A REVIEW OF CHALLENGES AND SOLUTION IN CYBER SECURITY USING ARTIFICIAL INTELLIGENCE

Kumar Siddamallappa U [1]

Assistant Professor, Department of Studies in Computer Science, Davangere University, Davangere, Karnataka, India

Abstract: -

Artificial intelligence (AI) is assisting under-resourced dedicated security analyst in staying ahead of cyber as cyber-attacks rise in volume and complexity. AI delivers quick insights to help you battle through the sound of hundreds of daily warnings, significantly lowering reaction times, by curating threat intelligence from millions of academic papers, blogs, and news items.

By eliminating manual analysis, proof collecting, and cyber threat correlation, AI helps the SOC be more successful, resulting in faster, better uniform, and correct responses. Some AI models can determine which sources of data should be used to gather various kind of evidence. They can also pick out useful information among the noise, recognize trends that have been seen in a variety of situations, and compare it to the most recent security data. In cyber security, artificial intelligence can create a chronology and threat chain for an event. All of this points to rapid reaction and repair.

Keywords: **"**Cyber Security Methods, Systems, Artificial Expert Intelligence, Visual nets."

1. INTRODUCTION:-

It is understandable because the only way to protect against clever cyber bats is to write smart code, and recent incidents have proven both malware and cyber-weapons are becoming increasingly sophisticated. Cyber mishaps are especially hazardous when net central warfare is used, and cyber security reforms are urgently needed.

Recent AI breakthroughs are game-changing, and they already outperform humans in fields such as image recognition, natural language processing, and analytics. Economic factors will drive the adoption of emerging Artificial intelligence that will have a good and negative influence on almost every aspect of business. and negatively. Artificial intelligence systems may be controlled, avoided, and mislead, posing serious security risks. For security tools, banking systems, and self-

driving cars, to name a few. As a result, Secure and robust techniques and best practices are required for applications such as monitoring tools, financial systems, and driverless cars. critical. As a result, it's critical to use secure and resilient approaches and best practices.

New security methods such as dynamic construction of protected perimeters, complete scenario awareness, and very machine-driven reaction to network threats will necessitate widespread use of AI methods and knowledge-based technologies. Why has intelligent code's importance in cyber operations grown so quickly? The following response may be found by looking closer at the cyber home. In terms of logical accuracy, decision theory, and risk evaluation, formal techniques to test AI and ML components, both individually and in concert, are urgently needed. New approaches are required to define what a device ought to do and how it should react to an assault. Quality that matches the criteria is tractable by each element in conventional systems. The installation and design of AI systems are difficult to analyses since they are so complicated. Research is required in architectural frameworks and analytical devices that help these parts to be verified, as part of a larger initiative to provide achievable standards, best practices, and resources, and procedures for reasoning about a system's behavior.

3. Challenges in Intelligent Cyber Security

When it comes to long-term research, research, and implementation of AI methods in Cyber Security, it's important to distinguish between short-term aims and long-term perspectives. There are a variety of AI approaches that are directly applicable to Cyber Security, and there are cyber security challenges that require more innovative approaches than are now in place.

We have just discussed these direct uses so far. Future prospects for the employment of entirely new data management ideas in situation management and selection will be encouraging. Within the determining software system, these concepts include introducing a uniform and hierarchical data design.

One does not have to believe in the danger of the Singularity; but, the rapid advancement of information technology will undoubtedly affect one's ability to incorporate substantially greater intelligence into software systems in the next years. Regardless of whether true universal intelligence is attainable or the Singularity arrives, having the ability to utilize greater AI in cyber security than the criminals is critical.

4. Specification and Verification of AI Systems

Accuracy isn't only a logical concept; noise and ambiguity necessitate limits for each component to prevent the system from malfunctioning. As it pertains to logical soundness, decision theory, and risk assessment, formal techniques to verify AI components, both individually and in concert, are urgently needed. New approaches are required to define what a machine should do and that it should react to an assault.

Quality that matches the criteria is tractable for each element in conventional systems. The installation and design of AI systems are difficult to analyses since they are so complicated. Research is required in architectural frameworks and analytical techniques that allow these features to be verified as part of a larger effort to develop fair standards, best practices, tools, and techniques for reasoning about a rational function.

An AI "building code" may be created through a new discipline and technology of AI architecture. A code like this might be based on theory and experience, record best practices, and include principles from different fields of computer science. The analysis of the source code would aid in a better understanding of AI concepts and advancement in the field. Performance, security, robustness, and fair must all be addressed throughout concept and verification. To fully understand performance tradeoffs and the operating conditions, further research is required, which may need the addition of a domain specialist to the team. Finally, an engineer is required to do.

5. Trustworthy AI Decision Making

Moreover, the techniques are nearly entirely focused on supervised learning at the moment, which is challenging to do without compromising system performance. AI systems which request assistance when they are unsure, a related field of study, can enhance trust in the final choice and expect the users to gather knowledge for future making decisions. AI efficiency is also domain-specific. When training set is not reflective of the particular environment, security risks occur. In contrast, if software architecture restrictions are not taken into account, excessively pessimistic vulnerability evaluations might emerge.

Among property AI settings, as well as when they become a part of the full-use ecosystem, more research is required on how inputs data is collected, protected, preserved, and assessed. An autonomous vehicle system is educated with pictures and circumstances gathered from real-world scenarios and is kept up to date as its surroundings change. Domain-specific vulnerabilities must be considered in vision, planning, supervised learning, information processing, and reasoning.

6. CONCLUSIONS

It is unavoidable to create intelligent cyber security methods in the current environment of rapidly expanding malware knowledge and classes of cyber-attacks. Expertise in Do's avoidance has proven that even with little resources, a protection against huge assaults may be overcome if clever methods are utilized. The study of artificial visual networks provides the AI results which are most broadly relevant in cyber security, according to a review of articles. Visual networks might continue to be used in cyber security.

In many sectors where neural networks are not the most suited technology, there is also a pressing need for the use of smart cyber security methods. Support, context awareness, and data management are the three areas in question. In this instance, professional management system is by far the most promising. Although it is unclear how quickly universal computing will advance, there is a risk that attackers will employ a replacement rate of computation as soon as it becomes available.

REFERENCES

[1] "U. Schade, M. R. Hieb. A Battle Management Language for Orders, Requests and Reports. In: 2007 Spring Simulatin Ineroperability Workshop. Norfolk, USA, 2006."

[2] "F. Barika, K. Hadjar, and N. El-Kadhi, "Artificial neural network for mobile IDS solution," in Security and Management, 2009."

[3] "P. Norvig, S. Russell. Artificial Intelligence: Modern Approach. Prentice Hall, 2000."

[4] "J. Kivimaa, A. Ojamaa, E. Tyugu. Pareto-Optimal Situation Analysis for Selection of Security Measures. Proc. MilCom, 2008. "

[5] "B. Iftikhar, A. S. Alghamdi, "Application of artificial neural network in detection of dos attacks," in SIN '09: Proceedings of the 2nd international conference on Security of information and networks. New York, NY, USA: ACM, 2009, pp. 229–234".

[6]" P. Salvador et al. Framework for Zombie Detection Using Neural Networks. In: Fourth International Conference on Internet Monitoring and Protection ICIMP-09, 2009."

[7] "J. Bai, Y. Wu, G. Wang, S. X. Yang, and W. Qiu, A novel intrusion detection model based on multi-layer self-organizing maps and principal component analysis, in Advances in Neural Networks. Lecture Notes in Computer Science. Springer, 2006."