International Journal of Multidisciplinary Studies and Innovative Technologies

e-ISSN: 2602-4888
dergipark.org.tr/en/pub/ijmsit
Research Article

2022, 6 (2), 193-197
DOI: 10.36287/ijmsit.6.2.193
Received: Oct. 20, 2022; Accepted: Dec. 6, 2022

Ensuring IoT Privacy using Padding Strategies against Machine Learning Approaches

Ahmet Emre ERGÜN [1*], Özgü CAN [2]

[1*] *Computer Engineering/Faculty of Engineering, Architecture and Design, Bartın University, Bartın, Turkey (aergun@bartin.edu.tr) (ORCID: 0000-0002-3025-5640)*
[2] *Computer Engineering /Faculty of Engineering, Ege University, İzmir, Turkey (ozgu.can@ege.edu.tr) (ORCID: 0000-0002-8064-2905)*

Abstract – The widespread usage of Internet of Things (IoT) devices is increasing by the recent advances in embedded systems, cloud computing, artificial intelligence, and wireless communications. Besides, a huge amount of data is transmitted between IoT devices over insecure networks. The transferred data can be sensitive and confidential. On the other hand, these transmitted data may not appear to be sensitive or confidential data. However, machine learning techniques are used on these non-confidential data (such as packet length) to obtain data such as the type of the IoT device. An observer can monitor traffic to infer sensitive data by using machine learning techniques to analyze the generated encrypted traffic. For this purpose, padding can be added to the packets to ensure traffic privacy. This paper presents privacy problems that are caused by the traffic generated during the communication of IoT devices. Also, security and privacy measures that should be taken against the related privacy problems are explained. For this purpose, the current studies are examined by considering the attacker and the defender models.

Keywords *– Deep Learning; Internet of Things; Machine Learning; Packet Length; Padding; Traffic Monitoring*

Citation: Ergün, A. E., CAN, Ö. (2022). Ensuring IoT Privacy using Padding Strategies against Machine Learning Approaches . International Journal of Multidisciplinary Studies and Innovative Technologies, 6(2): 193-197.

I. INTRODUCTION

Technology is growing at a rapid rate and the role of technological devices in people's lives is gaining importance day by day. Similarly, the use and importance of Internet is inevitable. The Internet of Things (IoT) has emerged due to the increased usage of Internet and new developments in embedded systems, cloud computing, artificial intelligence and wireless communications. These developments have facilitated users' communication with each other and have brought many innovations. IoT is a term that refers to a network of physical things that have been developed with sensors, software, and other technologies in order to connect and exchange data with other systems and devices over the Internet [1-3]. These devices can be household appliances, personal devices or industrial tools [4,5]. Data transfer between IoT devices over the network is achieved due to the communication of devices with each other by accessing the Internet [6]. In addition to non-sensitive information of users, the transferred data may also contain highly confidential information such as home address and personal activities. While IoT devices provide many benefits to users, they can also create threats to user privacy due to insufficient security [7]. Even if the IoT network traffic is encrypted, the personal data of users can be captured from IoT devices by analyzing the network packets [8]. Thus, data is not transmitted securely and it can be used by third parties. Therefore, various security issues and privacy threats are introduced by IoT devices and network traffic classification. For example, an attacker can see the content of the data on the network and capture users' activities by using machine learning techniques [9-11].

As IoT devices are widely used in our daily life, they generate significant traffic while they communicate with each other [12,13]. The generated traffic can contain confidential information. Therefore, observers can steal or gather information from the IoT traffic [14]. Even if the traffic is encrypted, the observer can watch the traffic and analyze the packets using their features like sent time and packet length [15-17]. By applying machine learning techniques, an IoT traffic observer can achieve the confidential information about the traffic. Consequently, an observer will have information about IoT devices and the traffic they generate. Thus, this will result in leaks of user data and behavior.

