International Journal of Research in Engineering, Science and Management
Volume 7, Issue 3, March 2024
https://www.ijresm.com | ISSN (Online): 2581-5792

A Review on Cyber Security and Machine Learning: Advantages, Challenges

Navjot Singh[1*], Deepika Jain[2]
[1,2]*Assistant Professor, Department of Electronics and Communication Engineering, Malout Institute of Management and Information Technology, Malout, Punjab, India*

***Abstract*: Machine learning is a subset of Computerized reasoning (simulated intelligence), which centers around the execution of certain frameworks that can gain from the verifiable information, recognize examples and pursue consistent choices with next to zero human intercessions. Network protection is the act of safeguarding advanced frameworks, like PCs, servers, cell phones, organizations and related information from vindictive assaults. Joining network protection and ML has two significant angles, to be specific representing network safety where the AI is applied, and the utilization of AI for empowering network protection. This joining can help us in different ways, similar to it gives upgraded security to the AI models, works on the exhibition of the network safety strategies, and supports compelling discovery of multi day assaults with less human mediation. In this review paper, we examine around two distinct ideas by joining digital protection and ML. We likewise examine the benefits, issues and difficulties of joining network safety and ML. Besides, we examine the different assaults and give an extensive near investigation of different procedures in two different thought about classes.**

***Keywords*: Cyber Security, Machine Learning, Internet of Things (IoT), Privacy, Security, Intrusion detection.**

1. Introduction

In this era of computing, most devices that we use are connected to the Internet in an Internet of Things (IoT). These types of devices share and transmit their data through the open communication medium, also called as the Internet. Mostly this data is sensitive in nature. The various entities, such as the online hackers are always in search of that, where it plays with the things (for example, they can launch attacks, like replay, man-in-the-middle, credential guessing, malware injection and data modification) [1], [2]. Therefore, from time-to-time several researchers propose different security protocols to mitigate these attacks. The security protocols or cyber security protocols can be divided into different categories: "authentication protocols", "access control protocols", "intrusion detection protocols", "key management protocols", and "blockchain enabled security protocols". The summary of these protocols is given below.

Authentication protocols: Authentication is a process of genuineness (authenticity) of someone of some device. It can perform through some credentials or factors (i.e., username, password, biometrics), these are closely associated to the users or device. We can have system to system authentication, user to device authentication or device to authentication. On the basis of available factors, user authentication protocols can be again divided into three categories, i.e., one-factor user authentication protocol, two-factor user authentication protocol and three-factor user authentication protocol.

Access control protocols: Access control is a technique of putting restrictions on the unauthorized access of someone or some device(s). Users can access the other users or devices in a secured manner after the completion of all steps of a user/device access control protocol. Access control protocol can be divided into two categories: (1) user access control and (2) device access control. User access control protocol can use for the access control of the unauthorized clients, whereas device access control protocol can be used for the access control of the unauthorized devices. It determines who is authorized to access a resource and who is not.

Access to a resource is determined by who has permission to use it. A permission system determines who has access to a particular resource and who does not. This determines who is permitted to access a particular resource. Permission is required in order to access a resource.

Intrusion detection protocols: These days, machine learning or deep learning-based intrusion detection (i.e., malware detection) is very popular. Intrusion detection based on machine learning (i.e., malware detection) has become very popular these days. Nowadays, machine learning (e.g., malware detection) is becoming very popular. Through the essential steps of an authenticated key agreement protocol, the devices/users may exchange their information in a secure manner after establishing a shared secret key (i.e., a session key). In an authenticated key agreement protocol, the devices and users exchange information in a secure manner after the establishment of a shared secret key (i.e., a session key).

It is possible for the devices/users to exchange their information in a secure manner after the creation of a shared secret key.

