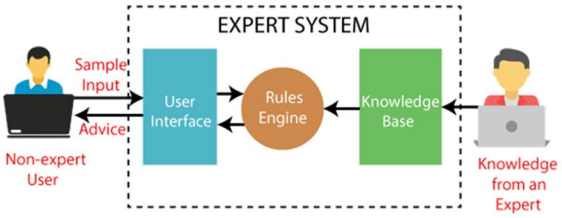


Fig 4.1 Expert system [4]

V. BENEFITS OF AI IN CYBERSECURITY

A. Unknown Threats

A human individual may not be able to recognize all of a company's dangers. Every year, hackers carry out hundreds of millions of assaults for a variety of reasons. Unknown threats may do a lot of harm to a network. Even worse is the damage they may do if you don't discover, identify, and prevent them. As attackers try new strategies, such as sophisticated social engineering and malware assaults, contemporary solutions are needed to protect against them. AI has shown to be one of the most successful technologies for spotting and preventing unanticipated threats from wrecking havoc on a company.

B. Better Vulnerability Management

Vulnerability management is essential to securing a company's network. As mentioned earlier, a median company deals with several threats daily. It must detect, establish and stop them to be safe. Analyzing and assessing the present security measures through AI analysis will facilitate in vulnerability management.AI helps you assess systems faster than cyber security personnel, thereby increasing your downside determination ability manifold. It identifies weak points in pc systems and business networks and helps businesses target necessary security tasks. That creates it potential to manage vulnerability and secure business systems in time.

C. Ai Authentication And Security

Most websites have a user account feature where one logs in to access services or buy products. Visitors are required to fill out sensitive information on some websites' contact forms. As a business, you must add an additional layer of protection because running such a site entails handling sensitive data and personal information. Your visitors' safety while using your network is guaranteed by the extra security layer. Every time a user tries to connect into their account, AI secures authentication. For identification, AI use a variety of techniques, including fingerprint scanners, CAPTCHAs, and facial recognition[6].

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue X Oct 2022- Available at www.ijraset.com

VI. APPLICATIONS OF AI IN CYBER SECURITY

A. Cognitive Security

Artificial intelligence and human intellect are combined in cognitive security. Cognitive computing (CC), a more advanced sort of artificial intelligence, makes use of a variety of AI techniques. It refers to technology and/or software that functions in a similar fashion to the human brain. In terms of goal, AI and CC are quite similar, yet they differ in their proclivity to connect organically with people. Artificial intelligence (AI) is a term used to describe technology that can do activities that would ordinarily need human intelligence. The goal of cognitive computing is to break beyond the limitations of traditional programmable (von Neumann) computers. Watson for cybersecurity, IBM's first cognitive system, exhibited its ability to answer challenging questions as well as the world's human champions in a Jeopardy exhibition match.

B. Parallel And Dynamic Monitoring:

The target systems' learning capacities necessitate some type of continuous monitoring during deployment. Monitoring is required to guarantee that any differences between a system's intended and actual behaviour are detected and addressed appropriately. To do so, AI system providers should maintain a clonesystem as a control system, which acts as a baseline against which the original system's behaviour is measured[3].

VII. AI-BASED APPROCHES IN CYBERSECURITY

A. Software Exploitation

Software has vulnerabilities, and some of them are exploitable, meaning that an attacker who is aware of the vulnerability can target the underlying software programme. Buffer overflow, integer overflow, SQL injection, cross-site scripting, and cross-site request forgery are all common software vulnerabilities. Some flaws have been detected and repaired. It would have been ideal if software developers had discovered and patched all vulnerabilities during the design and development phase, which is extremely difficult given the high expenses of software development and the need to get products to market quickly. As a result, detecting and repairing faults is done on a regular basis.“The Internet can be viewed as the most complex machine mankind has ever designed,” says Bruce Schneier. We don't even know how it works, let alone how to protect it". Going through code line by line to patch software defects is a tiresome operation, but computers can accomplish it if they are taught what the vulnerabilities look like. AI appears to have the capability to complete these jobs.

B. Malware Detection

Malware detection is a widely used method of identifying cyber attacks. Malevolent software includes viruses, worms, and Trojan horses. Because malware has such a huge impact on politics and the economy, it's vital to prevent and mitigate malware-related attacks. As a result, a number of researches on the use of AI techniques have been done. Below are some key research findings.To locate unknown malwares, the researchers in employed k-nearest neighbours and help vector gadget as ML classifiers. A deep studying structure turned into built in some other manner to become aware of smart malware. Mobile malware turned into the goal of a current malware detection look at. A deep convolution neural community turned into used to locate malware .The authors created a completely unique gadget studying approach, rotation forest, to locate malware .Another vicinity of look at turned into malware categorization the use of bio-stimulated computing. This technique turned into used to optimise parameters on the way to categorise them. As a result, detecting and repairing faults is finished on a ordinary basis."The net is probably regarded because the maximum complex gadget mankind has ever developed," says Bruce Schneier. We do not even recognize the way it works, not to mention a way to defend it. Going thru code line via way of means of line to patch software program defects is a tiresome operation, however computer systems can accomplish it if they may be taught what the vulnerabilities appearance like. AI seems to have the top hand phishing[5].

VIII. ATTACK AND SPAM DETECTION

A. Phishing Assault

A phishing assault attempts to souse borrow the identification of the user. Phishing assaults encompass brute-pressure attacks and dictionary assaults. Here are some enormous AI-primarily based totally strategies to handling this problem. The authors of defined a phishing detection device known as phishing e-mail detection device that used a changed neural community and reinforcement learning.

