Applications of Artificial Intelligence in Cyber Security

Uday Zorawar Singh

August 16, 2020

Applications of Artificial Intelligence in Cyber Security

Uday Zorawar Singh
COM8701 Fundamentals of Computing
Flinders University, South Australia

Sing0608@flinders.edu.au

Abstract

As Information Technology (IT) has advanced over the past few years, criminals have used cyberspace to commit cybercrimes. As new vulnerabilities are being discovered every single day, the speed of processing that data to tackle criminals or defend cyberspace can no longer handle by humans without the use of automation in some considerable tasks. Artificial Intelligence is an important area of science that can be used to solve large and complex problems by learning from what already has happened. This power of AI can be used to make a software or framework capable of advancing itself to make cyberspace secure.

Keywords: Artificial Intelligence, Cyber Security, Machine Learning, Intrusion detection system, Computer Security, Network Security.

1 Introduction

Cyber-attacks are growing at an alarming rate with more complexities and this problem is wider than the technical gap. Our world is strengthened by networked technologies from daily need of internet banking to national or governmental level of needs. Thus, keeping all data safe is a crucial thing. Although cyber security aids in minimising that risk of losing data, but with the exponential growth in the cyber-crimes, keeping security up-to-date and more complex to break in is becoming a hard task day-by-day. Just human intervention is not enough to tackle those issues at proper time and with appropriate response. Some attacks involve computer viruses and worms, and therefore, there should be an intelligent automated system that can detect, identify and response accordingly, eliminating the need of humans to some point and save time which can be used in some other tasks. AI offers many nature-inspired computational techniques such as Fuzzy Logic, Evolutionary Computation, Neural Networks, Intelligent Agent Systems, Cellular Automata which allows to build a robust and efficient decision support modules to provide cross linking aid to many cyber security applications (Dasgupta, 2006).

The aim of this paper is to identify some of AI applications in cyber security developed so far and to represent how those techniques are useful in order to detect and prevent against crimes.

2 Methodology

To study the relevant articles Google Scholar and findit@flinders both are used simultaneously. Google scholar is great for search, but some pdfs of the papers are restricted to subscribed users only, so in that case, findit@flinders is a great tool.

I try to search all the possible literature reviews related to the title. Among all, completeness of literature reviews is determined using different selected keywords. The following keywords are searched with different combinations to find some relevant papers:

“ Artificial Intelligence, Machine Learning, Artificial Neural Network, Intelligent Agent Systems, Multi-Agent Systems, Supervised ML, Unsupervised ML, Cyber Security, Network Security, IT security, Cyber Attack, Cybercrimes, Cyber threats, Neural Net, Artificial Immune System, Fuzzy Logic, Intrusion Detection System, IDPS, IDP, IPS, Intelligent Automation, Penetration Testing”.

I then go through all the possible literatures I could for few days and also while writing my own paper. Some literatures are published recently and most of them are based upon some previous work. So, I decide to select some new published papers for the general and latest information, and some dated 5 years ago or so to find remaining or incomplete paper. So far I found 2 incomplete or those which had some limitations to be addressed, one of which was completed 6 years later. Some papers are cross referenced.

3 What is the need of Cyber Security?

IT is so widespread that every person in this world is using it in one way or another. Where it has brought convenience to everyone's life, it has put a person at a greater risk of being affected by cyber-crimes. As people communicate, work, shop and do most of daily tasks over internet, the amount of digital data stored is increasing exponentially which potentially open the doors to try and attack different things to gain unauthorised access. As IT is a global phenomenon, it has make it more difficult to trace down and capture cyber criminals present in some other part of the world (Poonia et al., 2011).

Cyber-crime is a computer-based crime which involves a computer and a connected network. And, that computer can be used to get an unauthorised access to that network or in some cases, other networks that a computer might be connected to (Kruse II and Heiser, 2001). That unauthorised access can be used to threat a single person's or even, the whole nation's security (Morgan, 2016).

