A Review on Artificial Intelligence and Data mining in Cyber security

Rahul Jogendrapal Singh[1], Rahul Appaso Patil[2]

Student, Mechanical Engineering ,G .H .Raisoni College of Engineering, Nagpur, Maharashtra ,India

ABSTRACT

This review paper primarily focusses on artificial intelligence, the data mining and cyber security, the roles of artificial intelligence and data mining in cyber security. The role of artificial intelligence in cyber security, whereas the number attacks to the work space lead to heavy traffic, the areas which cannot be handled by human are handled by intelligent system. These help to prevent attacks and security cracks and also respond to the attacks. The role of data mining in cyber security is use to examine the data from various dimensions and approach searching the previously unknown hidden patterns classifying a grouping of the data and summarizing the identified relationships. Data mining of data and machine learning of data are important so that cyber data sets used in machine learning and data mining are described for cyber security is presented.

Keyword : - *Artificial Intelligence, Cyber security, Data Mining.*

---

1. INTRODUCTION

Computer were developed by humans for providing the better services to them. Currently Artificial intelligence and machine learning plays important role for them. There are number of techniques used in Artificial intelligence are search, knowledge representation, formal logics, neural networks, genetic algorithms.[5] Now a day's world is facing problems of intrusion of information. Cyber security is one of the major issues & commercial Information systems. The growing connectivity of computers through Internet. Increasing number of systems & the tapering growth of size of complexity of the systems have made cyber security a very big problem now days. Computers have now become an undetachable part of our systems. while there have been many benefits of the information revolution, the vulnerabilities have also increased proportionately.[2] In day to day cycle, increasing and progressing cyber security threat affects global businesses can be reduced by the integration of Artificial Intelligence into cyber security systems. With the help of AI, peak of abundant data could be carved down in fraction of time, which helps the enterprise to identify and recover from the security threat.[4] Data mining is a widely spreading technology, Data mining (DM), also called Knowledge-Discovery and Data Mining, in activities as diverse as using historical data to predict the chances of success. Looking for patterns in financial transactions to discover illegal activities.[3] The process searching large volumes of data for patterns using association rule and examine from various accepts automatically. There are different data mining approaches are Classification, Clustering etc. To gain the information or knowledge about network data.[6]

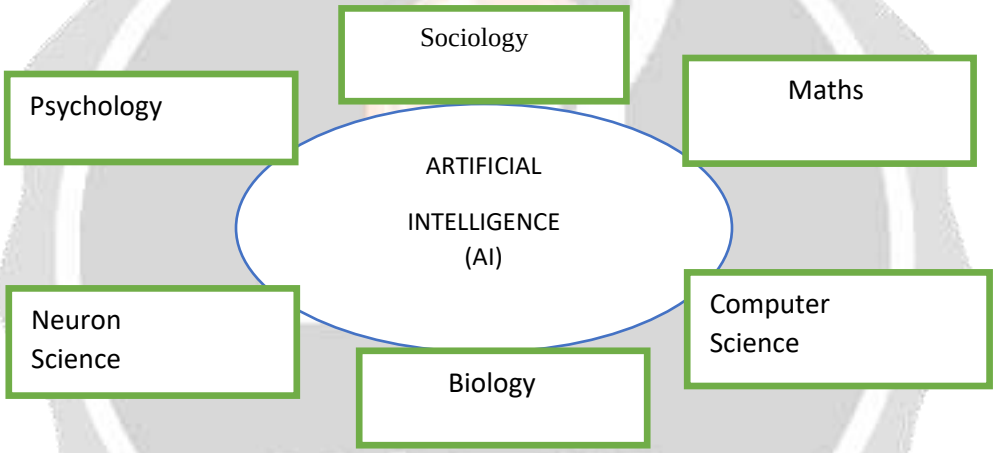
1.1 ARTIFICIAL INTELLIGENCE (AI)

According to the father of Artificial Intelligence, 'John McCarthy, it is "The science and engineering of making intelligent machine, especially intelligent programs".

