Analysis of AI Based Approach to Prevent Cyber Attack on Web Applications in Contemporary Digital Era

Praveen Kumar Shukla, C. S. Raghuvanshi, Hari OmSharan

Department of Computer Science and Engineering, FET Rama University, KanpurU.P.,India

praveenshukla26@gmail.com

Abstract:

Detecting and avoiding security crises is very critical to a country's total security for its businesses, governments, organizations, and its inhabitants. Cyber security services andmanagement are vital since governments, military, financial and medical institutions acquire, process, and store enormous quantities of data on computers and other devices. To safeguard networks, computers, programmes, and data against attacks, disruptions, or unauthorized access, the term 'cyber security' is often used. Security solutions like antivirus, firewalls, user authentication, encryption, and so on may not be in use because of today's various requirements. It is possible to employ prominent AI approaches, such as machine learning (ML) and deep learning (DL), as well as NLP, KRR, and rule-based expert system modelling, to rationally handle today's varied cyber security concerns, such as intrusion detection and prevention systems. Discrepancy-based intrusion detection systems are the focus of this study, which uses the Machine Learning area of Artificial Intelligence to increase detection quality. Machine learning algorithms can only learn about the traffic in a dataset, not the actual traffic under observation. "They must be re-trained on the monitored network, which is very challenging since labelled datasets containing assaults on a real network are necessary.''Consequently, the purpose of this article is to give details about an AI based approach for cyber security using intelligent computing.

Keywords: Machine Learning, Natural language processing, Knowledge representation and reasoning, Monitored Network, Intrusion detection system, Labelled datasets.

Number: 10.14704/nq.2022.20.7.NQ33224 **Neuro Quantology 2022; 20(7):1779-1788**

1. Introduction

Detecting and avoiding security crises in real time and with intelligence is critical to a country's total national security for its businesses, governments, organisations, and its inhabitants. As a result, cyber security services and management are vital since governments, military, corporations, financial, and medical institutions acquire, process, and store enormous quantities of data on computers and other devices. To safeguard networks, computers, programmes, and data against attacks, disruptions, or unauthorised access, the term 'cyber security' is often used. Known as information technology security or electronic information security, it is sometimes referred to as security. Security solutions like antivirus, firewalls, user authentication, encryption, and so on may not be in use because of today's various requirements. They are often controlled by a small group of skilled security specialists, where data processing is done

ad hoc and can't be run intelligently in accordance with the demands of the organisation. [1].

Machines that can think and act like humans are often referred to as artificial intelligence (AI), a discipline of computer science. It is possible to employ prominent AI approaches, such as machine learning (ML) and deep learning (DL), as well as NLP, KRR, and rule concerns, such as intrusion detection and prevention systems. "For example, these approaches may be used to identify harmful activities, detect fraud, anticipate cyber-attacks, manage access control, detect cyber-anomalies or intrusions, and so on and so on.'' Consequently, the purpose of this article is to give a reference guide for academics and industry representatives who want to collaborate and conduct research in the subject

of cyber security using intelligent computing. To address today's cyber security challenges, common AI-based approaches and their application are of major relevance.

The type of attacks we can disposed to:

A. Advanced Malware

B. Insider threats

C. Transaction frauds D.Encrypted attacks E.Data exfiltration

F.The exploitation of run-time application G.Acquisition of accounts

H.Network-Lateral-Movement.

Machines and apparatus that may have been attacked to predict, identify and prevent the potentially new threats this all can be possible with cyber security analytics.

Why do we need AI Cyber security Detection systems?

1. This is Rule-based detection systems for the handling of wrong positives results while treatment attacks.
2. Hunting of threats professionally.
3. Complete analysis of threat incidents and study.
4. Threat estimating
5. Retrieve the affected systems; examine the root causes of the attack, and improve the security system.
6. Monitoring of safety.

