CHAPTER

Machine Learning Techniques in Network Security: A Comprehensive Survey, Performance Analysis, and Time Complexity Comparison

PREETI[1],PRITI SHARMA[2]

[1,2]*Department of Computer Science and Applications, MDU university,Rohtak,124406,India*

[1]*Correspondingauthor:E-mail:miskhokhar121@gmail.com*

ABSTRACT

The web has transformed into a fundamental variable for all locales of the state-of-the art world. The world is ending up being progressively dependent onthe web for its standard of living. The rising dependence on the web has further expanded the risks of toxic exposure. In light of the advancement of online security bets, network wellbeing has turned into the most pressing part in the computerized world to battle against every single computerized risk, attacks, and cheats. The extension of the internet is profoundly related to the increasing chance of being pursued by wearisome digital dangers. The goal of this overview is to give a concise survey of various AI (ML) strategies to make quick work of the relative multitude of improvements made in location techniques for potential network protection. These online protection risk discovery strategies primarily include extortion recognition, interruptionlocation, spam discovery, and malware identification. In this Chapter, we expand upon the current literature on the uses of ML models in online protection and give an exhaustive survey of ML methods in network safety. As far as we could possibly know, we have prepared the principal endeavor to givea correlation of the time intricacy of generally utilized ML technique in network safety. “We thoroughly examined each classifier's performance; takinginto account commonly used datasets and advanced risk subspaces”. This chapter define a concise demonstration of simulated intelligence techniqueother than generally used protection datasets. Despite meeting every of the fundamental requirements, network security has its limitations. Furthermore, challenges This work, in like manner, explains the huge current hardships and cutoff points looked at during the usage of man-made intelligence techniques innetwork assurance.

1. INTRODUCTION

The web is becoming quicker as a principal focal point for a center- to-center in sequence movement, all with its charms and difficulties. The extensive variety of the web embraces the web, clients, organization capital, the specific capacities of individuals, and impressively more, notwithstanding the web. Advanced risks and attacks. Network security is a collection of events, devices, and strategies used to protect the web from computerized assaults and dangers [1-2]. In the high-level world of PC and information advancement, cybercrime is developing with faster endeavors that appear differently in comparison to the continuous web-based assurance system. “The feeble system plan uneducated workers and small proportion of techniques are factors that contribute to shortcomings in a PC's structure and posture perils [3]”. Because advanced risks are being created, more progress in developing network security procedures should be made. The outdated and standard organizational wellbeing methods have a significant disadvantage in that they are insufficient for managing dark and polymorphic protection attacks. There is an essential for strong and undeniable-level protection strategies that they can get from their encounters and perceive in long-ago and future dim attacks. Computerized perils are expanding in a gigantic way. It is turning out tobe uncommonly hard to change to the rapidity of wellness risks and presentvital responses to hinder them [4-5]. Experts have watched out for the degrees of progress, limitations, and prerequisites of applying simulated intelligence methodologies for recognizable proof of cyber-attacks and have outfitted standard procedures with computer-based intelligence techniques. Simulated intelligence is a secondary-meadow of man-made thinking. ML methodologies are worked in the midst of the abilities to acquire from encounters and information without being altered unequivocally [6]. Uses of ML systems are stretching out in different ordinary issues, for instance, preparing [7,8], clinical [9-11], business and online security [12-14]. ML strategies are applied to make prompt areas of strength for andprocedures. Computerized risks: man-made intelligence systems are expectinga urgent job in engaging against network security risks and pursue, for instance,the interference disclosure structure” [15, 16,17]. Phishing region [18, 19], spam affirmation [20, 21], and bending disclosure [22], to give a couple of reproductions. Malware is a great dealof decides that are anticipated pernicious presumption to upset the customary development of PC works out. Unsafe code innings on an allocated machine with the objective to do insidiousness and cooperation the fairness, secret, and receptiveness of PC assets and associations [23]. Talked about the super-fundamental issues in applying PC based knowledge strategies for malware affirmation. One more gamble to PC assets is a spam message [24]. Junk messages are undesirable and referenced mails that chomp a ton of affiliation assets nearby PC memory and speed.ML frameworks are being utilized to see and depict a message as spam or ham. ML techniques have a fundamental commitment to see junk mail on PC [26, 27], SMS messageson adaptable [28], junk tweets [29], or pictures and recordings [30,31].

An interference area system IDS is a fortification structure for PC systems against any interferences for looking at the association's shortcomings. peculiarity based, and creamer-based designs are seen as huge courses of action of an interference area structure for network assessment.

ML methodologies have a huge obligation to perceiving different sorts of breaks in associations and on have computers. In any case, there are different districts; for instance, the area of zero-day and new targets are seen as immense challenges for ML strategies [32].In this section, we develop the ongoing writing on the purposes of ML models in web-based security and give athorough review of ML methodology in network safety.

