International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-1, November 2019

Role of Artificial Intelligence in Cyber Security

Arab Mohammed Shamiulla

Abstract: ***Artificial Intelligence (AI) is a buzz word in the cyber world. It is still a developing science in multiple facets according to the challenges thrown by 21st century. Use of AI has become inseparable from human life. In this day and age one cannot imagine a world without AI as it has much significant impact on human life. The main objective of AI is to develop the technology based activities which represents the human knowledge in order to solve problems. Simply AI is study of how an individual think, work, learn and decide in any scenario of life, whether it may be related to problem solving or learning new things or thinking rationally or to arrive at a solution etc. AI is in every area of human life, naming a few it is into gaming, language processing, speech recognition, expert system, vision system, hand writing recognition, intelligence robots, financial transactions and what not, every activity of human life has become a subset of AI. In spite of numerous uses, AI can also used for destroying the human life, that is the reason human inference is required to monitor the AI activities. Cyber crimes has become quite common and become a daily news item. It is not just a problem faced in one country, it is across the world. Without strong security measures, AI is meaningless as it can be easily accessible by others. It has become a big threat for governments, banks, multinational companies through online attacks by hackers. Lot of individual and organizational data is exploited by hackers and it becomes a big threat to the cyber world. In this connection research in the area of AI and cyber security has gained more importance in the recent times and it is ever lasting also as it is a dynamic and sensitive issue linked to human life.***

Key Words: ***Artificial Intelligence, Cyber Security, Online attacks, Hackers, Human life***

I. INTRODUCTION

Cyber security is not just a problem of IT field. In fact its scope is very vast. Today everyone is familiar with internet. Even illiterate people are using smart phones and it has become indispensable from their day to day life. It is not an exaggerated statement that if someone says people are living on the internet today. Over a period of time internet has become the indispensable part of human life. Without proper knowledge and awareness, everyone is using AI in their daily walks of life. This is the golden opportunity for hackers to deceive the people easily. At times, hackers are also cheating the people who are having sound knowledge on AI. There for cyber security is a mutual problem across the globe. Hackers are becoming smarter day by day and they are more innovative in creating malicious software to exploit the vulnerable data of individuals, organizations and governments. Cyber attacks are increasing rapidly despite of enough security measures.

Revised Manuscript Received on November 30, 2019.
***** Correspondence Author
Dr. Arab Mohammed Shamiulla*, Associate Professor, School of Law, Presidency University, Bangalore, India.

It can be in the form of malicious software, phishing, password attacks, drive by downloads by using hyperlinks, virus attacks etc. As per the latest survey by the SSL Store, cyber crimes will generate 1.5 trillion profits in the year 2018. There is a high chance that the actual figures may be more.

Table-1.1: Various revenue sources of cybercrimes

Crime	Annual Revenues in $
Illegal Online Markets	$860000000000
Trade Secret, Intellectual Property Theft	$500000000000
Data Trading	$160000000000
Crime Ware / CaaS	$16000000000
Ransomeware	$10000000000
Total Cyber Crime Revenues	$1500000000000

*Source: Re-Hashed: 2018 Cybercrime Statistics

Cyber security holds a very significant part in the field of information technology. When someone comes across with a fraud, then cyber security comes into our mind. Protecting our own information on net has become a biggest challenge. The immediate word we get in our mind after hearing cyber security is cyber crimes. Governments are taking numerous security measures to prevent cyber crimes, in spite of that; cyber crime rate is increasing rapidly. In this paper an attempt is made to know the various challenges faced by cyber security and also the latest technologies which prevent cyber attacks.

Table-1.2: Revenue from Ransomeware statistics

Ransomeware	Year	Revenues in $
CryptoLocker	2013	$300000
CryptoWall	2014	$1800000 - $32000000
Locky	2015	$780000 - $1500000
Cerber	2016	$690000
WannaCry	2016	$55000 - $140000
Petya/NotPetya	2016	$10000

*Source: Re-Hashed: 2018 Cybercrime Statistics

The fact is over 50% of cyber crime revenues are from online markets. It is astonishing truth Ransomeware made $10000000000 with in a period of just three years i.e. from 2013-2016.

To avoid from all these cyber crimes/attacks, an organization must have sound cyber security measures. Hence, cyber security is the need of the hour. The emerging technologies like cloud computing, mobile computing, internet banking, electronic and mobile commerce also need cyber security.

It includes a set of techniques used to safeguard the integrity of networks, stored data, programs etc from damage, unauthorized usage and from attack by hackers.
The proper application of cyber security protect from data and information breach, theft of identity and many more cyber attacks by hackers. Therefore cyber security helps in protecting unauthorized access, modification and deletion of data.

II. REVIEW OF LITERATURE

Ganesan. R. (2010): In his study he cautioned about spam mails sent by hackers. He introduces a new word scareware which is fake mail detecting software.

It cautions about all sort of communications over internet and warns not to open mails from open sources.
Govardhan. S. (2010): In his paper, he emphasized more on dynamic challenges faced by cyber security. In this day and age, hacker's intentions are malicious and to achieve it they are thinking out of box which a great threat for cyber security. He explained this by taking a classic example of operation aurora.
Selvakani, Maheshwari and Karavanasundari (2010): This study reveals the importance of cyber laws to protect the interest of cyber victims. AI should help in designing a strong law which can use effectively to trace cyber crimes.
Shukla R and Upadyaya A. (2011): This paper focuses more on financial data vulnerability. Now a day's people are more dependent on electronic banking activities. 90% of total commercial transactions are done online. Majority of cyber crimes are in banking industry only. Therefore this field requires high security and best practices.
Karheek D. N., Kumar M. A., Kumar M. R. P. (2012): This paper throws an attention in cryptographic measures. The basic problem in cryptography is security. By introducing new measures like quantum channel, cyber attacks can be reduced.
Balamuralikrishna I. T., Raghavendrasai, Sukumar S. (2012): It focuses on online frauds by various sites. In order to reduce the frauds the two techniques i.e. image matching and web page matching mechanism are helpful.

III. PROBLEM STATEMENT

Internet usage has become an integral part of human life. Without using it, even a tiny work is not completing. On the other hand cyber crimes or attacks are also increasing in the same tempo and velocity. In this era of protecting information on net has become a Herculean task. Hence, one must know the strong security measures to protect their information safely. In this paper a detailed analysis is made on the necessity of cyber security measures and it significance in IT world.

IV. OBJECTIVES THE STUDY

The following objective are undertaken in this study

1. To know the various AI tools and its significance in cyber security.
2. To measure the impact of AI tools in identifying the different cyber attacks.

V. METHODOLOGY

Methodology specifies the boundaries of research within which it is conducted, sources and methods of collecting data and analysis of data. Research methodology should give answer to the following questions. They are (i) the various sources available to collect data, (ii) what are the tools or methods used to collect the data, (iii) what techniques should be used for analysis of collected data and (iv) what would be the ideal sample size?
To understand the role of artificial intelligence in cyber security and different technologies used to identify and prevent cyber attacks/crimes, data or reports related cyber security incidents are collected through secondary data. The following statistical tools are used to analyze the collected data.

1. Measures of central tendency (simple and weighed average)
2. Percentile analysis

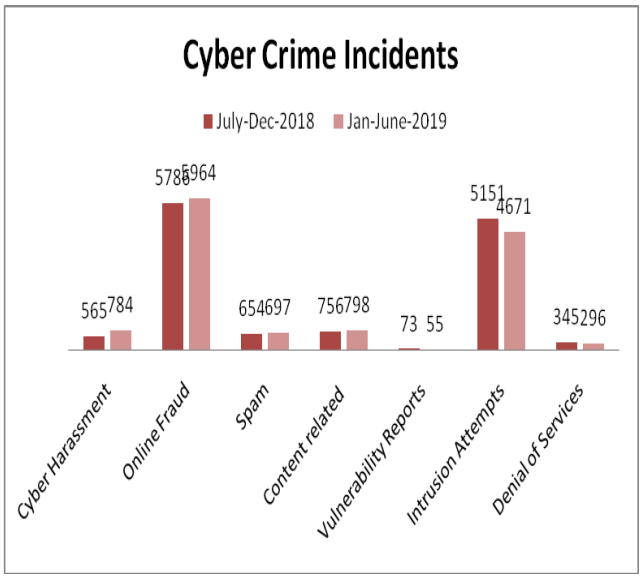
VI. DATA ANALYSIS

The data regarding various forms of cyber crimes is collected through secondary source. Simple average and percentile analysis are used to amylase the collected data.

Table-6.1: Cyber Crime Incidents Records

Cyber attacks / crimes Incidents	July-Dec-2018	Jan-June-2019	Increase /Decrease
Cyber Harassment	565	784	+219
Online Fraud	5786	5964	+178
Spam	654	697	+43
Content related	756	798	+42
Vulnerability Reports	73	55	-18
Intrusion Attempts	5151	4671	-480
Denial of Services	345	296	-49

*Source: Reports from National Crime Record Bureau-2019



Interpretation: From the above table it is clear that cyber harassment (+219), online fraud (+178) and spam (+43) and contend related attacks (+42) are increasing whereas intrusion attempts (-18), denial of services (-49), vulnerability reports attacks (-480) are decreasing.
Every organization pays high attention towards securing their data. For that they purchase different types of security software. It also leads to major business in cyber security area.

Table-6.2: Cyber crime as a service platform statistics

Cyber crime Product/Service	Price in $
SMS Spoofing	$20
Custom Spyware	$200
Hacker for Hire	$200
Malware Exploit kit	$200 -$700
Black hole Exploit kit	$700 -$1500
Zero day Exploit kit	$30000
Zero day IOS Exploit kit	$250000

*Source: Re-Hashed: 2018 Cybercrime Statistics

Interpretation: Providing security measures to prevent cyber attacks has also emerged as a huge profit business. People, organizations and governments are ready to pay more in order to secure their personal, financial and other official data.

VII. CONCLUSION

Today, people are living in cyber world where total data or information is maintained in digital/online form. The information may be related to personal life, financial transactions, intellectual property or any other official information which is important in nature. Even lot of information has been posted on social networking sites without knowing the safety measures. This is the fruit for cyber criminals as the information is in open access. Cyber security is not only a problem related to a person. It is even for an organization and for a government also. Not necessary that each time one can protect data or information on social networking sites but also the information related to bank transactions must have enough security measures. There are several techniques available to protect information on net naming a few are password security, authentication of data, malware scanners, firewalls, antivirus software etc. By implementing proper cyber ethics, majority of cyber attacks can be prevented. In a nut shell, computer security is a very broad area which is becoming significantly important as the world itself turning into digital mode with networks being used to carry out vital transactions. Cyber crimes or attacks are also continuing to diverge down various paths time to time. There is no perfect solution or universal remedy for cyber crimes/attacks as they are unprecedented in nature, but latest tools are used on par to minimize them in order to have a safe and secure future in cyber world.

REFERENCES

1. R. Hill, "Dealing with cyber security threats: International cooperation, ITU, and WCIT", 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace, pp. 119-134, 2015
2. S. Singh and S. Silakari, "A Survey of Cyber Attack Detection Systems", IJCSNS International Journal of Computer Science and Network Security, vol. 9, no. 5, 2009
3. J. Nogueira, "Mobile Intelligent Agents to Fight Cyber Intrusions", The International Journal of FORENSIC COMPUTER SCIENCE, vol. 1, pp. 28-32, 2006
4. S. Adebukola, Onashoga, Akinwale O. Bamidele and A. Taofik, "A Simulated Multiagent-Based Architecture for Intrusion Detection System", (IJARAI) International Journal of Advanced Research in Artificial Intelligence, vol. 2, no. 4, 2013
5. S. Dilek, H. Çakır and M. Aydın,"APPLICATIONS OF ARTIFICIAL INTELLIGENCE TECHNIQUES TO COMBATING CYBER CRIMES: A REVIEW", International Journal of Artificial Intelligence & Applications (IJAIA), vol. 6, no. 1, 2015
6. J.Raiyn, "A survey of Cyber Attack Detection Strategies", International Journal of Security and Its Applications, vol. 8, no. 1, pp. 247-256, 2014
7. Cerli and D. Ramamoorthy, "Intrusion Detection System by Combining Fuzzy Logic with Genetic Algorithm", Global Journal of Pure and Applied Mathematics (GJPAM), vol. 11, no. 1, 2015
8. O. Oriola, A. Adeyemo and A. Robert, "Distributed Intrusion Detection System Using P2P Agent Mining Scheme", African Journal of Computing & ICT, vol. 5, no. 2, 2012
9. S. Simmons, D. Edwards, N. Wilde, J. Just and M. Satyanarayana, "Preventing Unauthorized Islanding: Cyber-Threat Analysis", 2006 IEEE/SMC International Conference on System of Systems Engineering, pp. 5, 24-26
10. Ionita and L. Ionita, "An agent-based approach for building an intrusion detection system",RoEduNet International Conference 12th Edition: Networking in Education and Research, pp. 1-6, 26-28, 2013

AUTHORS PROFILE

Dr. Arab Mohammed Shamiulla, Associate Professor School of Law, Presidency University, Bangalore, India Email ID: arabmohammedshamiulla@gmail.com
Contact Number: 7702277901