The potential reason in the increment of cyber criminals is the lack of professional people which possibly includes the time spent in gaining required knowledge and most importantly, a suitable degree compare to a person who can even start by reading some blogs or watching videos on internet. It is estimated that by 2021, there would be around 3.5 million positions available in Cyber security area (Morgan, 2017). Meanwhile, automated systems can somewhat overcome this absence of trained people. For example, many recent AI algorithms use Machine Learning to detect, identify and isolate malware.

4 Artificial Intelligence

The term "Artificial Intelligence" was coined by John McCarthy in a research project at Dartmouth College in 1956. AI can be defined as a field of science which aims to develop intelligent machines capable of solving complex problems and make right choices based upon the large amount of data. An intelligent system should have some capabilities to solve a problem by dividing that into sub-problems. These capabilities involve reasoning, knowledge representation, planning, learning, natural language processing, motion and manipulation, creativity, and social intelligence to name a few (Luger, 2005).

As mentioned earlier AI provides "nature-inspired" techniques which means that there are chances of AI to be able to work as some biological systems. For example, Artificial Immune Systems (AISs) are computational models which mimic biological immune system capable of changing its environment and dynamical learning. AISs are developed to mimic natural immune systems in AI applications particularly for intrusion detection systems (IDSs) (Saurabh and Verma, 2016).

The main concern for the Network Security is the continuous change of malware appearances. Sometimes old systems are not adequate enough to detect and identify the behaviour of new malware as there are no rules or patterns related to that particular vulnerability to be matched to (Veiga, 2018). Zero-day attacks are best examples of this type of issue. A zero-day attack is when an attacker uses an already exploited vulnerability which has not yet patched or known to vendor. And, this can be sold in black market.

The traditional systems try to stop the malware before their execution but when they failed in doing so, there is nothing left to get an idea of what has happened. Whereas, in case of Machine Learning, a subfield of AI, algorithms identify malware strike in real time and with the help of AI decision making process, tries to isolate the infected part or whole network segments in few milliseconds.

A well-designed AI system is able to go through several years of logs to analyse data and can form a basic guideline as of user experience, learn various attack skills which can be used to tackle those issues even faster than an expert. This, undoubtedly, saves much of manual power, money, and time.

5 Intrusion Detection System (IDSs)

Intrusion detection system or intrusion detection and prevention system (IDPS) is a software or hardware device which is placed inside the network (Figure 1). IDPS can detect intrusions and respond accordingly to prevent them. An intrusion is defined as an attempt to overlap security mechanisms in a network or system. IDPS can be classified into two categories: network intrusion detection systems (NIDS) and host-based intrusion detection system (HIDS).

In order to provide sufficient security against cyber-attacks, an IDPS should possess certain characteristics (Patel et al., 2011):

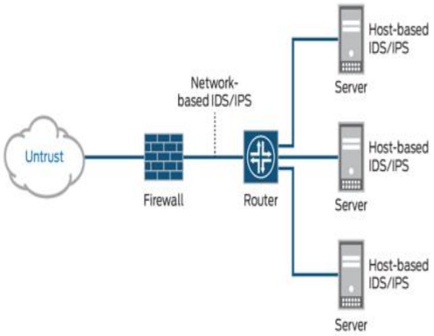

Figure 1: A Typical IDS/IPS model (Networks)

- Real-time intrusion detection,
- Human need should be minimised, and continuity of operations should be ensured,
- Able to recover from serious system crashes,
- False positive alarms must be minimised,
- Adaptable to system changes,
- Able to self-monitor and detect attacker's attempts to manipulate system.

6 Applications of AI to tackle Cyber threats

There are many methods for securing the data over networks such as anti-virus software, firewall, encryption, etc and many vulnerabilities in them are being discovered every day. And, available academic resources represent many AI techniques which are already available and being applied. For example, Artificial Neural Networks (ANN) is being used in Intrusion Detection and Prevention, Denial of Service detection, malware classification, spam detection and worm detection to name a few. Some AI techniques such as AISs, ANN and Data Mining are also being applied in the new-generation antiviruses (Wang et al., 2008). This section will outline related work and present some existing AI techniques.

6.1 Artificial Neural Network Applications

ANN is a computational technique inspired by biological neural networks which is used in system identification and control, pattern recognition, sequence recognition, data mining, machine translation etc.

Shenfield et al. (2018) proposed a neural network-based architecture which is a non-signature-based mechanism to detect Shellcode, an often used payload in system penetration tool which offers enhanced access and further leverage to an attacker. This approach was confirmed using 10-fold cross validation by achieving an average accuracy of 98% with less than 2% of false alarms. The limitation of this approach is that it is an offline approach yet and the work is being done in this field to integrate this approach with online network intrusion detection systems to test with real-time data.

Linda et al. (2009) presented the IDS-NNM – Intrusion Detection System using Neural Network Modelling, to demonstrate the correctness of the window based feature extraction mechanism which analyses the data in real-time, construct training dataset to generate random intrusion vectors and using two neural network learning techniques; the Error-Back Propagation and Levenberg-Marquardt, for normal behaviour model. The results achieved a well and good detection rate without giving any false positives alarms on previously unseen testing data.

Ahmad et al. (2009) presented a neural network approach to detect DOS attacks which used a supervised neural network called RPROP with a focus to increase attach detection and minimise false alarms. In this approach, normal traffic is separated from abnormal traffic in a manner of denial of services and multi-layered perceptron architecture and resilient backpropagation is used for testing against standard dataset. The results demonstrated that this approach was more accurate and precise compare to other methods.

Chen (2008) proposed NeuroNet, a neural network system and distributed security system plays a similar role as of the nervous system in human body and has the capability to monitor and detect traffic abnormalities and fluctuations in a core network, and triggers countermeasures. Its effectiveness was verified against low-rate TCP-targeted distributed Denial of Service attacks which is a hard to detect infrastructure-oriented attack. The first challenge of this architecture is to identify the metrics, parameters, and data format to monitor the traffic.

6.2 Intelligent Agent Applications

Intelligent agent is self-sufficient computer-generated force directed towards accomplishing its goals (i.e. an agent) upon an environment using sensors or actuators (i.e. intelligent). Intelligent agents are able to communicate with each other in order to share data and cooperate with each other to decide and execute appropriate responses even to unforeseen events. Their mobility and ability to collaborate and adapt to conditions they are deployed in, make them suitable to tackle cyber threats.

Gou et al. (2006) presented MWDCM, a Multi-agent system for Worm Detection and Containment in Metropolitan area networks as a first-class reaction mechanism to automatic containment strategies to halt the propagation of worms and protect Metropolitan Area Networks (MAN) against worm scan which can cause router crashes by wasting majority of network bandwidth in worm scanning. To detect unknown worms, worm detection agents use two stage-based decision processing which includes the study of access made in the whole network and dynamical changes in its the working parameters. Once a worm is detected, the system confines that into a macro or micro-cell of the MAN and ensures that the host continues to work without disruption. Although the system is very effective for avoiding fast scanning worms, but it is insignificant against other types of worms such as topological and flash worms.

Edwards et al. (2007) proposed a prototype MLSM, a Multi-Layered Security Model which can provide protection from entering an invalid input which could be used to attack the system. This model is also able to detect and recover from unseen attack techniques. This work was later validated by the author himself (Manickam et al., 2013) and the proposed methodology of the prototype was capable of detecting attacks on power grid. Not only that, as the mutated agents are regenerated, the system was able to continuously monitor and isolate the generator even under continuous attack.

7 Advantages of discussed AI techniques

Some advantages of some of AI techniques are discussed in Table 1 (Anwar and Hassan, 2017):

Table 1: AI techniques and their usage

AI Techniques	Usage
Applications of ANN	IDPS, High speed of operation, DoS Detection, Forensic Investigation.
Applications of Intelligent Agents	Agent communication language, Defence against DoS, Reactive, Mobility.

8 Conclusion

The fast-emerging IT field has so many positive impacts on everyone's life by providing conveniences in daily tasks. On its negative side, it has given opportunities for cyber threats which are becoming stronger and hard to combat with every passing day. New type of malwares, zero-day vulnerabilities and during these COVID-19 time, where most of the employees are working from home, dependency on third-party software such as ZOOM has increased for office work which has opened many opportunities to attempt and target every possible or vulnerable person connected to an organisation.