3. APPLICATIONS OF AI IN SECURITY

3.1 AI in Antivirus Services

Artificial intelligence-enhanced antivirus software detects questionable processes in the network. Networked assets are protected from all forms of attacks by AI antivirus when malicious software is released.

3.2 Modeling user behavior

Network users' performance is monitored by AI. ''The goal of the assessment is to determine how well users of the system are able to detect efforts at systemic overthrow." AI also monitors and analyses the behaviours of its users, identifying abnormalities in their behaviour as anomalies. It is possible for AI-powered systems to recognise suspicious activity when a new user comes in and either invalidate the user or warn system administrators.

3.3 Automated network and system analysis

Continuous monitoring and early identification of suspected cyber-attacks are assured by the use of automated network information analysis. In order to avoid detection by network security, attackers use command and control mechanisms. For example, DNS requests are used to bypass

firewalls and IDS/IPS. AI-enabled cyber security employs anomaly detection, pattern comparison, and data tracking. There are a huge variety of network or system assaults that may be detected bythis method.

3.4 Spam filter applications

Gmail use artificial intelligence (AI) to identify and prevent spam and fraudulent emails. For every 'Spam' or 'Not Spam' you click on an email in your Gmail account, you're really helping teach Gmail's AI to spotspam in the future. Thus, AI has advanced so much. Spam messages disguised as 'normal' emails are no match for this programme.

3.5 Fraud detection

To combat fraud, MasterCard has implemented Decision Intelligence, an AI-based system built on customer behaviour predictions. An unusual purchase is one that does not fit in with a customer's usual buying patterns, vendor, or geographic area, all of which are taken into account by a complex algorithm.

3.6 Botnet Detection

When it comes to botnet identification, patterns and timings in network requests are crucial. A botnet assault on a wide scale usually involves numerous 'users' making the same or similar requests on a website since botnets are often managed by a master script of instructions. Botnet brute force attacks, network scans for flaws, and other exploits are all possible causes

of this. Even if summarising the very intricate function artificial intelligence plays in botnet detection would be tough, we've found a great piece ofstudy that does just that.

4. CRIMINALS USE AI TOINCREASE THEIR HACKING RESULTS

4.1 AI Risks

Overflowing may be caused by AI errors. Even with the most cutting-edge artificial intelligence systems, developers and even individual data sources may introduce bias via omission. Unintentional development and implementation errors are the root causes of these dangers. However, a new set of issues develops when people attempt to bypass or weaponize artificial intelligence.

Human supervision, careful evaluation of AI systems during the design phase, and active monitoring of AI systems after they are operational help mitigate these dangers [4].

4.2 AI manipulation

intelligence may be tampered with by hackers, or suspicious situations might be created during the process of training AI. Forcing mistakes by changing inputs is a common tactic used by hackers when they do not have access to datasets. In order to make authenticating with a human ID more difficult, "AI systems trick their users into believing they are someone else.'' The dataset used to train AI systems is obtained by the attackers via the process of 'reverse engineering' of AI systems.Hackers get access to confidential databases, allowing them to contaminate data or create AI systems that can be replicated.

4.3 AI is the answer to AI-based attacks

New and trendy tactics are used by Hackers to infiltrate and destabilise administrations and weaken their information. There has been an increase in the usage of artificial intelligence (AI) in cyberattacks. It's a shame that artificial intelligence (AI) isn't only available to ethical hackers and computer security professionals. It can be hacked by those who aren't in the best of intentions.