The systems, which are connected in the cyber space, are prone to various kind of attacks i.e., replay, man-in-the-middle (MiTM), impersonation, credentials leakage, password guessing, session key leakage, unauthorized data update, malware injection, flooding, denial of service (DoS) and

*Corresponding author: navjotmimit@gmail.com

distributed denial of service (DDoS) and many more. Therefore, we need some security protocol to detect and mitigate these attacks. The machine learning models (machine learning ML algorithms) can learn about various cyber-attacks in the offline/online mode through the provided pre-processed dataset. The ML algorithms detect any sign of intrusion (some cyber-attack) in the real time i.e., online mode. The scenario of "machine learning in cyber security" is depicted in Fig. 1. Here, we have an Internet connected system (i.e., laptops, desktops, smartphones, IoT devices), which can be used to perform various online tasks i.e., online financial transactions, online access of healthcare data, social security numbers, etc. Hackers are always in search of some vulnerabilities in such systems and if they get anything like that then they start their attacks. For the detection and mitigation of cyber-attacks, different kinds of ML techniques i.e., supervised learning, un- supervised learning, reinforcement learning and deep learning can be used as per the situation. It is up-to the communication environment and available resources of the systems, which technique (i.e., supervised learning, unsupervised learning, reinforcement learning and deep learning) suites them in the best way. The learning (training) and prediction (testing) of cyber-attacks can be done through the cloud servers as they have good computation and storage resources.

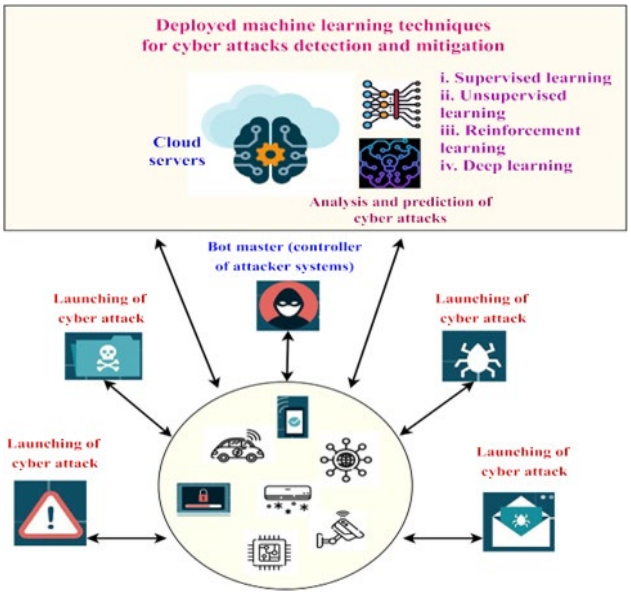

Fig. 1. Scenario of machine learning in cyber security

A. Cyber Security in Machine Learning

The scenario of "cyber security in machine learning" is given in Fig. 2, which is also referred to machine learning.

The ML techniques are used for the analysis and prediction of no. of concepts. So, the performance of ML techniques can be pompous through the launching of some attacks i.e., dataset poisoning attack, model poisoning attack, privacy breach attack, membership inference attacks, runtime disruption attack, etc., [6]. These attacks may lead to the inaccurate predictions about the associated. The model poisoning attack aims to corrupt the models by interfering with their internal workings and modifying their parameters The privacy breach attack aims to expose sensitive data to retrieve it. prediction.