B. Spam Detection

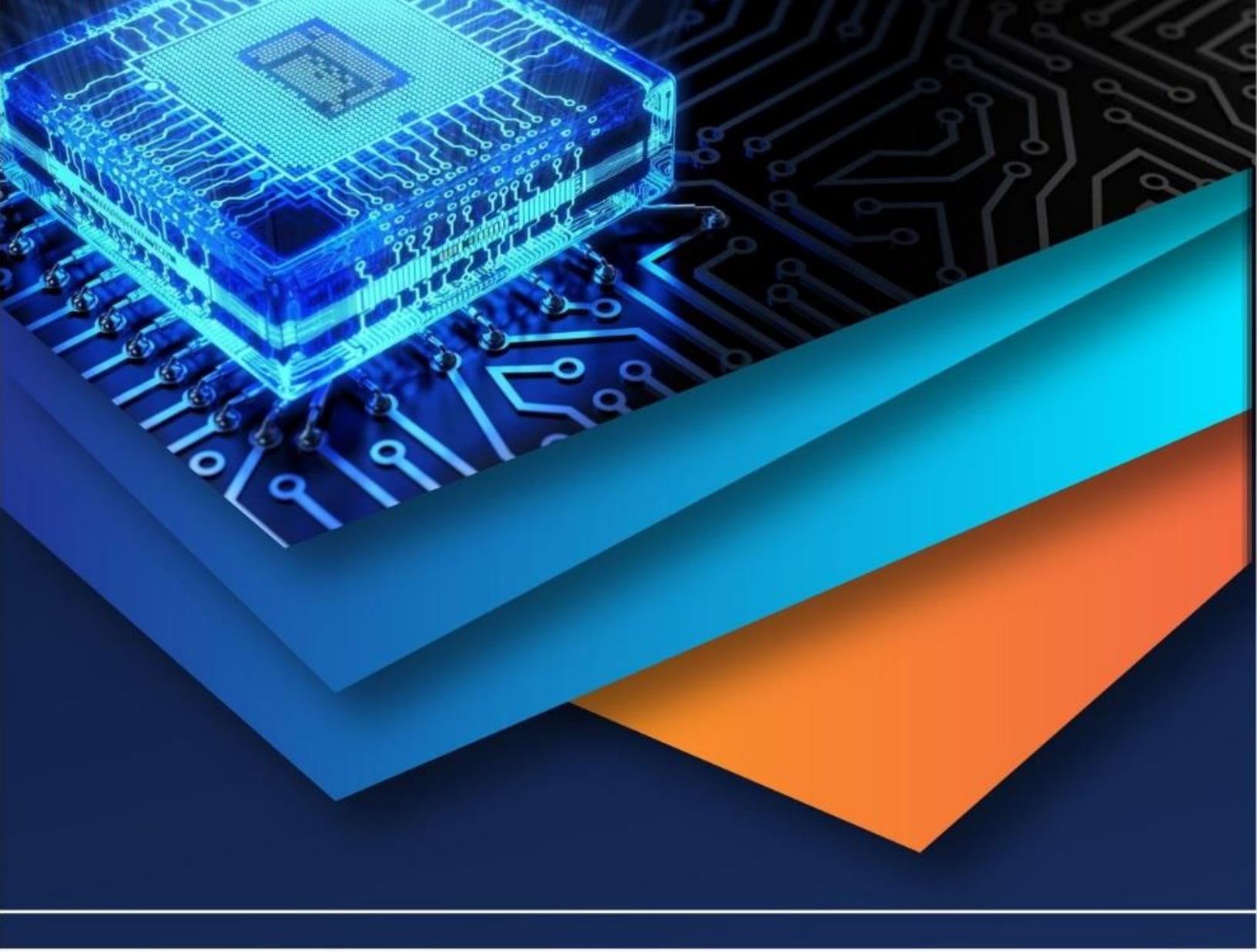
Uninvited mass e-mail is what this refers to. Spam emails may also encompass offensive information, posing a safety risk. Spam emails have lately been filtered the use of AI-primarily based totally algorithms. For example, Feng et al. confirmed one device. For junk mail e-mail filtering, this device included a help vector gadget with a naïve Bayes algorithm[5].

IX. CONCLUSION

The sophistication of assaults and the rapid expansion of cyber risks necessitate new, more resilient, adaptable, and scalable techniques. Malware detection and phishing and spam detection are the key aims of AI-based cybersecurity algorithms, according to current research. Various studies combined .Although AI's involvement in resolving cyberspace concerns is unavoidable, some difficulties with AI's trustworthiness, as well as AI-based threats and assaults, will be a source of worry in the cyber environment.

REFERENCES

[1] Shidawa Baba Atiku, Achi Unimke Aaron, Goteng Kuwunidi Job, Fatima Shittu, Ismail Zahraddeen Yakubu in Issn Volume 9, Issue 10, October 2020
[2] https://www.xenonstack.com/blog/tag/cyber-security
[3] S.Bhutada and P.Bhutada application of artificial intelligence in cyber security in IJERCSE,2018
[4] https://www.javatpoint.com/expert-systems-in-artificial-intelligence
[5] Katanosh Morovat and Brajendra Panda survey of AI in cybersecurity in CSCI 2020
[6] https://www.cm-alliance.com/cybersecurity-blog/8-benefits-of-using-ai-for-cybersecurity
[7] https://www.xenonstack.com/blog/tag/cyber-security



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY