International Journal of Management, IT & Engineering
Vol. 8 Issue 9, September 2018,
ISSN: 2249-0558
Impact Factor: 7.119Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com

Trends and developments in Artificial Neural Networks for Cyber Security during spread of H1N1 swine flu.

Aditi Gupta
Astt Prof Dept of Computer Sc
DAV College for boys, Hathi Gate , Amritsar

Abstract

The spread of H1N1 swine fluhas affected all sectors across the globe. It is not only a health emergency but has also affected the work culture in various organisations. It made many employees work from their home environment while using their personal computers and laptops where they use their own antivirus software, firewalls and web routers and hence getting more exposed to hacker attacks and viruses. It has completely changed the way cyber security tools function and generated new challenges. Protection of digital assets and Intellectual property has become more difficult for organisations. According to many recent studies, hackingfrom an external source is the basic cause of data theft in most corporate units. Major technologies like Artificial Intelligence, block chain, Radio frequency identification and Intrusion Detection and prevention Systems (IDS/IPS) are employed by companies these days for their network security. The major objective of this study is to survey and comprehensively compare various technologies and to investigate the problems, merits and shortcomings of the methods proposed.

1.Introduction

In recent times most of the business activities at various levels are carried out in cyberspace. However along with these the threat of Cyber-attacks had also increased manifold. Modern era is the era of electronic and digital technology. While the technology has made many things easier but it is not free from challenges. One such challenging threat faced by all in this sector are Cyber-attacks. These attacks are aimed at harming the finances of the companies. It can create a lot of damage to the company in the form of data distribution disruptions and knowledge breaks etc.

Presently the whole world is functioning under the threat of mutations in H1N1 swine flu. The danger of getting infected is forcing people to work from home where the Cyber security mechanism is the weakest. Various organisations are using different solutions to prevent these damages.

Technicians are working day in and out to get probable solutions. They have given various methods some of which are already operational while other are still being analysed and reviewed at different levels. As we already know that almost all the activities of the world are connected via worldwide web. The databases created by the companies now are not in the manual form but in the digital form. The corporate, banks and government are getting more and more dependent on their hardware and software mechanism and networking methods. It is therefore understood that if we fail to protect our data from these Cyber-attacks, things like customer details, sales, profitability and even things like national security will be in danger. The major problem is that it is a never ending process with the hackers developing new technologies to enter into a system and steal important data.

Some important sectors of the economy including the health sector, the power sector and even military establishments have been the victim of such Cyber-assaults in the recent past. We have also seen an alarming increase in ransomware attacks on small enterprises also.

Since the technology is created by Man, the solution to this problem will have to be developed by the Man himself.There cannot be any security mechanism which could be considered as fully secure. There is therefore a need to consistently develop and use newer technologies to counter the problem of Cyber- attacks.

1.1 Cyber security Technologies

There are many technologies used by various infrastructures these days. These technologies are successful in their own right and therefore widespread and trustworthy as well. However it would be wrong to say that they are hundred percent secure.

1.1.1 Artificial Intelligence & Deep Learning

Quite like the two factor authentication, AI is getting importance these days as an effective tool to counter malware attacks. It considers at least two or three parameters to have a confirmation of the identity of the user. It is further armoured with an additional security requirement which is related to identity verification. Any file entering into the system is checked on certain pre-identified parameters and the necessary permissions are sought and this is where AI is made to work for the security of the system. In order to make an analysis of the data related to various transactions and log entries, deep learning is also used. For the detection of various kinds of threats, communications (real time based) are also used.

1.1.2 Behavioural Analytics

It is an effective method which makes use of the data mining technology and popularly used in the advertising sector. Social media has taken the world like a storm and the advertisers have also found a way to popularise their products with the potential customers. Online advertising is becoming more popular as it targets the customers taking into account their tastes and preferences. Therefore technicians are researching possibilities in behavioural analytics to counter the threat of malware attacks.

1.1.2 Embedded Hardware Authentication

Earlier the protection of a system was done through using PIN’s and various types of passwords. At one time it was thought that if the password is strong, it will protect the system’s Hardware. But now we know that even this does not guarantee us the security of the system. Hence these days an important technology is emerging which is called the Embedded authenticator. In this technology some very effective and strong authentication chips are put inside the hardware and they are created in such a way that they can verify the identity of the user.

1.1.3 BlockchainOne of the most recent technologies which is becoming increasingly popular is the Blockchain technology. It is a two way technology which works to establish the identity of both the parties involved. In this technology verification is required at every stage of data addition. Since verification is done at every step it makes it very very difficult for a hacker to execute any kind of breach in the security mechanism. Many infrastructures are laying their trust these days on the blockchain technology. Infact a Combination of AI, deep learning and blockchain is proofing quite effective in preventing Cyber-attacks.

1.1.5 RFID- Radio Frequency Identification Device

Another emerging technology which used radio sound waves in order to identify the data composition and nature is the RFID technology. They make use of a RFID reader to read the data which is stored on a device in a coded form and convert it into another form for the purpose of protection. Therefore even if the hacker gets an access to the data he cannot use it as it is already encoded.

1.1.6 Network Traffic Analysis

The network traffic Analysis is also an effective tool for understanding the nature of Cyber-attacks and can help in this relation by classifying and identifying malicious activities.

1.1.7 Intrusion Detection and Prevention Systems (IDS/IPS)

In order to prevent any intruder entering into the system IDS/IPS system was developed. It initially worked because the common type of Cyber-attacks could be easily detected by this system and an alert message could be transmitted to the users. Problems like data sharing and data leaks sere easily defended by the use of IDS/IPS. The use of ML algorithms was made to perform these tasks.

The system however in many cases proved too much vigilant. It generated frequent unrequired alarms and caused unnecessary burden on the data security management personnel.

It is however suggested that a combination of different technologies like CNN and RNN may help the security personnel to make a distinction between a normal and a malicious activity thereby controlling the frequency of dubious alarms. This will bring more reliability and accuracy in the system.User Entity and Behaviour Analysis (UEBA), Next Generation Firewall (NGFW) and Web Application Firewall (WAF) have now been deployed to make this system more user friendly and simple.

2. Anatomy of Cyber-attacks

Cyber-attacks can be more devastating than Nuclear Bombs. A bomb has a limited space to target and can cause damage in an area confined to certain limits or targets. But a Cyber-attack has a wide range where it can potentially cause damage. It is across barriers of political frontiers and can cause harm in different countries simultaneously.

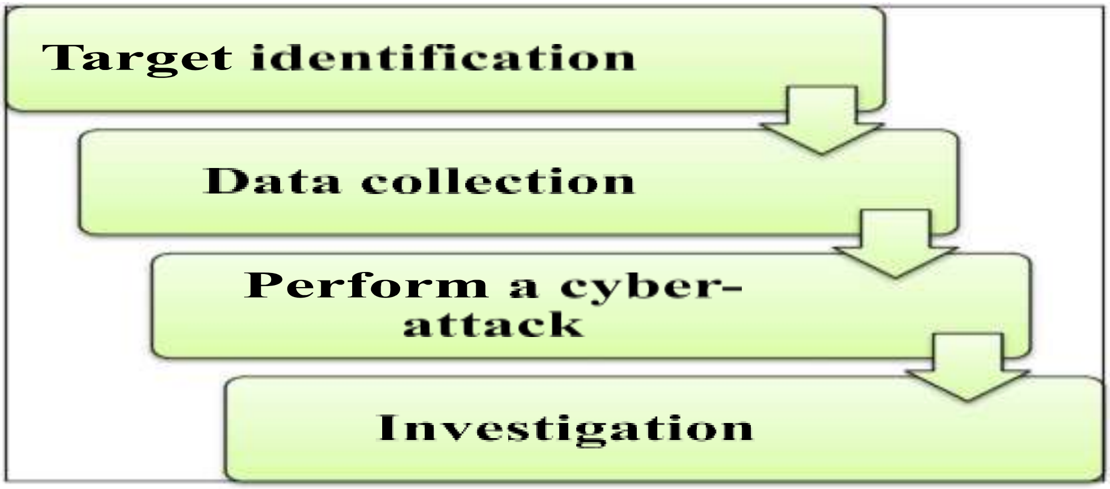

Diagram 1: Anatomy of Cyber-attacks.

H1N1 swine fluforced everyone to remain behind closed doors. However online methods of working made it possible for the world to carry out its activities. Payment apps, online transactions, shopping websites and online educational sources made it possible for people to do some kind of commercial and other activities. But these activities were done using personal mobiles or PCs which made it possible for the system intruders to breach into the software and hardware systems around the world.

The H1N1 swine flubecame more newsworthy due to widespread instances of infections and fatality. But there were a lot of Cyber security violations during that period as well. People were caught off-guard and there were many instances of Cyber-frauds. Since most of the companies allowed their employees to resume official duties from their living space, vulnerability levels increased. As a result there arose a need for stricter security mechanisms and safety parameters.

There is a general lack of IT or cyber security expertise in common users. They allow activities or download software without sensing the possibilities of frauds. It was a big challenge for the engineers to make it possible that the intrusions are checked and the system remain safe. They have to work on various technologies to make this happen.

Of the major technologies which emerged during this period is the Intrusion Detection System as a useful tool of ANN.

3. Artificial Neural Network in Network security

The popularity of Artificial Neural Networks is consistently on the rise in the field of network management. In order to make the monitoring system more effective, ANN depends on a combination of things including AI and Intrusion detection system.

3.1 Intrusion detection system

IDS works just like a traffic controller. It monitors and review all network activities and see if they are normal. Whenever it suspects anything fishy, it sets an alarm and alerts the user.

IPS on the other hand, is more of a preventing system. Therefore instead of detecting and documenting harmful activities, it goes a step further and prevents any potentially harmful event to happen.

3.2 Working of Intrusion Detection System

It is always better to catch the thief before he conducts any mischief. Hence the working of IDS is based on finding out irregular network activities and prevent potential losses. There are two types of Intrusion detection systems; host based and network based. Both the systems are effective and used at appropriate places.

3.3 of intrusion detection systems-Types

3.3.1 System which is installed at a pivotal point or points which are of strategic importance for the network is called a network intrusion detection system (NIDS). It keeps a close eye on all the network traffic and monitors it no matter whether it is inbound or outbound.

3.3.2 Another system is a host based system which is normally installed on all machines or devices connected with the internal internet network of an enterprise. A host intrusion detection system (HIDS) scores over NIDS as it is able to recognise those malicious events which occur within the organisation and which the NIDS is not able to detect.

3.3.3 The system which keeps a vigil on all network points and continuously keeps them comparing to a database of known malicious attributes is called a signature-based intrusion detection system (SIDS).

3.3.4 Sometimes another system is used which compares the network traffic with certain predefined parameters of internet like the bandwidth, hardware and software settings and permissions etc. This system is called as an anomaly-based intrusion detection system (AIDS).

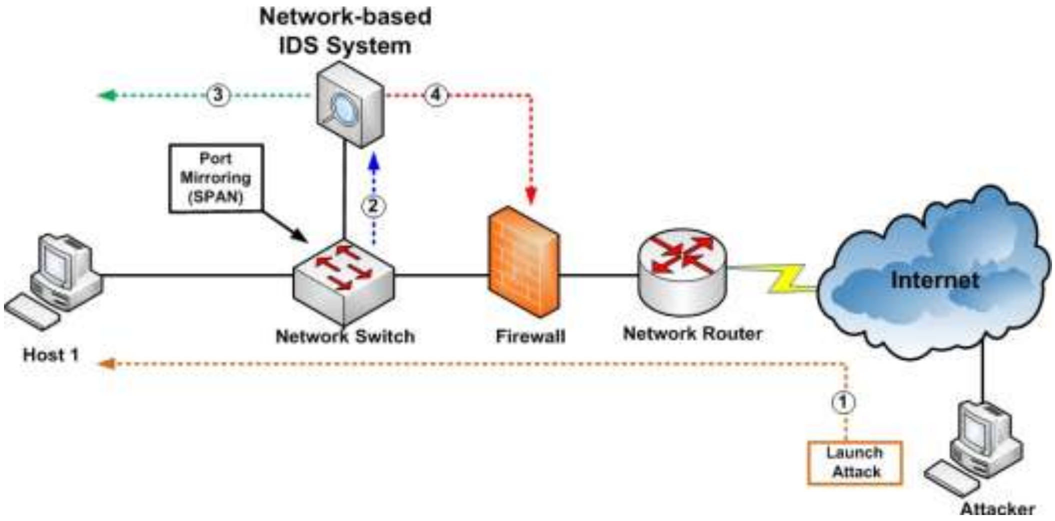

Diagram 2: Intrusion detection system

4. Primary Model Approachesin IDS

There have been different approaches for the use of IDS depending upon its requirements. Some are reviewed by the Centerfor Education and Research in Information Assurance and Security(CERIAS).

4.1 Misusedetection Approaches

- When the cyber-attacks originate from a series of audit events signature verification approach is followed
- petrinets approach is used in case of a graphical formation could be created due to an attack
- When there are different cases and transitions and various kinds of goals of an attack sate-transition diagrams are used.
- Expert systems are also deployed in many cases.

4.2Anomalydetection Approach

It includes:

- Thres hold recognition of any unusual event on the network or the network server.
- statistical formulations and approaches likedata derived from previous values
- Rule-based measures created by the developers.
- non-linear algorithms

5. Advantages of Neuralnetworkincybersecurity

In circumstances when rules are unknown, the usage of Artificial Neural Networks (ANN) can build pattern recognition and identify attack, according to several case studies. A neural network approach may be tailored to specific limitations, allowing it to recognise patterns and compare recent actions to previous behaviour, allowing it to solve numerous problems without the need for human interaction. The system claims to not only detect misuse but also to increase the consistency with which dangerous events are recognised. A neural network can detect any possible misuse, allowing the system administrator to defend their entire business by increasing their flexibility in the face of attacks.

6. Conclusion

Most of the expertise are of the opinion that ANN is the best suited for deriving and recognising various patterns of potential Cyber Attacks. Its quality is better than other mechanisms and is more reliable as well. We are advancing in the digital world rapidly and it is accepted that there are bound to be more challenges in the form of malicious activities as well. The security solutions must include a combination of available and progressive technologies to make the digital world safe and reliable. This can only be done by using AI and NN both because they have proved their worth already in helping detect many potential threats. However they are still in the progressive stage and further enhancement is required by making requisite changes and adjustments to the available technology to make it more potent and accurate to notice a Cyber-assault and protect the digital activities.

7. References.

1. Lazarevic, A.|Ertoz, L.|Kumar, V.|Ozgur, A.|Srivastava, J.: A Comparative Study of Anomaly Detection Schemes in Network Intrusion Detection. In Proceedings of the Third SIAM International Conference on Data Mining 2003, pp. 25{36).
2. Hochreiter, S.; Schmidhuber, J. Long short-term memory. Neural Comput. 1997, 9, 1735–1780.
3. El Hihi, S.; Bengio, Y. Hierarchical recurrent neural networks for long-term dependencies. In Advances in Neural Information Processing Systems; MIT Press: Cambridge, MA, USA, 1996; pp. 493–499
4. Patcha and J.-M. Park, ``An overview of anomaly detection techniques: Existing solutions and latest technological trends," Comput. Netw., vol. 51, no. 12, pp. 34483470, Aug. 2007.
5. Sperotto, A.; Schaffrath, G.; Sadre, R.; Morariu, C.; Pras, A.; Stiller, B. An overview of IP flow-based intrusion detection. IEEE Commun. Surv. Tutor. 2010, 12, 343–356.
6. Wu, S.X.; Banzhaf, W. The use of computational intelligence in intrusion detection systems: A review. Appl. Soft Comput. 2010, 10, 1–35. [CrossRef]
7. Nguyen, T.T.T.; Armitage, G. A survey of techniques for internet traffic classification using machine learning. IEEE Commun. Surv. Tutor. 2008, 10, 56–76.
8. Tzortzis, G.; Likas, A. Deep Belief Networks for Spam Filtering. in Tools with Artificial Intelligence. In Proceedings of the 2007 19th IEEE International Conference on ICTAI, Patras, Greece, 29–31 October 2007; Volume 2, pp. 306–309.
9. Koen J. A practical method for field diagnoses of swine diseases. *Am J Vet Med.* 1919;14:468–70.
10. Zhang H, Chen L. Possible origin of current influenza A H1N1 viruses on. *The Lancet.* 2009;9:456–457.