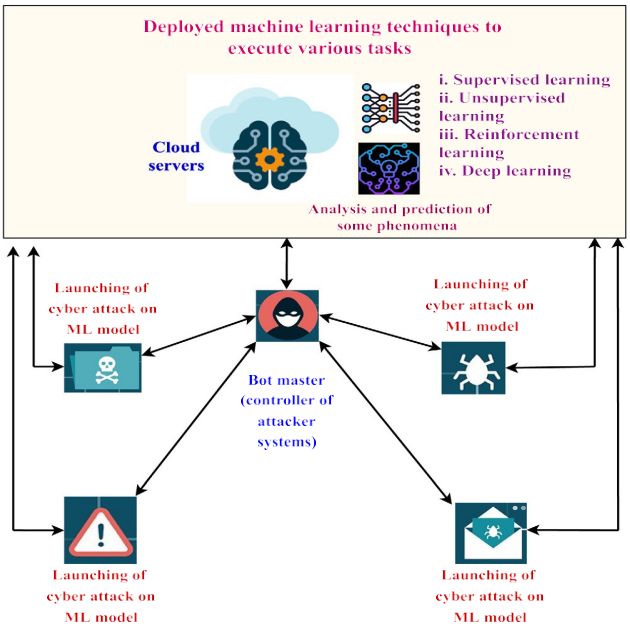

Fig. 2. Scenario of cyber security in machine learning

2. Advantages of Uniting Cyber Security and ML

Both digital protection and ML are fundamental for one another and can work on their common exhibitions. A portion of the upsides of their joining are as per the following. As examined before, the ML models are defenseless against different assaults. The happen of these assaults might influence the working, execution and forecasts of the ML models. Nonetheless, these undesirable frequencies can be gotten through the sending of certain network protection instruments. Under the organization of digital protection systems, the working and execution and the information datasets of the ML models become gotten and we get the right expectations and results [7].

Further developed execution of network safety strategies: At the point when we utilize the ML calculations in the network safety plans. (i.e., interruption identification frameworks) that work on their performances (i.e., further developed precision and discovery rate with less bogus positive rate). ML methods, as administered mastering, unaided learning, support learning and profound learning calculations can be utilized according to the correspondence climate and the related frameworks.

Effective detection of zero-day attacks: The cyber security methods, which detect the intrusion through the ML models seem very effective for the detect of zero-day attacks (i.e., unknown malware attacks). It happens because they per- form the detection with the help of some deployed ML models. The ML models work through collection and matching of certain features, if the features of a program match with the malicious program's features, then that can the malicious program.

Limited requirements of human intervention: Mostly the task in the Machine learning based systems occur through the deployed ML techniques. When we unit cyber security with ML, most of the tasks for which these systems are deployed, they do that without any human involvement or with very less

human intervention.

Scanning and mitigation: The ML based intrusion systems work very quickly to detect the presence

of the attacks because they work through certain ML algorithms. Therefore, uniting of ML with the cyber security systems performs the scanning of intrusions very fast and provide fast response in case of any sign of intrusion. The main thing that needed to take care is the suitable ML algorithm selection.