As seen in the literature, it has been observed that by padding the IoT traffic, the attackers are prevented from obtaining IoT user information significantly and the obtained information rate about the device information is being reduced. Moreover, it is important to ensure the balance between privacy and utility. Thus, data privacy is preserved and data can also be used by IoT device users [18, 19]. For this purpose, the minimum amount of noise to be added should be determined to obtain the highest accuracy and utility while ensuring confidentiality [20]. As shown in Figure 1, the padded packet size is created by padding the original packet length.

Figure 1: Padding the original packet length.

Attackers obtain confidential information from IoT devices by using machine learning techniques, and the padding method is applied to ensure privacy on IoT devices. Therefore, the most used methods in classification are Random Forest (RF) and k-Nearest Neighbors (k-NN). In addition, Long Short-Term Memory (LSTM) deep learning method is also used effectively in terms of accuracy rates. On the defense side, various padding methods are used according to the requirements of data and traffic. When choosing the padding method, using optimal padding has importance to ensure the availability of traffic. Consequently, it is essential to develop a padding method to ensure the traffic privacy of each IoT device.

This paper presents privacy problems that are caused by the traffic generated during the communication of Internet of Things (IoT) devices. Also, security and privacy measures that should be taken against the related privacy problems are explained. The structure of the paper is organized as follows. The literature review on padding and IoT traffic classification is presented in Section 2. Section 3 explains the attacker and defender models. Finally, Section 4 concludes the paper.

II. Materials and Method

A. Padding

This paper focuses on providing a better understanding of the balance between data privacy and utility in IoT devices by reviewing the relevant literature published recently. There are strategies based on adding extra bytes to the current packet length based on packet size. These strategies are mice and elephants, linear, exponential, MTU, random, random 255 [21]. In the mice and elephant's strategy, packets smaller than 100 bytes are increased to 100 bytes and others to 1500 bytes [21]. In the linear strategy, the original packet length is increased by 128 or the nearest multiple of the Maximum Transfer Unit (MTU), depending on whichever is less [21]. The exponential method raises the initial length to the next power of two or the MTU, depending on whichever is less [21]. Random 255 determines the number of bytes to insert at random from 1 to 255 bytes [21]. In the MTU strategy, packets have the same length as the MTU, which is usually 1500 bytes [21]. The number of bytes added to packets is chosen at random based on the variation in length from the original and the MTU in the random approach [22]. There are other padding strategies in the literature. Independent Link Padding (ILP) includes modifying transmission rates to adhere to a specified pace or schedule in order to shield an attacker from learning anything about a device's behavior [23]. During user activities, stochastic traffic padding (STP) executes traffic shaping and selectively injects padding traffic at other times [24]. In the Adaptive Packet Padding strategy, the padding rate changes dynamically according to the current packet size and network usage [25]. These strategies are padding mechanisms developed to obfuscate the traffic and packet length. Researchers have been conducting a study on IoT traffic padding for the past decade. The number of studies on IoT traffic padding has been increasing in recent years. As a result of the investigations most of the studies are based on applying padding to the packet length and based on datasets generated from traffic analyses of IoT devices passing in the network.

B. IoT Traffic Classification

IoT devices can be classified by traffic observers using machine learning techniques. An IoT traffic observer can reach sensitive information about the traffic and devices by observing the traffic. Figure 2 shows an observer who takes packet features of encrypted IoT device traffic as input for the machine learning algorithm. Further, the observer uses them to make a classification of IoT devices and expects to reach a high rate of accessing correct information about device types in the traffic.

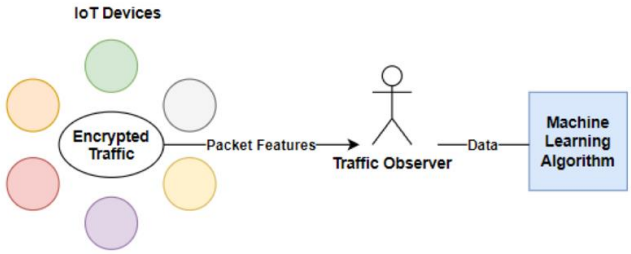

Figure 2: IoT traffic classification workflow.

By using machine learning techniques, various statistics such as pre-padding and post-padding accuracy rates can be compared and the attacker's self-confidence rates can be measured. In [25], the accuracy rate is reduced from 96% to 4,96% for the Random Forest classifier measurement with the padding method. In [26], it is shown that at a granularity of 1 second time windows, the attacker can discriminate time windows containing solely bogus cover packets from windows with real device activity with an accuracy of 81%. They evaluated a variety of machine learning techniques, including Random Forest (RF) and Support Vector Machine (SVM), but the k-NN approach proved to be the most effective in their work. Classification performance of several machines and deep learning algorithms that use six IoT-related datasets is evaluated in [27]. The evaluation results show that the Random Forest algorithm outperforms other techniques. A deep learning method bassequence learningarning, LSTM (Long Short-Term Memory) can also be used to detect IoT devices by sniffing the traffic packets [28]. Their LSTM model can reach 99.2% and 97.7% accuracy on IoT devices in NAPT and VPN configurations, respectively.

III. Results And Discussion

In this section, IoT attacker and defender models are discussed along with the technologies they use.

A. Attacker Model

In today's technology, IoT technology finds its place in many areas such as household equipment, personal d,evices or industrial environments [29-31]. In parallel with the increase in the use of IoT devices, researchers have increased their studies in this field. IoT devices, especially used in home environmentshave a great importance in people's lives. Most of the devices consist of smartphones, sensors, heat meters, smart home appliances, cameras, smoke sensors, blood pressure meters etc. [32-40]. With the use of these devices, many security problems such as privacy issues arise. In the

literature works which focus on padding strategies, it is aimed to increase the confidentiality as a result of the operations performed on the packet size of the data sent by the devices during their communication with each other. At the same time, it is desirable to provide a trade-off between privacy and utility with the minimum amount of padding to be added to maintain transmission performance. Hence, the attacker is imitated with the learning techniques and the learning techniques are applied to the data before and after the padding process. By observing the statistical data such as the accuracy rate used in the learning techniques and the accuracy rates before and after the padding method, it is inferred how beneficial the padding method is in terms of privacy.

The basic idea in implementing the attacker model is based on the ability to learn, for example, from which device this data comes from, with high accuracy rates, by using data characteristics such as packet size, even if the traffic is encrypted. Among the machine learning techniques, techniques such as Random Forest (RF), k-Nearest Neighbors (k-NN), Decision Tree (DT) are the most used in studies. A deep learning method which is Long Short-Term Memory (LSTM), also has significant accuracy results in the literature. Decision Tree algorithm deals with developing decision-making models based on the actual values of data properties [41]. These algorithms work by teaching the system how to classify and predict data [42]. Until a choice is made, the algorithms search the tree structure. The Decision Tree algorithm is used in [43] to identify 33 IoT devices with a high accuracy rate of 98%. Random Forest (RF), as the name suggests, consists of a large number of individual decision trees that work as a community [44,45]. The class with the most votes determines the model's forecast, with each tree in the random forest predicting a different class. An accuracy rate of 92% is reached in [46] by using Random Forest algorithm. k-NN algorithm is a widely used non-parametric classification method [47]. It is employed in the categorization and regression of data. The important feature of any k-NN technique, whether it's for classification or regression, is to locate the k-NN, which let us estimate the value or class for a given point [48]. The vanishing gradient problem is a significant drawback of RNNs [49]. By introducing a continual error flow into the internal states of specific memory cells, LSTM presents a viable solution to this problem [50]. In [51], a deep learning-based LSTM-CNN cascade model is proposed to automatically identify devices. The proposed model outperforms other techniques by achieving 99.7% accuracy.

