Cyber Securence Affected by Big Data and Artificial Intelligence

Vidit Kumar[1], Dr. Deepak Chahal[2]

[1]MCA Student, Department of IT, Jagan Institute of Management Studies, New Delhi. India

[2]Professor, Department of IT, Jagan Institute of Management Studies, New Delhi India

***Abstract*- A throughout review must be done while considering the approach of Big Data and Artificial Intelligence for Cyber security by an organization. So its implementation must affect the organization in a positive way. Big Data is a new channel in the leading computer industry that is being monitors by both kinds of field members one having positive and another having negative perspective of this enhancing technology that is growing rapidly with the time span and bring new challenges in the cyber security environment. Enlistment of some aspects of Big Data and Artificial Intelligence in cyber security**

***Index terms*- Big Data, Cyber threats, Risk, Artificial Intelligence (AI), Security**

I.INTRODUCTION

The process of building applications has been a journey and it varies depending on one's application requirements and purpose [1]. Big Data can be defined as an enormous or a huge amount of data that cannot be stored and processed using long existing approach within a given lapse of time.

As in the present time Big Data Analytics is playing the major role in the industry not only in the field of computer science but as well as in every field which deals in analyzing their co related data for their growth and risk management.

And as the Risk management arrives the terminology security arrives, as in field of computer science is termed as cyber security, for which Artificial intelligence can be used.

As the expansion of data is being going on with its analysis. Several cyber security breaches (Cyber threats) also arrive. As a result big data also help in analyzing the persistent amount of data but also encounter several methods to overcome different types of risk involved.

But the Question arises that Is Big data analytics for cyber security is sufficient by the use of AI.

II. BIG DATA CYBER SECURITY DEFINITION

Big data can be referred as immense volume of data that cannot be sort out using customary approach within a given time frame. And analysis of these kind of data is Big data Analytics.

We usually use the byte terms such as gigabytes, terabytes or zettabytes or the biggest yottabytes or the data that has enormous size. But even a small amount of data can be referred as Big Data depending on the context it is being used.

Cyber Security is a sort of mechanism and protocols to protect us from all sorts of cybercrimes that are as follows:

1. Malware- It is a boundless term for diversity of cyber threats including Trojans, Viruses, Drive by Download, Mal advertisement and Bombs that generate malicious event for data manipulation, steal or destruction in computer system.
2. Phishing- Phishing are similar to spams but are more harmful than just a simple advertisement.
3. Password Attacks-In this a third party (non-trusted) tries to get access to your system by cracking the user password.
4. DDos (Distributed Denial of Services)-It focuses on disrupting the services of the network, the network can no longer be functional.
5. Rogue Software- These are basically malwares that pretends as original security software that will keep your system safe, but in real they are threats.
6. Man in the Middle- This type of attack can obtain information from end user and the entity

in communication by impersonation as a middle man.

Artificial Intelligence – Artificial Intelligence is the combination of two words, in which the word Intelligence means the ability to calculate complex algorithms, solve reasoning, perceive relationships and analogies, learn from experience, store retrieve, analyze and manipulate information of the surroundings [2]

Artificial Intelligence can be defined as process of making a machine to mimic human actions especially his intelligence and decision making capabilities.

Commonly known as AI, Artificial Intelligence is being developed to make more humanly like machines to reduce to problem generated by humans in a working environment.

III. POPULAR BIG DATA MECHANISMS BEING USED FOR CYBER SECURITY

AI is by no means is a pure solution to cyber security [3]. In this going on era many of the tools of Big Data are being used for cyber security to prevent against all possible cyber threats by proper designing and planning to maintain the Confidentiality, Integrity and Availability to get protected from:

1. Unauthorized modification.
2. Unauthorized detection.
3. Unauthorized Access.

Such tools are:

1. Threat detection and identification- By keeping a log of data (Big data) for all the kinds of threats with their behavior or effect on the computer system and networks a data scientist can easily detect and identify threats present in the data being processed and can take adequate action on it.
2. Perspicacious Risk Administration- By the help of Big Data threats can easily be interpreted by using its automation tools developed by using artificial intelligence by the help of machine learning to provide better risk Administration and management.
3. Forecasting models- The analysis of enormous amount of data for cyber threats process different results that can be used to develop methods or models or mechanism to protect the organization data from cyber threats

IV. DILEMMA OF USING BIG DATA FOR CYBER SECURITY

As the artificial intelligence created for cyber security by using machine learning where a human brain is behind its existence to mimic the action of human to process the data, there arrives a condition that if the brain behind this particular AI gets corrupted the Ai can also become corrupted and can work against the organization in which it is being used.

As all the existing technologies somehow have a loop hole that cannot be removed or is being improved to remove the potential threat loop hole, so there can be a chance of a loop hole in Big data and that is why we cannot be fully dependent on it.

As the time phase is being passing newer and newer ways are being introduced to develop threats and vulnerabilities that cannot be handled by using Big Data methodologies and enhances the risk of cyber threats and crimes.

According to a survey of the year 2018-19 6.4 billions of fake emails are sent worldwide daily, around 50% of local authorities are working with unsupported server software, thousands of people using easily crackable passwords and much more so how Big Data can defend tis much of risk factors.

More over if an organization uses Artificial Intelligence for cyber security there can be contradiction such as:

1. Inadequate amount of data being processed by the Artificial Intelligence producing insufficient result that can degrade the organization in terms of growth and generate losses.
2. Managerial bodies are unable to understand the result of processing of the co-related data.
3. If the organization is not data literate and does not implements data model in their working strategy.
4. Organization having less number of employees having the knowledge of data science.
5. Organizational body outsourcing the data causing data leak problem.
6. Issues of security in Big Data.

V. CONCLUSION

For implementing Big Data for cyber security the approach should be conducted in such a manner that covers all the dilemma mentioned above by taking following steps:

1. Development of robust and rigid algorithms that cannot be corrupted easily and providing the access to authenticated personalities.
2. Updation of Artificial Intelligence in real-time so it can resist new cyber threats being Introduced.
3. Enhancing and refining the decision making ability of mechanism being used.
4. Time series forecasting and analysis of the data must be done.
5. Isolation of source must be done to prevent data being theft.
6. Should not purely relay on single data-set analysis results.

REFERENCES

[1] Kharb L., "A Perspective View on Commercialization of Cognitive Computing," 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, 2018, pp. 829-832. doi: 10.1109/CONFLUENCE.2018.8442728

[2] Chahal D. et al. Artificially Intelligent Robotics-A survey, International Journal of Advance Engineering and Research Development Volume 4, Issue 10, October -2017.

[3] Chahal D, Kharb L. et al. A Futuristic Approach: Incorporating Artificial Intelligence with Cyber Security, International Journal of Research in Engineering, Science and Management Volume-1, Issue-12, December-2018.