3. Overview of Various Threats and Attacks

- In this segment, we give the subtleties of the accompanying different assaults, which might happen in various registering environments.
- Listening in: This assault is uninvolved in nature which is otherwise called sniffing or sneaking around assault. In this assault.
- An enemy attempt to listen the mysterious discussion of the conveying parties.
- Traffic examination: This assault is detached in nature.
- In this assault, an enemy A captures the continuous discussion and afterward looks at the messages to get data like sort of discussion, its example and conduct, area following and timing of data. The caught information further aides A to send off other related assaults.
- Man-in-the-middle attack (MiTM): In this dynamic assault, A makes free associations with conveying substances what's more, transfers the messages to the two finishes. Under such situations, the two conveying substances believe that they are directly speaking with one another. In this way, A may block, erase, change or supplement another data for transmission with next to no acknowledgment [8].
- Impersonation attack: This assault is likewise dynamic in nature, wherein A mimics one of the real party of the organization by concluding its character and afterward sends the changed or a new messages for the sake that party to the next real party.
- Denial-of-Service (DoS) attack: In DoS attack, A sends various phony solicitations (i.e., HTTP flood messages) to flood the casualty's registering assets. Accordingly, the help solicitation of the authentic client can't be handled. Under such circumstance, the authentic client can't get the help of the organization. There is one more type of DoS assault, which is known as conveyed forswearing of-administration (DDoS) assault in which A purposes numerous machines (i.e., botnet) to send multiple eques simultaneously to the victim’s machine that consumes all computing resources of the system and that happens very fast. DoS or DDoS attacks can be performed through various flooding attacks i.e., SYN flood, HTTP flood, UDP flood, etc.
- Scripting attack: These assaults allude to the divulgence of data from some web-based data set, which are principal with some web server (i.e., internet banking data set). For instance, "secret word breaking, organized question language (SQL) infusion assault and cross-site prearranging (XSS) assault" can be utilized to get the privileged data from the framework, similar to passwords, credit and charge card subtleties.
- Privileged insider attack: This assault is performed by any favored client of the framework, who approaches the enlistment data of different clients and gadgets. Since favored insider approaches the delicate data, this assault turns into significantly more enthusiastically to guard and furthermore has more unfriendly effect.
- Physical stealing of smart devices: These days the greater part of the figuring conditions are worked using shrewd gadgets, like savvy home machines, shrewd medical services gadgets, brilliant assembling gadgets. The savvy gadgets are conveyed with no actual security. On the off chance that these shrewd gadgets are genuinely taken by a foe A, they can be utilized for the extraction of delicate data by utilizing power investigation assaults. After the extraction of delicate data, the unapproved undertakings like unlawful meeting key calculation can be performed [9].
- Birthday attack: A birthday assault is a kind of cryptographic assaults that exploits the mathematics behind the birthday issue, which might be tracked down in a likelihood hypothesis. The birthday assaults can be utilized for the pernicious purposes, like speculating accreditations (passwords). As depicted in the birthday conundrum, this assault depends on a proper level of stages and the higher chance of impacts recognized between irregular assault endeavors. The birthday Catch 22 (birthday issue) addresses the probability that a few matched individuals in a gathering of n haphazardly chose individuals will share a birth date. The math behind this issue enlivened the birthday assault, a notable crypto-realistic assault, that utilizes this probabilistic technique to diminish the trouble of breaking a hash capability [10].
- Stolen verifier attack: In this noxious demonstration, an aggressor first attempts to take a few gadgets (i.e., savvy IoT gadgets) and then plays out a power examination assault on the memory units of these gadgets to separate delicate data (i.e., secret credentials and keys) from their memory. The assailant listens in a portion of the traded messages and afterward utilizes the removed data to send off other expected assaults in the organization, as unapproved meeting key calculation, secret word speculating, MiTM and pantomime assaults.
- Unauthorized session key computation attack: In this malicious act, an assailant attempts to figure the meeting key, which is laid out between the authentic substances of the organization. To play out this undertaking, the aggressor attempts different techniques, for example, actual gadget taken assault, favored insider assault and taken verifier assault. It is constantly prescribed to utilize the drawn-out mysteries (i.e., pseudo personalities, secret keys) and transient insider facts (i.e., arbitrary mystery nonce values) for the calculation of the meeting keys. This component gives particular keys in various meetings among various elements. Sadly, on the off chance that a meeting key is uncovered to the assailant, other meeting keys will be in safe

hand, and it will give the security to the leftover piece of the correspondence.

- Attacks on machine learning models: We can extensively ordered the assaults on ML model into four classifications: (a) dataset harming assault, (b) model harming assault, (c) privacy break assault and (d) runtime interruption assault [11].
- Dataset poising attack: In this attack, A uses the different methods to invade the training and testing data to affect the normal functioning of the ML task. A can use adversarial examples to attack the data server from where raw data has to be extracted. The compromising of the data sources helps to inserts the erroneous data, which possibly alters the functioning of the ML model. These further changes the output of the ML based system [12].
- Model poisoning attack: In model harming assault, A does boundary change through which A creates flawed yield by means of impeding the classifier. The boundaries through which the classifier plans ML model get modified. A can change responsiveness limits, pace of promotion and cause under-fitting or over-fitting that further influences the typical execution of ML task [13].
- Privacy breach: The client's touchy information and model's interior working component can be compromised through different techniques. The unprotected documents and nonattendance of encryption component in the preparation and sending periods of the ML assignment can cause the spilling of information. That further empowers the unauthorized user to interfere with the model. It increases the privacy risks associated with the data as the privacy of the sensitive data may be breached [14]. Papernot et al. [15,16] discussed the different privacy preserving schemes to protect the privacy of model. They also discussed about the usage of noise generation to provide differential privacy to the data and ML model by "randomizing model's behavior" [17].

4. Issues and challenges of uniting of cyber security and machine learning

Though uniting of cyber security and machine learning provides enormous number of advantages. At the same time it has some issues and challenges, which need to be handled very carefully. Some of them are discussed below.

Compatibility issues: The uniting of cyber security and machine learning contains different types of security techniques (i.e., encryption algorithms, signature generation and verification algorithms, hashing algorithms) and machine learning algorithms (clustering, classification, convolutional neural networks (CNNs)). Moreover, the data, which is the main input for analysis process comes from the different sources i.e., IoT devices. These IoT devices are operated through different communication techniques. During the amalgamation of these many algorithms, there may be the issues related to the compatibility. Therefore, we have to very selective, which algorithm works well with which algorithm and scheme. Hence compatibility related issues should be handled very carefully [18].

Overloading: In uniting cyber security and machine learning, we use various algorithms as discussed earlier. For the execution of such algorithms, we need the resources in extra amount. Otherwise, the system will not work properly. Therefore, the amalgamation and use of various algorithms may cause the overloading to the system that may further affect the actual working of the system. For example, we cannot allocate entire resources of the system for the security related processes. We also need some resources for the execution of ML-related tasks. Hence, we should select the algorithms wisely and as per the resources of the communication environment. For example, for an encryption purpose, we would prefer to use the symmetric-key based encryption, known as the Advanced Encryption Standard (AES) algorithm in place of any public key cryptographic algorithm for the secure communication of IoT, since AES requires less computation, communication and storage costs as compared to public key cryptographic algorithms. In that situation, we can also allocate the resources of the system for the execution of important tasks.

Accuracy: In the joining of network protection and AI, we utilize different ML systems i.e., machine learning (ML) models to foresee about a few actual peculiarities (i.e., chances of side of the road mishap in the clever transportation framework). The ML models work with the assistance of certain datasets, assuming that we have some mistake in the dataset or in the settings of the ML model then this can give enormous difficulty. For instance, the acquired precision isn't completely right [19].

Flaws in security mechanisms: In the joining of network protection and ML, we might utilize different digital protection mechanisms. On the off chance that these components have a few defects, it might bring the hardship to the security to the framework. More often than not, the programmers attempt to look for the zero-day weaknesses and afterward exploit them. In such circumstances, the touchy information of the framework might be uncovered, changed or it might become inaccessible. Hence, the creators of the security conventions ought to must be extremely cautious while they plan another security convention. The security of the recently planned convention can be tried through specific components, similar to the Robotized Approval of Web Security Conventions and Applications (AVISPA) [20], which really looks at the security of the convention against the replay and man-in-the-middle attacks through the formal security verification. Moreover, we can also go for the "Burrows–Abadi–Needham (BAN) logic test [21], which identifies the possibility of "secure mutual authentication among the communicating entities". Apart from these, we can also analysis the formal security of a security protocol through the Real-or-Random (ROR) model [22] implementation, which identifies the possibility of unauthorized session key computation attack on the designed authentication or access control or key management protocol. The security of the designed protocol can be evaluated and analyzed in this way.

5. Future Research

In this part, we examine a portion representing things to come research directions of the "joining of digital protection and AI", which ought to be viewed as by the specialists working in a similar space.