B. Defender Model

The main goal of the padding strategies is to minimize the accuracy of classifying IoT traffic data with machine learning techniques, while keeping the overhead amount low. Rather than padding each package, it is most convenient and cost-effective to do it adaptively and with the minimum amount of padding required. In this context, it has been observed that the selection of the appropriate padding method depends on the data itself and the traffic density. When the literature on the field of IoT traffic padding was examined, it was seen that the first effective study was done by Liberatore et al. and their claims are substantiated by experiments and their findings are supported by simulations and experiments performed on more than 400,000 traffic streams that they gathered over the course of two months from 2,000 different websites. They looked at four simulation padding techniques: linear, exponential, mice and elephants, MTU. According to their experiments on naive Bayes classifiers and Jaccard's coefficient, MTU is more effective in accuracy than the other three padding methods they used. In the literature, Independent Link Padding (ILP) is firstly used in [23]. ILP can be used to make anonymity systems more secure against traffic analysis attacks. ILP schemes use a predefined schedule to send the user flow. When there is no user packet in the stream, the anonymity system sends fake packets to fill the connection [52]. Another padding technique in literature is Stochastic Traffic Padding (STP), a traffic shaping algorithm, limits the information provided about user activities through traffic rate metadata by using intermittent traffic pad periods. STP provides an adjustable balance between adversary confidence and bandwidth overhead, allowing adequate privacy protection without significantly degrading network performance or exhausting data caps [24]. An efficient padding technique in another study is Adaptive Packet Padding. Based on software defined networking (SDN), this method modifies the number of extra bytes added to packets in response to variations in home network usage. The suggested method observes the network and gives instructions. This article proposes a padding mechanism through the representative state transfer (REST) interface. By using this method, linked devices can alter the length of their packets [25].

IV. Conclusions And Recommendations

IoT devices are necessary to everyday life. However, user information that is captured by IoT devices introduces several privacy risks. Therefore, padding-based mechanisms are used in IoT communication to ensure privacy. This study presents information about the recent studies on padding strategies that are applied to ensure IoT privacy. There are several methods introduced by researchers. The main goal is to keep the utility at the highest possible level while ensuring privacy. The selection of the appropriate padding method has been observed depending on the data itself and the traffic density. It is convenient and cost-effective to apply the minimum amount of padding required to the packages. In this context, the selection of the appropriate padding method has been observed depending on the data itself and the traffic density. In this way, while keeping the accuracy rate of the machine learning methods low in classification, the amount of overhead is kept low.

This paper examines the current IoT padding strategies against machine learning classification techniques for traffic analysis. Traffic analysis is a major threat to data security and personal privacy. In addition to ensure traffic safety, traffic performance is also extremely important. In future research, there is a need to develop a general padding method that can be applied to all IoT packages to ensure that the method can be integrated into all IoT devices by keeping the tradeoff between privacy and utility an optimal level

References

[1] Chegini, H., Naha, R. K., Mahanti, A., & Thulasiraman, P. (2021). Process automation in an IoT–fog–cloud ecosystem: A survey and taxonomy. *IoT*, *2*(1), 92-118.

[2] Benson, K. E., Wang, G., Venkatasubramanian, N., & Kim, Y. J. (2018, April). Ride: A resilient IoT data exchange middleware leveraging SDN and edge cloud resources. In *2018 IEEE/ACM Third International*

Conference on Internet-of-Things Design and Implementation (IoTDI) (pp. 72-83). IEEE.

[3] Sinha, B. B., & Dhanalakshmi, R. (2022). Recent advancements and challenges of Internet of Things in smart agriculture: A survey. *Future Generation Computer Systems*, *126*, 169-184

[4] Saravanan, G., Parkhe, S. S., Thakar, C. M., Kulkarni, V. V., Mishra, H. G., & Gulothungan, G. (2022). Implementation of IoT in production and manufacturing: An Industry 4.0 approach. *Materials Today: Proceedings*, *51*, 2427-2430.

[5] Perez-Camacho, B. N., Rodriguez Gomez, G., Gonzalez-Calleros, J. M., & Martinez-López, F. J. (2022). Methodology for Designing an Electricity Demand System in the Context of IoT Household. *Applied Sciences*, *12*(7), 3387.