Artificial Intelligence (AI) is an intriguing tool for cybercriminals. As long as they can blend in with the distortion, they will be able to evade notice. Attacks based on artificial intelligence (AI) areable to recognise and mimic actual user behaviour in order to evade traditional security measures.Suggestions for what to do:

a.Experts need to plan for the best AI software system that can evaluate all likely threat parameters, choose the right plan, implement effectively, and locate malware.

b.Use AI software to fight AI when tracking logs.

c.AI security log analysis is a great technique to look for irregularities. It can find for and generate predictive insight using a very large number of factors, resultant in predictive capabilities.

d.Organizations need to assess how AI attacks are likely to be used against their AI system. And then develop response plan strategies to moderate the impact.

e.Natural language processing can be used to gather data of all sorts of cyber-attacks, collect threat data, and improve secrecy features.

f.AI computerization of operations makes the Data sets used in the training of artificial human experts capacity and optimizes response time[5].

4.4 AI attacks are basically altogether very different from old fashioned attacks

Algorithmic approaches to processing AIsystems make them vulnerable to assault. We can't modify them in a safe way as we can in old-fashioned cyber-attacks because of the security challenges and problems that come with it. With the usage of old-fashioned

cyber-attack prevention and security software, there is a lack of common protocols to enable businesses to deploy AI solutions that halt and protect them from all sorts of assaults on their AI-based systems.

It's now really fun and simple to teach an AI system new skills. Intruders may readily edit and manipulate the data set used to train AI, allowing them to obtain their desired outcomes. Intruders may resort to elusion, tampering with inputs in order to force obligations, when they are unable to locate data. Artificial intelligence (AI) systems may be programmed to produce incorrect identifications by altering input data. It

is very difficult to verify the accuracy of data and inputs, and hence efforts should be taken to acquire data from reliable sources.

Handling implication, in which intruders make every attempt to reverse engineer, is tough. systems of artificial intelligence to discover what kind of input data is utilised to order them. Having access to sensitive data and being able to manipulate an AI system for their own purposes is made possible by this concept.

4.5 Artificial intelligence could be used as a weapon

Artificial intelligence (AI) has been the subject of several tests by security firms, computer scientists, and other professionals. No human involvement is required for AI-based devices and software systems to detect and react to cyber threats rapidly and effectively. When it comes to online safety, artificial intelligence (AI) tools are a game changer. 45 percent of IT businesses use AI and machine learning for cyber security inside their organisations for safety concerns Detection and reaction procedures are both improved and automated by

AI. This saves money and time that would otherwise be spent on human intervention and detection[7].

5. LITERATURE REVIEW

PAPERTITLE	RESEARCH TECHNIQUE	FUTURESCOPE
The Role ofArtificialIntelligence inCyberSecurityJanuary 2019DOI:10.4018/978-1-5225-8241-0.ch009	In this papermalwaredetection has been done using various machine learning techniques like supervised ml,unsupervisedml,patternrecognitionapproach,signaturebasedtechniques,malware detectionusing ai, network intrusion detection using AI .	If AI isimplementedand trainedwith propercare, it canimprovecyber securityin many ways.It can protectagainst thecyber-attacksin real timewith lesserresources.Using Deeplearning andmachinelearning indefensesystems willsurelytake cybersecurity to anew level ofintelligence.
AI-DrivenCybersecurity: AnOverview,SecurityIntelligenceModeling and ResearchDirections 26 March2021	In this paper basic security properties,CIA triad, cyber security and their related terms, defense strategies and attack are discussed. Moreover, in this a security intelligence based model lingsystem designed which uses NLP(natural language processing) approach.	Several important issues such as data aggregation, redundancy in rule generation, effectiveness of prediction algorithms, data inconsistency, recent patternanalysis for predictionmight be animportant issue foreffectivedata-drivenmodeling. Thus,advanced analyticstechniques, improved machine ordeep learningtechniques, new datadrivenalgorithms, orhybrid methods couldgive better results for modelingsecurity intelligence, depending onthenature of thesecurity problems,which could be a potential research direction in the area.Therefore, adeeper understanding and designing an effectiverule-basedSystem by taking intothese propertiesCould beanother research issue in the area of AI-driven cyber security
ArtificialIntelligence for	In this papervarious AIalgorithmssuch	AI hasfacilitated areduction in