Mystery of traded and put away information: Mystery of the traded and put away information matters a great deal. To keep up with the mystery of the information various kinds of safety conventions have been proposed. Be that as it may, these conventions flop in the event of any blemish in the plan or because of the occurrence of around multi day assault. Accordingly, there is some extent of enhancements as online attackers (hackers) are going advance and use advance tools to break the security of the system. Hence, there is a requirement of new security protocols with additional security and functionality features, which can resist the zero-day vulnerabilities as well.

Compatibility of different mechanisms and tools: The "joining of network safety and ML" utilizes different systems what's more, devices (i.e., various kinds of safety methods. like encryption calculations, signature age and confirmation calculations, hashing calculations and AI algo-rithms, like grouping, order, CNNs). They additionally require different sort of equipment and arrangements. Under such conditions, there might be a few issues connected with the similarity of these systems and devices.

Overloading and performance: In the joining of network safety and ML, we utilize different calculations as examined prior. For the execution of these numerous calculations, we really want a few additional assets. If not, the undertakings won't be executed appropriately. In this way, combination and utilization of different calculations might make the over-burdening the framework that might additionally influence the real working of the framework. Thus, we ought to choose the calculations astutely and attempt to develop new lightweight calculations might be in ML or in the security, which consume less assets of the frameworks.

Improvement in accuracy of the system: The ML models work with the assistance of certain datasets, in the event that we have some mistake in the dataset or in the settings of the ML model then this can create issues. For instance, the got exactness isn't completely right or the situation might make wrong expectation about something. Subsequently, the analysts ought to attempt to defeat from such circumstances, new techniques can be designed to recognize the blunders in the datasets or to work on the precision of the frameworks.

Lesson learned: We examined around two unique ideas by joining network protection and ML. We then examined the benefits, issues and difficulties of joining network protection and ML. A portion of the benefits are as per the following: "full confirmation security of ML models", "further developed execution of network protection strategies", "effective location of multi day assaults" and "speedy filtering and relief". Notwithstanding, this joining additionally has a few issues and difficulties, similar to "similarity issues", "over-burdening", "accu-shocking", and so on. Moreover, we talked about different assaults of the space (i.e., listening in, rush hour gridlock examination, replay, MiTM, pantomime, DoS, malware addition, prearranging, birthday, actual taking of savvy gadgets, word reference, dataset balancing, model harming and runtime disturbance assaults. From that point forward, we gave a complete near investigation of different methods in two different thought about classes. For test, the plan of Kumar et al. [23] performed better under the classification of "AI in digital protection", though the plan of Chen et al. [32] performed better under the classification of "digital protection in ML". Some future examination headings (i.e., "mystery of traded and put away information", "compatibility of various instruments and devices", "over-burdening and performance" and "improvement in accuracy of the system") were also given so that other researchers could provide some solutions for those. Thus, there is a trade-off between the learning cost and performance. For example, DL is costlier than ML, however, it attains good predictive scores. Moreover, if we want to put more security, we need to invest more on the system resources.

6. Conclusion

We introduced the subtleties of two distinct ideas by uniting of network protection and machine inclining: "AI in network safety" and "network safety in AI". We then, at that point, talked about the benefits, issues and difficulties of joining of digital protection and ML. Further, we featured the various assaults and furthermore gave a near investigation of different strategies in two different thought about classes. At last, some future exploration headings are given.

References

[1] I. Butun, P. Osterberg, H. Song, Security of the internet of things: Vulnerabilities, attacks, and countermeasures, IEEE Commun. Surv. Tutor. 22 (1) (2020) 616–644.

[2] Z. Lv, L. Qiao, J. Li, H. Song, Deep-learning-enabled security issues in the internet of things, IEEE Internet Things J. 8 (12) (2021) 9531–9538.

[3] Y. Wang, J. Yu, B. Yan, G. Wang, Z. Shan, BSV-PAGS: Blockchain-based special vehicles priority access guarantee scheme, Comput. Commun. 161 (2020) 28–40.