2. Literature Review

With the help of the program, a selective method for addressing basic logical and design inquiries is given by the AI applications [33]. During most recent twenty years, extremist headways have been seen in the field of AI with a simple admittance to the fledglings [34]. A lab "black box" environment has fundamentally set off the AI, which has then changed into a commonsense application, and business organizations are continuously carrying it out for a huge scope [33, 34]. The product applications PC vision [35, 36], normallanguage handling [36-37], discourse acknowledgment [36-38], robot control [36]and other arising applications are the advancements of AI [33]. For enhanced client experiences, to advance exceptional contributions, and to recommend purchases [33], AI is utilized by significant organizations like Amazon, Facebook, and Google It is far less difficult for computer-based intelligence designers to set up a structure than it is to programmed the standard data processing yield. They accomplish this by propagating from the normal yield [34]. Various endeavors have seen the impact of artificial intelligence, which seems to pose serious data issues, for instance in network safety [33]. A few fields, ranging from science [39-40] to cosmology to social science [41- 42], can similarly benefit from computer-based intelligence for significant transformations [34]. The trial information can be handled and broken down by AI in new ways [34].

Hypothetically, we can more readily comprehend the idea of "enormous information" by dealing with AI calculations. Also, these advancements can be utilized to further develop related execution measurements in vertical applications. There can be an extraordinary variety in the AI calculations as for exceptional capabilities (e.g., strategic relapse, direct Relapse, Guileless Bayes, choice trees, irregular woods, support vector machines, profound learning and Slope Helping calculations). By and by, AI acquaints imaginative ways with break down enormous measures of information with an expect to produce transformative methodology. Also, more noteworthy improvements can be given by the progressive ages of calculations [34]. The huge volume of information can in a perfect world be handled through AI and cybersecurity [34]. The stages and organizations are defenseless against assault. The viability of these assaults relies upon the quantity of instruments to check and assess targets [33]. AI is utilized by the enemies to additional increment their assaults. As of late, some There have been fewstudies on the security viewpoint of AI and man-made consciousness [43, 44]. Likewise, underlines contemporary writing on interruption location for PC network security and AI strategies utilized in the Web of Things. In this manner, for network examination of interruption recognition. Furthermore, [43,44,45] advised on security issues with respect to man-made brainpower, particularly the support and administered learning calculations.

3. Research Gap:-.

Pub. Year	Title of the Paper	Authors	Techniques Used	Research Gaps	Future scope
2021	“Detection of Phishing Websites Using Deep Learning Techniques ”[47]	**Md. Faisal Khana and B.L.Ranab**	DNN,CNN, LSTM,IG (select best features)	Proposed deep learning model for phishing detection with URL features.	In highlights, the outcomes can be improved by utilizing more heuristic elements to prepare the model.
2021	Malicious URL Detection using Deep Learning[48]	Sriram Srinivasana, Vinaya kumar Rb, Ajay Arunachal amc, Mamoun Alazabd:-	CNN,RNN, LSTM, CHARACT RLEVEL EM-BEDDING TEC.(to Train the model)	This model based on deep learning algorithms and character level embedding tech.	Exactness can be improved by considering the addition of helper modules, such as enrollment administrations, site content, network notoriety, document methods, and registry keys.
2021	“A hybrid DNN–LSTM model for detecting phishing URLs”[49]	“Alper Ozcan, Cagatay Catal,Emr ah Donmez, Behcet Senturk”	LSTM,DNN, N LP, CHARATER LEVEL EMBEDDIN G TEC.	In this examination work, proposed a half and half profound learning models use both person implanting	A more generic and robust model can be built by using word embedding tech.

				and NLP Features.	
2021	URLTran improving Phishing URLDetection Using Transformers [50]	"Pranav Maneriker, Jack W. Stokes, Edir Garcia Lazo"	"state-of-the-art transformer models, BERT and RoBERT"	In this investigation, they performed a thorough examination of the transformer model on the phishing identification task.	In feature, Results can be improved by using explicit danger models when adversarial expand the preparing information utilized for preparing them.
2021	"A Malicious URL Detection Model Based on Convolutiona l Neural Network" [51]	"Zhiqiang Wang, Xiaorui Ren, Shuhao Li",	DCNN, Word-Embedding, Charact er-Embedding	In this exploration work, proposed phishing location model utilizing profound learning strategy with word implanting on character inserting can accomplish higher precision.	In feature, can Improving the accuracy by simplify detection model.(try to select simple architecture to implement DCNN)
2020	"A comprehensive survey of AI-enabled phishing attacks detection techniques" [52]	"Abdul Basit ,Maha mZafar Xuan Liu2"	ML,DL.	This paper give an exhaustive comprehensive on of Phishing Assault and simulated intelligence Tech.	More adaptable and powerful strategy including the shrewd module arrangement.