AI techniques-based applications are already being used to aid humans in tackling cyber threats and those techniques also provide flexibility and capabilities to IDPS software such as McAfee, CISCO NGIPS to make real-time decisions and support cyber defence.

This paper has discussed some already available AI techniques and how they are being applied to make cyberspace more secure and advance.

Acknowledgment

The author would like to thank the PC members of the conference FoCI 2020 for their valuable reviews in order to make some additional changes.

References

AHMAD, I., ABDULLAH, A. B. & ALGHAMDI, A. S. Application of artificial neural network in detection of DOS attacks. Proceedings of the 2nd international conference on Security of information and networks, 2009. 229-234.

ANWAR, A. & HASSAN, S. I. 2017. Applying Artificial Intelligence Techniques to Prevent Cyber Assaults. *International Journal of Computational Intelligence Research,* 13**,** 883-889.

CHEN, Y. NeuroNet: Towards an Intelligent Internet Infrastructure. 2008 5th IEEE Consumer Communications and Networking Conference, 2008. IEEE, 543-547.

DASGUPTA, D. Computational intelligence in cyber security. 2006 IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety, 2006. IEEE, 2-3.

EDWARDS, D., SIMMONS, S. & WILDE, N. Prevention, detection and recovery from cyber-attacks using a multilevel agent architecture. 2007 IEEE International Conference on System of Systems Engineering, 2007. IEEE, 1-6.

GOU, X., JIN, W. & ZHAO, D. 2006. Multi-agent system for worm detection and containment in metropolitan area networks. *Journal of Electronics (China),* 23**,** 259-265.

KRUSE II, W. G. & HEISER, J. G. 2001. *Computer forensics: incident response essentials*, Pearson Education.

LINDA, O., VOLLMER, T. & MANIC, M. Neural network based intrusion detection system for critical infrastructures. 2009 international joint conference on neural networks, 2009. IEEE, 1827-1834.

LUGER, G. F. 2005. *Artificial intelligence: structures and strategies for complex problem solving*, Pearson education.

MANICKAM, A., KAMALASADAN, S., EDWARDS, D. & SIMMONS, S. 2013. A novel self-evolving intelligent multiagent framework for power system control and protection. *IEEE Systems Journal,* 8**,** 1086-1095.

MORGAN, S. 2016. Cyber crime costs projected to reach $2 trillion by 2019. *Forbes. Retrieved September,* 22.

MORGAN, S. 2017. Cybersecurity labor crunch to hit 3.5 million unfilled jobs by 2021. *Cybersecurity Business Report*.

NETWORKS, J. *What is IDS and IPS?* [Online]. Available: https://www.juniper.net/us/en/products-services/what-is/ids-ips/ [Accessed April 23 2020].

PATEL, A., QASSIM, Q., SHUKOR, Z., NOGUEIRA, J., JÚNIOR, J., WILLS, C. & FEDERAL, P. Autonomic agent-based self-managed intrusion detection and prevention system. Proceedings of the South African Information Security Multi-Conference (SAISMC 2010), 2011. 223-234.

POONIA, A. S., BHARDWAJ, A. & DANGAYACH, G. Cyber Crime: Practices and Policies for Its Prevention.

The First International Conference on Interdisciplinary Research and Development, Special No. of the International Journal of the Computer, the Internet and Management, 2011.

SAURABH, P. & VERMA, B. 2016. An efficient proactive artificial immune system based anomaly detection and prevention system. *Expert Systems with Applications,* 60**,** 311-320.

SHENFIELD, A., DAY, D. & AYESH, A. 2018. Intelligent intrusion detection systems using artificial neural networks. *ICT Express,* 4**,** 95-99.

VEIGA, A. P. 2018. Applications of artificial intelligence to network security. *arXiv preprint arXiv:1803.09992*.

WANG, X.-B., YANG, G.-Y., LI, Y.-C. & LIU, D. Review on the application of artificial intelligence in antivirus detection system i. 2008 IEEE Conference on Cybernetics and Intelligent Systems, 2008. IEEE, 506-509.