[4] N. Magaia, R. Fonseca, K. Muhammad, A.H.F.N. Segundo, A.V. Lira Neto, V.H.C. de Albuquerque, Industrial internet-of-things security enhanced with deep learning approaches for smart cities, IEEE Internet Things J. 8 (8) (2021) 6393–6405.

[5] S.A. Parah, J.A. Kaw, P. Bellavista, N.A. Loan, G.M. Bhat, K. Muhammad, V.H.C. de Albuquerque, Efficient security and authentication for edge-based internet of medical things, IEEE Internet Things, J. 8 (21) (2021) 15652–15662.

[6] Y. Sun, A.K. Bashir, U. Tariq, F. Xiao, Effective malware detection scheme based on classified behavior graph in IIoT, Ad Hoc Netw. 120 (2021) 102558.

[7] J. Yang, Z. Bian, J. Liu, B. Jiang, W. Lu, X. Gao, H. Song, "No Reference Quality Assessment for Screen Content Images Using Stacked Autoencoders in Pictorial and Textual Regions."

[8] Y. Zhao, J. Yang, Y. Bao, H. Song, Trustworthy authorization method for security in industrial internet of things, Ad Hoc Netw. 121 (C) (2021).

[9] T.S. Messerges, E.A. Dabbish, R.H. Sloan, Examining smart-card security under the threat of power analysis attacks, IEEE Trans. Comput. 51 (5) (2002) 541–552.

[10] M.R.K. Soltanian, I.S. Amiri, Chapter 3 - problem solving, investi- gating ideas, and solutions, in: M.R.K. Soltanian, I.S. Amiri (Eds.), Theoretical and Experimental Methods for Defending Against DDOS Attacks, Syngress, 2016, pp. 33–45.