2020	“Intelligent Phishing Detection Scheme Algorithms Using Deep Learning” [53]	“M. A. Adebowa le, K. T. Lwin, M. A. Hossain, ”	CNN,LSTM, Character Embedding and Word Embedding Tech.	In this examination work, They propose a phishing identification model utilizing profound learning with complex features. The proposed model achieved a precision rate of 93.28%.	They intend to concentrate on the most proficient method to work on the discovery model's design and abbreviate the preparation time while keeping the location execution unaltered later on.
2020	“Phishing URL Detection Using Machine Learning” [54]	“Preeti, Rainu Nandal, Kamaldeep Joshi”	LR,DT,SVM, RF.	In this research work, we critically analyses the performance of ML models.	In feature the Exactness of proposed model can be gotten to the next level using Deep Learning.
2020	“Analysis of Phishing Website Detection Using CNN and Bidirectiona LSTM”[55]	“A S S V Lakshmi Pooja1”	CNN,LSTM	Parallel Execution Of LSTM-CNN techniques could lead to better accuracy	Later on, can carry out strategy in an internet browser implanting module for distinguishing phishing site.
2018	“Web Phishing Detection Using a Deep Learning Framework” [56]	“Ping Yi,1 Yuxiang Guan,1 FutaiZou,”	Deep Belief Networks, for testing used IP flow and ISP.	This proposed model is train using original and interactive features. DBN model is test on the basic of IP	The precision of the forecast model can be moved along by using Multi-dimensional features.

				flow and ISP with 90% genuine positive rate and 0.6%flase positive rate.	
2018	“Deep Learning Based Phishing E-mail Detection” [57]	“Hiransha M, Nidhin A Unnitha n, Vinayak umar R, Soman KP”	Word Embedding technique and CNN	This proposed model is used to classify Phishing Mails using header with 0.942accuracy and without using header with 0.968 accuracy.	Exactness can be upgrade by adding a few extra information sources it will be increment the identification pace of phishing messages for the proposed strategy.
2017	“Phishing Website Detection basedon Supervised Machine Learning with Wrapper Features Selection” [58]	[Waleed Ali]	ML with Wapper-based feature extraction, PCA,IG feature Selection Methods.	BPNN, RF,KNN achieved best CCR; RBFN,NB performed worst.	Wrapper features enhance ensemble performance.

4. Cyber Security Technique:

Cyber-attack is currently a worldwide worry that hacks the framework, and other security assaults could imperil the worldwide economy.

In this way, it is fundamental to have a phenomenal network safety technique to safeguard delicate data from high-profile security breaks. As advanced attacks rise, organizations, especially those handling sensitive data, must establish robust security measures to protect information.

Network safety Objectives:

Network safety's primary goal is to guarantee information security. Thesecurity local area gives a triangle of three related standards to safeguard the information from digital assaults. This standard is known as the CIA group of three. The CIA model is intended to direct approaches for an association's data security framework. Security breaches stem from rule neglect.

Confidentiality

Secrecy is identical to security that keeps away from unapproved access of data. It includes guaranteeing the information is available by the individuals who are permitted to utilize it and impeding admittance to other people. It keeps fundamental data from contacting some unacceptable individuals. Information encryption is a magnificent instance of guaranteeingclassification.

Integrity

This standard guarantees that the information is legitimate, exact, and shielded from unapproved change by danger entertainers or unplanned client alteration. Assuming any changes happen, specific measures ought to be taken to safeguard the delicate information from defilement or misfortune and quickly recuperate from such an occasion. Likewise, it shows to make the wellspringof data authentic.

Availability

This rule makes the data to be accessible and helpful for its approved individuals generally. It guarantees that these gets to are not obstructed by framework glitch or digital assaults.

Types of Cyber Security Threats:-

A Threats in online protection is a malevolent movement by an individual or association to ruin or take information, get to an organization, or upsets computerized life overall. The digital local area characterizes the accompanying dangers accessible today:

Malware: Malware infers harmful programming, which is the most broadly perceived advanced pursuing instrument. It is used by the cybercriminal or developer to disturb or hurt a certifiable client's system. Coming up next are the critical sorts of malware made by the software engineer.

Virus: Malicious code spreads between devices, infecting files, spreading through networks, stealing data, and causing device damage.

Spyware: Surreptitious software records user behavior, potentially capturing sensitive information like credit card details for unauthorized activities like shopping or withdrawals.

Trojans: Malicious code masquerades as genuine software to deceive user into downloading and running it, aiming steal or destroy data.