Cybersecurity:A Systematic Mapping of Literature July 30, 2020Digital Object Identifier 10.1109/ACCESS.2020.301 3145	asKNN,K-means,CNN,Random forest,RNN,S VM,ANN are used on variousapplication domains for a longer period of time to identify the most dominantmethod used.	computational complexityand reduced model training times. It wasalso observed that there is a considerableskewnesswithinthe domain.Moreover, researchers have focusedon feweralgorithms andas such newer algorithms are not popular.This stands as both achallenge and also anopportunity forresearchers.
ArtificialIntelligence in CyberSecurity 2021J. Phys.:Conf. Ser.1964 042072	In this paperthe method used to get anall-roundimpression ofthe junctionbetween cybersecurity andAI, we usedfour databases:Scopus, Webof Science,ACM digitallibrary andIEEE Xplore.Along withthat, we alsoused theGoogleScholar searchengine. A setof keywordsmatching thetopics weresearched for inthesedatabases andthen obtainedresults werefiltered.	When youintend future study,production,andimplementation of an AIapproach oncyber security,you willdifferentiateamongimminenttargets andlong-termoutlooks.Multiple AIapproachescan be usedon cybersecurityquickly, andurgent cybersecuritychallengesneed smartersolutions thanthey areactuallyapplied.Theintroduction ofentirely newconcepts ofinformationprocessing inthemanagementofcircumstancesand decisionmaking in thefuture wouldbe exciting.
System (IDS) International Journal ofScientific & Engineering Research, Volume 2,Issue 1,January-2011 1ISSN 2229-5518	monitor network assets to detect anomalous behaviour andmisuse in the network.Basics of IDS, theircategories(signature based, anomaly based,specification based) andclassification of IDS like host based ids,network based ids, hybridbased ids are discussed indetail.	responsible formonitoring the processes and matching the actual datawith theprogram and incase of any Abnormal behaviour will be issued an alert and mustbe maintainedand updated whenever achange wasmade on the surveillance programs in order to beable to detect the previousattacks theunknown andthe number of false positiveswhat can beless than the anomaly detectionsystemapproach. So from this paperanyone can take reference and understandthe basics and can implementit in various domains in

		future.
The future of ArtificialIntelligence in Cybersecurity: AComprehensive Survey07 July 2021doi:10.4108/eai.7-7-2021.170285	In this paperalgorithms areproposed for learning thesystem whichis concentratedin IDSscenarios. Inorder to dothat, acategorizationis taken intoconsiderationfor cybersecurity datasets groupingtheir data intomany groups.This work willdecide themodels in theneural network(multilayer orrecurrent),activationfunctions andlearningalgorithms,depending onthe database,to achievehigheraccuracy.Finally, theresults wereused todeterminewhich datacategory of thecyber safetydata set wasmoreimportant forintrusiondetection andthe mostadequateconfigurationof the machinelearningalgorithm to minimizecalculationburden.	Artificialsmart methods contributed remarkably tocybercrimesbysignificantlyimprovingintrusiondetectionsystems but itwas also foundthat computercomplexity,model trainingtimes and falsealarms havebeen reduced.However, thedomain issignificantlyskewed. Mostresearchcentred onintrusiondetection andpreventionsystems andsupport vectormachines werethe mostdominanttechniqueused. Sincecybercrimesare becomingincreasinglycomplex,cyber securityapproaches areneeded to bemore robustand intelligent.This will allow can react effectively to sophisticatedattacks.
ArtificialIntelligenceApplicationsin CybersecurityIJCSNSInternationalJournal ofComputerScience andNetworkSafety,VOL.20 No.2,February2020	This researchpaper aims toshed light onthe concept ofartificialintelligence,identify themost importantareas ofartificialintelligencethat can beused in cybersecurity, andclarify the rolethat these areascan play(especiallymachinelearning, datamining, deeplearning andexpertsystems) insupportingcyber securityinOrganizations.	The mostrelevant resultsof the presentresearch papercan be drawnas cybersecurity is acritical andvital topic forprotectingdata,information,and systems.Moreover,many areasandapplications ofartificialintelligencecan contributeto enhancingcyber security,such asmachinelearning, deeplearning, datamining, andexpertsystems. Thepossibility ofutilizing dataminingalgorithms todevelop and
Technique	**Description**	**Algorithm**
Classification	For determiningwhether the security eventis reliable or notandbelongs to the group or not.	ProbabilisticAlgorithmssuch as Naive Bayesian andHMMInstance-based algorithmssuch as KNN,SVM, andSOM. NeuralNetworksDecisionTrees
Pattern Matching	Detection ofmalicious patterns andindicators inlarge datasets.	Boyer MooreKMP EntropyFunction
Regression	Determinationof trends in securityevents as well as predictionof thebehavior ofmachines andusers.	LinearRegressionLogisticRegression MultivariateRegression
Deep Learning	Creatingautomated playbooks based on pastactions for hunting attacks.	DeepBoltzmannMachineDeep Belief Networks

AssociationRules	Alerting afterdetectingsimilarattackers andattacks.	AprioriyEclat
Clustering	Determinationof outlier and anomaly.Creation ofpeer groups of machines andusers.	K-means-ClusteringHierarchical Clustering
AL usingNeuroscience	Increase of human intelligence, learning with each interaction to proactively detect,analyzes, and offersactionable insights intothreats.	Cognitivesecurity

a. Threats to cybersecurity are always evolving. In certain places, cybercrime is a separate budget. Artificial intelligence-based security solutions have to be retrained when new threats arise in order to stay pace.

b. Artificial intelligence (AI) is used by cybercriminals, too. In order to test their harmful programmes against AI-driven cyber security systems, they are able to obtain them. Thus, scientists may hypothetically generate an AI-resistant malware strain. If they can figure out what an AI-based security system is searching for, they may either mask their attack or contaminate thesample in order to make their assault seem benevolent. Only in the sphere of security do AI systems engage in a counterattack.

c. Taking precautions is always a good idea. ''There is still a long way to go before AI systems can distinguish between harmful and non-malicious behaviour with 100% accuracy." It is common for most cyber security systems to err on the side of caution while protecting networks, applications, and data. That is, if anything seems out of the ordinary, mark it as potentially dangerous.

As a result, unusual activity may be detected and human analysts can study it further. Another way to be careful is to lose actual assaults by reducing the amount of false positives.

6. LIMITATIONS

7. ADVANTAGES

a. The loudness is no problem for AI. Detecting cutting-edge dangers is made possible thanks to artificial intelligence. It takes AI a fraction of the time to evaluate the huge amount of data that is sent and received over a company's network, including emails, files, and websites visited by workers. A

computer's ability to classify the overwhelming majority of activity and samples as innocuous frees up human analysts' time to concentrate on the comparatively small number of suspicious or possibly harmful events that may be detected by artificial intelligence (AI).

b. It is possible for AI to learn about cyber security over time. The behaviours of programmes and the network as a whole may be used by AI to detect malicious assaults. As a network's normal traffic and activity patterns are studied over time, AI cyber security systems may detect departures from thenorm.

c. Artificial intelligence finds unknown threats. Hundreds of millions of malicious attacks are launched every year.

8. AIMS AND OBJECTIVES OFRESEARCH

Discrepancy-based Intrusion Detection System detection is the focus of this study, which uses the Machine Learning area of Artificial Intelligence to increase detection quality. Because the final findings obtained do not apply to actual networks, working on and refining detection algorithms on well-known datasets is insufficient and inefficient for achieving this aim. Machine learning algorithms can only learn about the traffic in a dataset, not the actual traffic under observation. "They must be re-trained on the monitored network, which is very

challenging since labelled datasets containing assaults on a real network are necessary.'' As a result, the second goal of the thesis is to create a system for detecting disruptions in unfamiliar networks without the need of predefined datasets.

9. RESEARCH METHODOLOGY

Machines and equipment that may have been attacked to predict, identify and prevent the possiblenew threats this all can be possible with cyber security analytics.

How Machine Learning and Deep Learning is helping in Cyber Security?

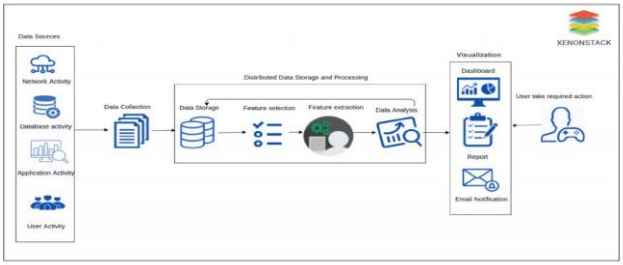
approach are forgotten or disregarded. ''The sheer number of rules in rule-based systems creates a cognitive strain that prevents full comprehension." As a final point, these system outputs are difficult to measure and only improve slowly over time.

https://www.researchgate.net/figure/Unnecessary

-data-removal tactic_fig3_323118409

9.1. Unnecessary Data Removal

9.2FeatureExtraction



Due to their restrictions, the algorithms outlined above are unable to be used for security analytics. Itis thus necessary to adopt a number of main methodologies for security analytics [9]..

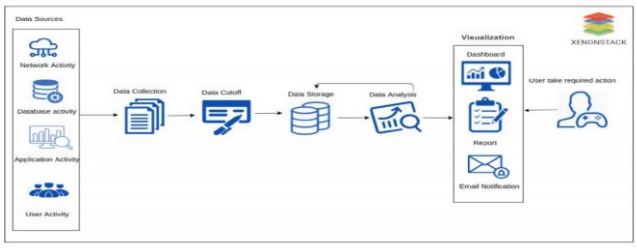
Specialized Knowledge

Security analytics is a complex job that requires specialized knowledge of risk management systems,log files, network systems, and analytics techniques.

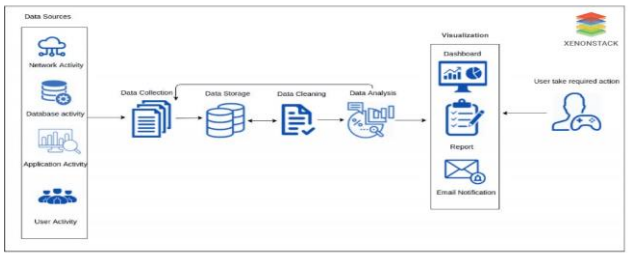
Opacity

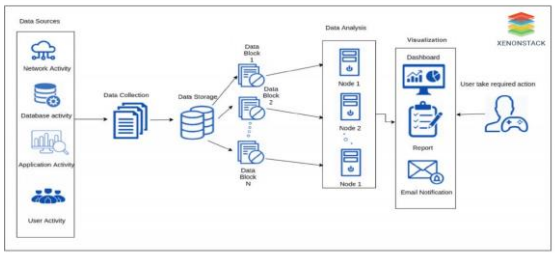
Once a decision has been made, the statistics, machine learning, and mathematics underlying each

9.3 Data Cutoff

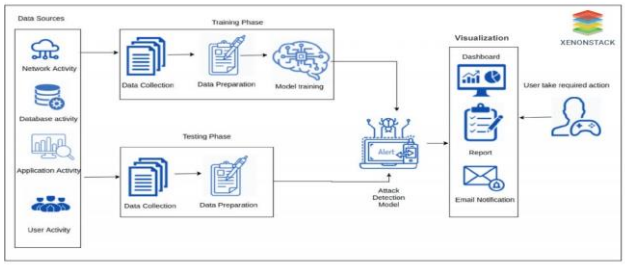


9.4 Parallel Processing





9.5 ML and DL algorithms for EnablingArtificial Intelligence Cyber security



10. CONCLUSION

Detecting intrusions is an element of the overall defence strategy, which includes firewalls, anti-virus software and other security measures. Attack indications are detected by the intrusion detection system, which subsequently sends a warning message. These systems are often classified as abuse and irregularity detection systems, depending on how they are detected. In terms of implementation, they may be categorised as either network-based or host-based IDS. Network and host resources are combined in modern intrusion detection systems. An intrusion detection system's accuracy improves as the number of assaults it detects grows and the number of false positive alerts decreases.

Refined tactics and social engineering strategies are used by cybercriminals to lead computer users. Some cybercriminals are becoming more and better at their craft and their goals. It has been established that cybercriminals can conceal their identities, mask their communication, separate their identities

from unlawful gains, and deploy infrastructure that is impervious to hacking attacks. As a result, effective intrusion detection systems capable of identifying contemporary viruses are becoming more critical for computer systems. Such IDS systems need a thorough understanding of the strengths and weaknesses of existing IDS research. Zero-day attacks are examined using various machine learning approaches.

11. REFERENCES

1. Kirti Raj Bhatele, Harsh Shrivastava 'The Role of Artificial Intelligence in Cyber Security' January 2019 DOI: 10.4018/978-1-5225-8241-0.ch009

2. Iqbal H. Sarker, Md Hasan Furhad,Raza Nowrozy, 'AI-Driven Cyber security: An Overview, Security Intelligence Modeling and Research Directions' 26 March 2021

3. ISAAC WIAFE1, FELIX NTI KORANTENG, EMMANUEL NYARKO OBENG, NANA ASSYNE,ABIGAIL WIAFE, AND STEPHEN R.

GULLIVER 'Artificial Intelligence for Cyber security: A Systematic Mapping of Literature' July 30, 2020 Digital Object Identifier 10.1109/ACCESS.2020.3013145

4. Rammanohar Das and Raghav Sandhane 'Artificial Intelligence in Cyber Security' 2021 J. Phys.: Conf. Ser. 1964 042072

5. Asmaa Shaker Ashoor, Prof. Sharad Gore, 'Importance of Intrusion Detection System (IDS) International Journal of Scientific & Engineering Research, Volume 2, Issue 1', January-2011 1 ISSN

2229-5518

6. Feng Tao,Muhammad Shoaib Akhtar, and Zhang Jiayuan.'The future of Artificial Intelligence in Cyber security: A Comprehensive Survey' 07 July 2021 doi:10.4108 / eai.7-7-2021.170285

7. Azzah Kabbas, Atheer Alharthi, and Asma Munshi 'Artificial Intelligence Applications in

Cyber security IJCSNS International Journal of Computer Science and Network Security', VOL.20 No.2, February 2020.

8. Bai J., Wu Y,Wang G,Yang S. X., Qiu W(2006).

'A very distinctive intrusion detection model based on multilayer self-organizing maps and

principal part analysis.Advances in Neural Networks. Springer'.

9. Barika F.,Hadjar K., & El-Kadhi N.(2009). 'Artificial neural network for mobile IDS resolution. Security and Management ' Journal, 271–277.

10. Bostrom N.(2015), 'TED Talk on Artificial Intelligence.'Retrieved fromhttps://en.tiny.ted.com/talks/nick_bostrom_what_happens

11. Chatzigiannakis V., Androulidakis G., & Maglaris B. (2004). 'A Distributed Intrusion Detection Prototype Using Security Agents. In Proceedings of Workshop of the HP Open View University Association. University of Evry'.

12. Iftikhar B., & Alghamdi A. S.(2009). 'Application of artificial neural network within the detection of dos attacks. Proceedings of the ordinal international conference on Security of knowledge and networks', 229–234.