[11] T. Lei, Z. Qin, Z. Wang, Q. Li, D. Ye, EveDroid: Event-aware android malware detection against model degrading for IoT devices, IEEE Internet Things J. 6 (4) (2019) 6668–6680.
[12] J. Steinhardt, P.W. Koh, P. Liang, Certified defenses for data poisoning attacks, in: 31st International Conference on Neural Information Processing Systems, in: NIPS'17, Curran Associates Inc. Long Beach, California, USA, 2017, pp. 3520–3532.
[13] M. Aladag, F.O. Catak, E. Gul, Preventing data poisoning attacks by using generative models, in: 1st International Informatics and Software Engineering Conference, UBMYK, Ankara, Turkey, 2019, pp. 1–5.
[14] C. Huang, S. Chen, Y. Zhang, W. Zhou, J.J.P.C. Rodrigues, V.H.C. de Albuquerque, A robust approach for privacy data protection: IoT security assurance using generative adversarial imitation learning, IEEE Internet Things J. (2021) 1.
[15] N. Papernot, P. McDaniel, X. Wu, S. Jha, A. Swami, Distillation as a defense to adversarial perturbations against deep neural networks, in: 2016 IEEE Symposium on Security and Privacy, 2016, pp. 582–597.
[16] N. Papernot, A marauder's map of security and privacy in machine learning, in: 11th ACM Workshop on Artificial Intelligence and Security, Toronto, Canada, 2018.
[17] S. Pirbhulal, W. Wu, K. Muhammad, I. Mehmood, G. Li, V.H.C. de Albuquerque, Mobility enabled security for optimizing IoT based intelligent applications, IEEE Netw. 34 (2) (2020) 72–77.
[18] J. Yang, Y. Han, Y. Wang, B. Jiang, Z. Lv, H. Song, Optimization of real-time traffic network assignment based on IoT data using DBN and clustering model in smart city, Future Gener. Comput. Syst. 108 (2020) 976–986.
[19] R.R. Guimaraes, L.A. Passos, R.H. Filho, V.H.C.d. Albuquerque, J.J.P.C. Rodrigues, M.M. Komarov, J.P. Papa, Intelligent network security monitoring based on optimum-path forest clustering, IEEE Netw. 33 (2) (2019) 126–131.
[20] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P.H. Drielsma, P.C. Heám, O. Kouchnarenko, J. Mantovani, S. Mödersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Viganò, L. Vigneron, The AVISPA tool for the automated validation of internet security protocols and applications, in: K. Etessami, S.K. Rajamani (Eds.), Computer Aided Verification, Springer Berlin Heidelberg, Berlin, Heidelberg, 2005, pp. 281–285.
[21] M. Burrows, M. Abadi, R. Needham, A logic of authentication, ACM Trans. Comput. Syst. 8 (1) (1990) 18–36.
[22] M. Abdalla, P.A. Fouque, D. Pointcheval, Password-based authenti- cated key exchange in the three-party setting, in: 8th International Workshop on Theory and Practice in Public Key Cryptography, PKC'05, in: Lecture Notes in Computer Science, vol. 3386, Les Diablerets, Switzerland, 2005, pp. 65–84.
[23] R. Kumar, X. Zhang, W. Wang, R.U. Khan, J. Kumar, A. Sharif, A multimodal malware detection technique for android IoT devices using various features, IEEE Access 7 (2019) 64411–64430.
[24] H.-T. Nguyen, Q.-D. Ngo, V.-H. Le, IoT botnet detection approach based on PSI graph and DGCNN classifier, in: 2018 IEEE International Conference on Information Communication and Signal Processing, ICICSP, Singapore, Singapore, 2018, pp. 118–122.
[25] S.M. Pudukotai Dinakarrao, H. Sayadi, H.M. Makrani, C. Nowzari, S. Rafatirad, H. Homayoun, Lightweight node-level malware detection and network-level malware confinement in IoT networks, in: Design, Automation Test in Europe Conference Exhibition, DATE, Florence, Italy, 2019, pp. 776–781.
[26] J. Su, D.V. Vasconcellos, S. Prasad, D. Sgandurra, Y. Feng, K. Sakurai, Lightweight classification of IoT malware based on image recog- nition, in: IEEE 42nd Annual Computer Software and Applications Conference, Vol. 02, COMPSAC, Tokyo, Japan, 2018, pp. 664–669.
[27] M. Jagielski, A. Oprea, B. Biggio, C. Liu, C. Nita-Rotaru, B. Li, Manipulating machine learning: Poisoning attacks and countermeasures for regression learning, in: IEEE Symposium on Security and Privacy, SP, San Francisco, CA, USA, 2018, pp. 19–35.
[28] N. Peri, N. Gupta, W.R. Huang, L. Fowl, C. Zhu, S. Feizi, T. Goldstein, J.P. Dickerson, Strong baseline defenses against clean-label poisoning attacks, in: ECCV Workshop, 2020, pp. 55–70.
[29] J. Chen, X. Zhang, R. Zhang, C. Wang, L. Liu, De-pois: An attack-agnostic defense against data poisoning attacks, 2021, CoRR, arXiv: 2105.03592.
[30] L.T. Phong, Y. Aono, T. Hayashi, L. Wang, S. Moriai, Privacy-preserving deep learning via additively homomorphic encryption, IEEE Trans. Inf. Forensics Secur. 13 (2018) 1333–1345.
[31] P. Mohassel, Y. Zhang, SecureML: A system for scalable privacy-preserving machine learning, in: IEEE Symposium on Security and Privacy, S&P, San Jose, USA, 2017, pp. 19–38.
[32] B. Chen, W. Carvalho, N. Baracaldo, H. Ludwig, B. Edwards, T. Lee, I. Molloy, B. Srivastava, Detecting backdoor attacks on deep neural networks by activation clustering, in: SafeAI@AAAI, Honolulu, USA, 2019.
[33] K. Liu, B. Dolan-Gavitt, S. Garg, Fine-pruning: Defending against backdooring attacks on deep neural networks, 2018.
[34] M. Weber, X. Xu, B. Karlas, C. Zhang, B. Li, RAB: Provable robustness against backdoor attacks, 2020.