Worms: "A piece of programming spreads copies of itself starting with one device then onto the next without human collaboration. It doesn't anticipate that they should affix themselves to any program to take or damage the data".

Adware: Adware, a marketing tool, spreads malware and displays ads without user consent generating revenue for its creator through browser advertising.

Phishing: Phishing is a cybercrime where deceptive sources, posing as legitimate entities, contact targets through email, phone, or text, urging them to click malicious link. This leads to divulging sensitive information or installing malware for remote control.

Man-in-the-middle (MITM) attack:" A man-in-the-middle attack involves a cybercriminal intercepting communication between two parties, posing as them to access sensitive information on business or clients.

5. Result and Discussion:

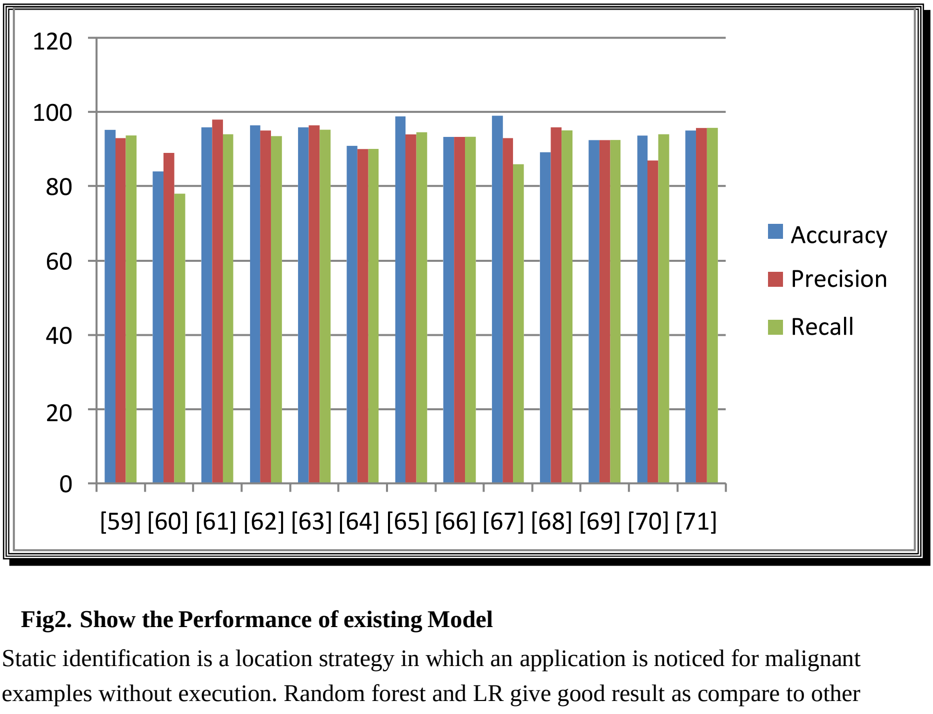

Fig2. Show the Performance of existing Model

Static identification is a location strategy in which an application is noticed for malignant examples without execution. Random forest and LR give good result as compare to other model exist in machine.Fig2.show the graphical representation of Table2.

Table2.Comparitevely analysis the performance of existing Model

Ref No	Accuracy	Precision	Recall	Technique
[59]	95.2	93	93.6	SVM
[60]	84	89	78	NB
[61]	96	98	94	DT
[62]	96.4	95.13	93.59	DBN
[63]	95.86	96.49	95.31	DBN
[64]	91	90	90	ANN
[65]	98.88	94	94.47	SVM
[66]	93.4	93.3	93.4	PCA AND RF
[67]	99	93	86	LR

[68]	89.2	96	95	DBN
[69]	92.41	92.4	92.4	ANN
[70]	93.7	87	94	ANN
[71]	95	95.7	95.7	RF

Conclusion:

Network protection has turned into a question of universal concern in accomplishing upgrades in safety efforts to distinguish and respond against cyber -attacks. The recently utilized ordinary security frameworks are no longer sufficient in light of the fact that those frameworks need of cadency in identifying already concealed and polymorphic assaults. AI procedures are playing a fundamental role in various uses of digital protection frameworks. Our survey here has uncovered a quickly developing interest in AI and network safety in academia and industry has brought about a number of new distributions, especially somewhat recently. In this paper, we have overcome any issues between ML strategies and dangers to PC organizations and portable correspondence by introducing an exhaustive review of the hybrids between the two regions. This overview presents the writing survey on machine learning methods for interruption location, spam discovery, also, malware location on PC organizations and versatile gadget somewhat recently. This chapter examines the use of AI models in the management of organizational well-being over the last decade. There are flaws in every advanced danger that make it difficult to manage such digital assaults, even with the most cutting-edge ML model. Making one proposition for every one of the attacks considering one model is troublesome. Various measures like ID velocity moment involvedness, characterization time to recognize new moreover, “zero-day attacks, and precision of a ML model should be considered while picking a particular model to distinguish a digital assault”. To depicted the fundamentals of organizational security, for instance, the arrangement of digital assaults on PDAs and PCs. Due to the meaning of ML, In this chapter furthermore depicted the basis of simulated intelligence. There are extensive systems in place for a juvenile to obtain superior information around here. We don't know anything about any work that discusses the purposes of ML systems in the advanced protection space on both mobile phones and PC networks in a single paper. This Chapter created a graphical representation of the threats to the web and presented ML strategies to combat these cyber-crimes. We have similarly provided appraisal estimates to evaluate any more tasteful activities. The dataset is outstandingly crucial for the arrangement and taxing of ML models. We have presented a depiction of consistently utilized safekeeping datasets. There is a team of specialists on hand, as well as benchmark datasets for each risk area. AI systems were not essentially expected to work with computerized insurance. By providing opposing data sources, evasion can doom the ML model without a significant stretch. Reliable simulated intelligence is the safeguarded use of computer-based intelligence techniques for the web to give some critical-level rightness guarantees as opposed to the rapidity and correctness of the model. We have furthermore added piece of the critical troubles of using AI techniques in network security as well as given a wide list around here. The referred to hardships merit thought for future investigation.

KEYWORDS

- **Cyber Security**
- **Standards of Cyber Security**
- **Machine Learning**
- **Threats and Vulnerabilities**

REFERENCES

1. ICT Facts and Figures 2017. Available online: https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx (accessed on 9 October 2019).
2. Craigen, D.; Diakun-Thibault, N.; Purse, R. Defining cybersecurity. Technol. Innov. Manag. Rev. 2014, 4, 13–21. [CrossRef]
3. Farahmand, F.; Navathe, S.B.; Enslow, P.H.; Sharp, G.P. Managing vulnerabilities of information systems to security incidents. In Proceedings of the 5th International Conference on Electronic Commerce, Pittsburgh, PA, USA, 30 September–3 October 2003; pp. 348–354.
4. Szor, P. The Art of Computer Virus Research and Defense: ART COMP VIRUS RES DEFENSE _p1; Pearson Education: London, UK, 2005.
5. Firdausi, I.; Erwin, A.; Nugroho, A.S. Analysis of machine learning techniques used in behavior-based malware detection. In Proceedings of the 2010 Second International Conference on Advances in Computing, Control, and Telecommunication Technologies, Jakarta, Indonesia, 2–3 December 2010; pp. 201–203.
6. Michie, D.; Spiegelhalter, D.J.; Taylor, C. Machine learning. Neural Stat. Classif. 1994, 13, 1–298.
7. Shaukat, K.; Nawaz, I.; Zaheer, S. Students Performance: A Data Mining Perspective; LAP Lambert Academic Publishing: Saarbrücken, Germany, 2017.
8. Shaukat, K.; Nawaz, I.; Aslam, S.; Zaheer, S.; Shaukat, U. Student's performance in the context of data mining. In Proceedings of the 2016 19th International Multi-Topic Conference (INMIC), Islamabad, Pakistan, 5–6 December 2016; pp. 1–8.
9. Shaukat, K.; Masood, N.; Mehreen, S.; Azmeen, U. Dengue fever prediction: A data mining problem. J. Data Min. Genom. Proteom. 2015, 2015. [CrossRef]
10. Jusas, V.; Samuvel, S.G. Classification of motor imagery using combination of feature extraction and reduction methods for brain-computer interface. Inf. Technol. Control 2019, 48, 225–234. [CrossRef]
11. Uktveris, T.; Jusas, V. Comparison of feature extraction methods for EEG BCI classification. In Proceedings of the International Conference on Information and Software Technologies, Vilnius, Lithuania, 10–12 October 2015; pp. 81–92. Energies 2020, 13, 2509
12. Shaukat, K.; Rubab, A.; Shehzadi, I.; Iqbal, R. A Socio-Technological analysis of Cyber Crime and Cyber Security in Pakistan. Transylv. Rev. 2017, 1, 84.

13. Canhoto, A.I.; Clear, F. Artificial intelligence and machine learning as business tools: A framework for diagnosing value destruction potential. Bus. Horiz. 2019, 63, 183–193. [CrossRef]
14. Maqsood, H.; Mehmood, I.; Maqsood, M.; Yasir, M.; Afzal, S.; Aadil, F.; Selim, M.M.; Muhammad, K. A local and global event sentiment based efficient stock exchange forecasting using deep learning. Int. J. Inf. Manag. 2020, 50, 432–451. [CrossRef]
15. Dey, S.; Ye, Q.; Sampalli, S. A machine learning based intrusion detection scheme for data fusion in mobile clouds involving heterogeneous client networks. Inf. Fusion 2019, 49, 205–215. [CrossRef]
16. Geluvaraj, B.; Satwik, P.; Kumar, T.A. The future of cybersecurity: Major role of artificial intelligence, machine learning, and deep learning in cyberspace. In International Conference on Computer Networks and Communication Technologies; Springer: Berlin/Heidelberg, Germany, 2018; pp. 739–747.
17. Jain, P. Machine Learning Versus Deep Learning for Malware Detection. Master's Thesis, San Jose State University, San Jose, CA, USA, 2019.
18. Rao, R.S.; Pais, A.R. Detection of phishing websites using an efficient feature-based machine learning framework. Neural Comput. Appl. 2019, 31, 3851–3873. [CrossRef]
19. Alauthman, M.; Almomani, A.; Alweshah, M.; Omoushd, W.; Alieyane, K. Machine Learning for phishing Detection and Mitigation. Mach. Learn. Comput. Cyber Secur. Princ. Algorithmsand Pract. 2019, 26, 48–74.
20. Alurkar, A.A.; Ranade, S.B.; Joshi, S.V.; Ranade, S.S.; Shinde, G.R.; Sonewar, P.A.; Mahalle, P.N. A Comparative Analysis and Discussion of Email Spam Classification Methods Using Machine Learning Techniques. In Applied Machine Learning for Smart Data Analysis; CRC Press: Boca Raton, FL, USA, 2019; p. 185.
21. Dada, E.G.; Bassi, J.S.; Chiroma, H.; Adetunmbi, A.O.; Ajibuwa, O.E. Machine learning for email spam filtering: Review, approaches and open research problems. Heliyon 2019, 5, e01802. [CrossRef] [PubMed]
22. Shukur, H.A.; Kurnaz, S. Credit Card Fraud Detection Using Machine Learning Methodology. Int. J. Comput. Sci. Mob. Comput. 2019, 8, 257–260.
23. Afek, Y.; Bremler-Barr, A.; Feibish, S.L. Zero-day signature extraction for high- volume attacks. IEEE/ACM Trans. Netw. 2019, 27, 691–706. [CrossRef]
24. Saad, S.; Briguglio, W.; Elmiligi, H. The Curious Case of Machine Learning In Malware Detection. arXiv 2019, arXiv:1905.07573.
25. . Ambalavanan, V. Cyber Threats Detection and Mitigation Using Machine Learning. In Handbook of Research on Machine and Deep Learning Applications for Cyber Security; IGI Global: Hershey, PA, USA, 2020; pp. 132–149.
26. Shah, N.F.; Kumar, P. A comparative analysis of various spam classifications. InProgress in Intelligent Computing Techniques: Theory, Practice, and Applications; Springer: Berlin/Heidelberg, Germany, 2018; pp. 265–271.
27. Chandrasekar, C.; Priyatharsini, P. Classification techniques using spam filtering email. Int. J. Adv. Res. Comput. Sci. 2018, 9, 402. [CrossRef]
28. Shafi'I, M.A.; Latiff, M.S.A.; Chiroma, H.; Osho, O.; Abdul-Salaam, G.; Abubakar, A.I.; Herawan, T. A review on mobile SMS spam filtering techniques. IEEE Access 2017, 5, 15650–15666.
29. Chen, C.; Zhang, J.; Xie, Y.; Xiang, Y.; Zhou, W.; Hassan, M.M.; AlElaiwi, A.; Alrubaian, M. A performance evaluation of machine learning-based streaming spam tweets detection. IEEE Trans. Comput. Soc. Syst. 2015, 2, 65–76. [CrossRef]
30. Biggio, B.; Fumera, G.; Pillai, I.; Roli, F. A survey and experimental evaluation of image spam filtering techniques. Pattern Recognit. Lett. 2011, 32, 1436–1446. [CrossRef]
31. Kumar, A.D.; KP, S. DeepImageSpam: Deep Learning based Image Spam Detection. arXiv 2018, arXiv:1810.03977.
32. Jusas, V.; Japertas, S.; Baksys, T.; Bhandari, S. Logical filter approach for early stage