Artificial Intelligence is a way of making a computer, a computer-controlled robot, or a software think intelligently, in the similar manner the intelligent humans think.

Artificial Intelligence is accomplished by studying how human brain thinks, and how human learn, decide, and work while trying to solve a problem, and then using the outcome of this study as a basis of developing intelligent software and system.

The purpose of AI is to make the expert system which exhibit intelligent behaviour, learn, demonstrate, explain, and advice its user. To implement Human Intelligence in machine – creating system that understand, think, learn, and behave like human.[5]



1.2 ROLE OF ARTIFICIAL INTELLIGENCE TECHNIQUES FOR CYBER SECURITY

Intelligence is the ability of system to calculate, reason, perceive relationships and analogies, learn from experience, store and retrieve information from memory, solve problems, understand complex ideas, use of natural language fluently, classify, generalise and adapt new situation.

The various Artificial intelligence (AI) techniques used for the cyber security are; Applications of Intelligent Agent, Neural Nets, Expert System, Learning, Future Issue Consideration. As we know that we are moving towards a future in which we will interact with machine which will be smarter than human beings. As the technologies are developing day by day likewise the threats and assault are also enhancing to fight against this assault we need to implement AI techniques in our security system. [4], [8]

1]Expert System: - Expert system is for security arranging in cyber defence. It helps in determination of safety efforts, and gives direction for ideal use of resources which are limited in quantity. Expert systems utilization in intrusion detection is already known. [8]

2]Intelligent agent: - Intelligent agents is utilized in resistance against Distributed Denial of Service (DDoS) assaults. In the wake of settling some lawful and furthermore business issues, it ought to be conceivable on a basic level to build up cyber-police which comprises of intelligent agents (portable). [8]

3] Neural nets: - Neural nets are famous in cyber defence because of its high speed, when installed in hardware or as a graphic processors component. Neural nets are used to carry out the detection and prevention of intrusion. [8]

4] Future Enhancement: - We can use AI in various ways for the benefit of cyber security. In future we may have most intelligent systems than these techniques. Even the attackers or intruders will also use the AI for attacks. Hence the expert system innovation will require advancement in future. [4]

2. DATA MINING AND CYBER SECURITY

Data mining is methodological approach by analysis of data. In data mining the analysis of data being done from various dimensions and perspectives, finding previously unknown hidden patterns, classifying and grouping the data and summarizing the identified relationships.

The Protection of computer systems from the theft or damage to their hardware, software or electronic data, as well as from disruption or misdirection of the service they provide is called as cyber security. cyber security can help prevent cyberattacks, data breaches and identity theft and can aid in risk management.[2]

2.1 ROLE OF DATA MINING IN CYBER SECURITY

Data mining it's a popular technological innovation, in which Analysing of data takes place through methodological approach. In data mining machine learning algorithm are commonly used in data mining data. For Example, in such cases speech recognition has issue as in other cases, then the algorithm based on machine learning results much better than other methods. A more technical explanation: Data Mining is the set of methodologies used in observing data from various dimensions and approaches and finding the unknown hidden patterns, classifying and grouping the data and explain the identified relationships. The useful knowledge that can help the data owners/users make informed choices and take smart actions for their own benefit. Data mining has many applications in security including in cyber security (e.g., virus detection) as well as in national security (e.g., surveillance) Data mining is also being applied to provide solutions such as intrusion detection and auditing. The conventional approach to securing computer systems against cyber threats is to design mechanisms such as firewalls, authentication tools, and virtual private networks that create a protective shield. Data mining techniques are being used to identify suspicious individuals and groups activities, and to discover which individuals and groups are capable of carrying out unauthorized activities in any reasons. [1][3][6] [10]

2.2 DATA MINING TECHNIQUES

1] Seeking of incomplete data: -As the name indicate the seeking of incomplete, hence if the data is incomplete, the result would be completely off-mark. Therefore, it is essential to have an intelligence to expel out incomplete if possible.