cyber-attack detection. Comput. Sci. Inf. Syst. 2019, 16, 491–514. [CrossRef]
33. Jordan, M.I., Mitchell, T.M.: Machine learning: Trends, perspectives, and prospects. Science(80-.) 349(6245), 255–260 (2015)
34. Fraley, J.B., Cannady, J.: The promise of machine learning in cybersecurity. SoutheastCon 2017, 1–6 (2017)
35. Alazab, M., Tang, M.: Deep Learning Applications for Cyber Security. Springer, Heidelberg(2019)
36. Li, J.: Cyber security meets artificial intelligence: a survey. Front. Inf. Technol. Electron.Eng. 19(12), 1462–1474 (2018)
37. McNeil, N., Bridges, R.A., Iannacone, M.D., Czejdo, B., Perez, N., Goodall, J.R.: Pace: pattern accurate computationally efficient bootstrapping for timely discovery of cybersecurity concepts. In: 2013 12th International Conference on Machine Learning and Applications, vol. 2, pp. 60–65 (2013)
38. Zhang, Q., Man, D., Yang, W.: Using HMM for intent recognition in cyber security situation awareness. In: 2009 Second International Symposium on KnowledgeAcquisition and Modeling, vol. 2, pp. 166–169 (2009)
39. Alhashmi, S.F.S., Salloum, S.A., Abdallah, S.: Critical success factors for implementing artificial intelligence (AI) projects in Dubai government United Arab Emirates (UAE) health sector: applying the extended technology acceptance model (TAM). In: International Conference on Advanced Intelligent Systems and Informatics, pp. 393– 405 (2019)
40. Pacheco, A.G.C., Ali, A.-R., Trappenberg, T.: Skin cancer detection based on deep learning and entropy to detect outlier samples (2019). arXiv Prepr. arXiv:1909.04525 Salloum, S.A., Al-Emran, M., Monem, A., Shaalan, K.: A survey of text mining in social media: facebook and twitter perspectives. Adv. Sci. Technol. Eng. Syst. J. 2(1), 127–133(2017)
41. Salloum, S.A., Al-Emran, M., Monem, A., Shaalan, K.: A survey of text mining in social media: facebook and twitter perspectives. Adv. Sci. Technol. Eng. Syst. J. 2(1), 127–133 (2017)
42. Salloum, S.A., Mhamdi, C., Al-Emran, M., Shaalan, K.: Analysis and classification of Arabic newspapers' facebook pages using text mining techniques. Int. J. Inf. Technol. Lang.Stud. 1(2), 8–17 (2017)
43. Amodei, D., Olah, C., Steinhardt, J., Christiano, P., Schulman, J., Mané, D.: Concrete problems in AI safety (2016). arXiv Prepr. arXiv:1606.0656544. Papernot, N., McDaniel, P., Sinha, A., Wellman, M.: Towards the science of security and privacy in machine learning (2016). arXiv Prepr. arXiv:1611.03814
44. Papernot, N., McDaniel, P., Sinha, A., Wellman, M.: Towards the science of security and privacy in machine learning (2016). arXiv Prepr. arXiv:1611.03814
45. Xin, Y., et al.: Machine learning and deep learning methods for cybersecurity. IEEE Access 6, 35365–35381 (2018)
46. Liu, Q., Li, P., Zhao, W., Cai, W., Yu, S., Leung, V.C.M.: A survey on security threats and defensive techniques of machine learning: a data driven view. IEEE Access 6, 12103–12117(2018)
47. Md. Faisal Khana and B. L. Ranab ," Detection of Phishing Websites Using Deep Learning Techniques", Turkish Journal of Computer and Mathematics Education, Vol.12 No.10 (2021), 3880-3892 April 2021.
48. Sriram Srinivasana, Vinayakumar Rb, Ajay Arunachalamc, Mamoun Alazabd,"Malicious URL Detection using Deep Learning", Published by Springer, Cham, DOI no:https://doi.org/10.1007/978-3-030-62582-5_21,January2021.
49. Alper Ozcan1,2 • Cagatay Catal3 • Emrah Donmez4 • Behcet Senturk5," A hybrid DNN–LSTM model for detecting phishing URLs", Neural Computing and Applications, https://doi.org/10.1007/s00521-021-06401-z, part of Springer Nature 2021

50. Pranav Maneriker∗ , Jack W. Stokes, Edir Garcia Lazo,"URLTran:Improving Phishing URLDetection Using Transformers", arXiv preprint arXiv:2106.05256 (2021).
51. Zhiqiang Wang, Xiaorui Ren,Shuhao Li,1 Bingyan Wang, Jianyi Zhang ,"A Malicious URL Detection Model Based on Convolutional Neural Network", Published in: Hindawi Security and Communication Networks ,Volume 2021, Article ID 5518528, 12 pages https://doi.org/10.1155/2021/5518528, ; Published 15 May 2021.
52. Abdul Basit1 · Maham Zafar1 · Xuan Liu2 · Abdul Rehman Javed3 · Zunera Jalil3 · Kashif Kifayat3, "A comprehensive survey of AI-enabled phishing attacks detection techniques",Published in:-Telecommunication Systems, https://doi.org/10.1007/s11235-020- 00733-2, Published online: 23 October 2020.
53. M. A. Adebowale, K. T. Lwin, M. A. Hossain," Intelligent Phishing Detection Scheme Algorithms Using Deep Learning"Published in:,Journal of Enterprise Information Management, ISSN: 1741-0398, DOI:https://doi.org/10.1108/JEIM-01-2020-0036 May 2020.
54. Preeti,Rainu Nandal,Kamldeep Joshi,"Phishing URL Detection Using Machine Learning",published by Advances in Communication and Computational Technology , pp 547-560, Springer 2020,DOI: https://doi.org/10.1007/978-981-15-5341-7_42.
55. A S S V Lakshmi Pooja1, Sridhar.M2," Analysis of Phishing Website Detection Using CNN and Bidirectional LSTM" Published in: 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA), IEEE 2020,DOI: 10.1109/ICECA49313.2020.9297395.
56. Ping Yi, ,1 Yuxiang Guan,1 Futai Zou,1 Yao Yao,2 WeiWang,2 and Ting Zhu," Web Phishing Detection Using a Deep Learning Framework", published in Wireless Communications and Mobile Computing,Volume 2018, https://doi.org/10.1155/2018/4678746.
57. Hiransha M, Nidhin A Unnithan, Vinayakumar R, Soman KP," Deep Learning Based Phishing E-mail Detection",2018,CEUR-WS.ORG/VOL-2124.
58. Waleed Ali," Phishing Website Detection based on Supervised Machine Learning with Wrapper Features Selection", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 9, 2017.
59. C. Chen, J. Zhang,Y. Xie,Y. Xiang,W. Zhou, M. M. Hassan, A. AlElaiwi,and M. Alrubaian, ``A performance evaluation of machine learning-based streaming spam tweets detection,'' IEEE Trans. Comput. Social Syst.,vol. 2, no. 3, pp. 65_76, Sep. 2015.
60. D. K. Renuka, P. Visalakshi, and T. Sankar, ``Improving E-mail spamclassi_cation using ant colony optimization algorithm,'' Int. J. Comput. Appl., pp. 22_26, Jan. 2015.
61. Z. Khan and U. Qamar, ``Text mining approach to detect spam in emails,'' in Proc. Int. Conf. Innov. Intell. Syst. Comput. Technol. (ICIISCT), 2016,p. 45.
62. I. J. Alkaht and B. Al Khatib, ``Filtering SPAMusing several stages neural networks,'' Int. Rev. Comput. Softw., vol. 11, no. 2, p. 123, Feb. 2016.
63. A. Tyagi, ``Content based spam classi_cation_A deep learning approach,'' M.S. thesis, Dept. Comput. Sci., Univ. Calgary, Calgary, AB,Canada, 2016.
64. W.-H. Chen, S.-H. Hsu, and H.-P. Shen, ``Application of SVM and ANN for intrusion detection,'' Comput. Oper. Res., vol. 32, no. 10,pp. 2617_2634, Oct. 2005.
65. R. Sagar, R. Jhaveri, and C. Borrego, ``Applications in security and evasions in machine learning: A survey,'' Electronics, vol. 9, no. 1, p. 97,Jan. 2020
66. T. Gangavarapu, C. Jaidhar, and B. Chanduka, ``Applicability of machine learning in spam and phishing email _ltering: Review and approaches,'' Artif. Intell. Rev., vol. 53, pp. 1_63, Feb. 2020.
67. L. GuangJun, S. Nazir, H. U. Khan, and A. U. Haq, ``Spam detection approach for secure mobile message communication using machine learning algorithms,'' Secur.

Commun. Netw., vol. 2020, pp. 1_6,Jul. 2020.
68. T. Zaki, M. S. Uddin, M. M. Hasan, and M. N. Islam, ``Security threats for big data: A study on enron e-mail dataset," in Proc. Int. Conf. Res. Innov. Inf. Syst. (ICRIIS), Jul. 2017, pp. 1_6.
69. M. Bassiouni, M. Ali, and E. A. El-Dahshan, ``Ham and spam e-mailsclassi_cation using machine learning techniques," J. Appl. Secur. Res.,vol. 13, no. 3, pp. 315_331, Jul. 2018.
70. M. Soranamageswari and C. Meena, ``A novel approach towards image spam classi_cation," Int. J. Comput. Eng., vol. 3, no. 1, p. 84, 2011.
71. M. Mccord and M. Chuah, ``Spam detection on Twitter using traditionalclassi_ers," in Proc. Int. Conf. Autonomic Trusted Comput. Berlin,Germany: Springer, 2011, pp. 175_186.