2] Dynamic dash board: - The technique of give the live insight and monitoring of data to the owner. This is the representation of data, on a computer of an organising person, which is fed with real time of data.

(a) Dynamic analysis (b) Text analysis (c)Efficient handling of Complex and Relational data

(d) Relevance and scalability of chosen data mining algorithms

2.3 TOOLS FOR DATA MINING

1. Rapid Miner (erstwhile YALE)

2. WEKA

3. R-Programming Tool

4. Python based Orange and NTLK

5. Knime

Based on results of data mining tools one can predict whether any unauthorized intrusions occurred or not. Data mining algorithms used for intonement detection are: -

1)Bayes classify -This encodes probabilistic relationship between variable but they required high computational efforts. Also, their results are much similar to that of threshold-based result.

2)K-nearest neighbour: - It is the simplest algorithm which can be used along with statistical schemes of intrusion detection.

3)Decision tree: - Predictive modelling technique and they puss's generalization accuracy. Because of their high performances they are used for real time intrusion detection.

4)Support vector machining: - These are novel technique some time it uses linear separating hyper plane for creating classifier and if problems not solved with linear separating hyper plane, then it uses 'kernel' feature. [6]

3. CONCLUSIONS

Cyber security in recent years largely depends upon the major reliable elements i.e. artificial intelligence and data mining tools. In future we may have various modern techniques which were gifted by advanced technology but in recent era these two elements shield the ocean of information and data ,up to a great extent ,from various threats of data extrusion.

4. REFERENCES

[1] "Data Mining for Computer Security Applications" (Lazarevic, A., et al.), Tutorial Proc. IEEE Data Mining Conference, 2011.

[2] Paper on cyber security analysis using policies and procedures by (ER. ASAD ULLAH QURESHI, ER. SARVESH RAI). Mathematical Sciences International Research Journal: Volume 4 Issue 1 (2015) ISSN 2278-8697

[3] Role of Data Mining in Cyber Security, (P. SANTHOSH RAJ, G. SILAMBARASAN), IJESC Paper, Volume 7 Issue No.7.

[4] Artificial Intelligence Techniques for Cyber Security (AROCKIA PANIMALAR.S, GIRI PAI.U, SALMAN KHAN.K), IRJET Paper Volume 5 Issue 3, March 2018.

[5] Research paper on AI, (Jaspreet Singh), International Journal of Scientific Research and Management (IJSRM) ||Volume||5||Issue||11||Pages||7411-7417||2017|| Website: www.ijsrm.in ISSN (e): 2321-3418

[6] Data Mining Technology for Efficient Network Security Management Ankit Naik [1], S.W. Ahmad [2] Student [1], Assistant Professor [2] International Journal of Computer Science Trends and Technology (IJCST) – Volume 3 Issue 3, May-June 2015

[7] A Survey on Supply Chain Cyber Security Shreya Sharma1 Janki Thakkar2 Jalpa Patel3 1,2UG Student 3Assistant Professor 1,2,3, IJIRST || National Conference on Latest Trends in Networking and Cyber Security || March 2017

[8] Applying Artificial Intelligence Techniques to Prevent Cyber Assaults [Amaan Anwar1 & Syed Imtiaz Hassan2] International Journal of Computational Intelligence Research ISSN 0973-1873 Volume 13, Number 5 (2017), pp. 883-889

[9] How Big Data Can Improve Cyber Security (Haydar Teymourlouei1, Lethia Jackson2) Int'l Conf. on Advances in Big Data Analytics | ABDA'17 |

[10] Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection (Jithin Mathew1, S. Ajikumar2 [1]) International Journal of Scientific Research in Computer Science, Engineering and Information Technology © 2017 IJSRCSEIT | Volume 2 | Issue 2 | ISSN: 2456-3307