[6] Alam, T., & Benaida, M. (2018). CICS: cloud–internet communication security framework for the internet of smart devices. *Tanweer Alam. Mohamed Benaida." CICS: Cloud–Internet Communication Security Framework for the Internet of Smart Devices.", International Journal of Interactive Mobile Technologies (iJIM)*, *12*(6).

[7] Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. *Computer networks*, *148*, 283-294.

[8] Pinheiro, A. J., Bezerra, J. D. M., Burgardt, C. A., & Campelo, D. R. (2019). Identifying IoT devices and events based on packet length from encrypted traffic. *Computer Communications*, *144*, 8-17.

[9] Acar, A., Fereidooni, H., Abera, T., Sikder, A. K., Miettinen, M., Aksu, H., ... & Uluagac, S. (2020, July). Peek-a-boo: I see your smart home activities, even encrypted!. In *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks* (pp. 207-218).

[10] Copos, B., Levitt, K., Bishop, M., & Rowe, J. (2016, May). Is anybody home? inferring activity from smart home network traffic. In *2016 IEEE Security and Privacy Workshops (SPW)* (pp. 245-251). IEEE.

[11] Zantalis, F., Koulouras, G., Karabetsos, S., & Kandris, D. (2019). A review of machine learning and IoT in smart transportation. *Future Internet*, *11*(4), 94.

[12] Gupta, B. B., Chaudhary, P., Chang, X., & Nedjah, N. (2022). Smart defense against distributed Denial of service attack in IoT networks using supervised learning classifiers. *Computers & Electrical Engineering*, *98*, 107726.

[13] Macedo, E. L., Delicato, F. C., de Moraes, L. F., & Fortino, G. (2022). Assigning Trust to Devices in the Context of Consumer IoT Applications. *IEEE Consumer Electronics Magazine*.

[14] Kim, H., Lee, H., & Lim, H. (2020, February). Performance of packet analysis between observer and wireshark. In *2020 22nd International Conference on Advanced Communication Technology (ICACT)* (pp. 268-271). IEEE.

[15] Apthorpe, N., Reisman, D., & Feamster, N. (2017). A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic. *arXiv preprint arXiv:1705.06805*.

[16] Subahi, A., & Theodorakopoulos, G. (2019). Detecting IoT user behavior and sensitive information in encrypted IoT-app traffic. *Sensors*, *19*(21), 4777.

[17] Msadek, N., Soua, R., & Engel, T. (2019, April). Iot device fingerprinting: Machine learning based encrypted traffic analysis. In *2019 IEEE wireless communications and networking conference (WCNC)* (pp. 1-8). IEEE.

[18] Geng, Q., Ding, W., Guo, R., & Kumar, S. (2018). Privacy and utility tradeoff in approximate differential privacy. *arXiv preprint arXiv:1810.00877*.

[19] Xu, L., Jiang, C., Chen, Y., Ren, Y., & Liu, K. R. (2015). Privacy or utility in data collection? A contract theoretic approach. *IEEE Journal of Selected Topics in Signal Processing*, *9*(7), 1256-1269.

[20] Frustaci, M., Pace, P., & Aloi, G. (2017, September). Securing the IoT world: Issues and perspectives. In *2017 IEEE Conference on Standards for Communications and Networking (CSCN)* (pp. 246-251). IEEE.

[21] Dyer, K. P., Coull, S. E., Ristenpart, T., & Shrimpton, T. (2012, May). Peek-a-boo, i still see you: Why efficient traffic analysis countermeasures fail. In *2012 IEEE symposium on security and privacy* (pp. 332-346). IEEE.

[22] Pinheiro, A. J., Bezerra, J. M., & Campelo, D. R. (2018, June). Packet padding for improving privacy in consumer IoT. In *2018 IEEE Symposium on Computers and Communications (ISCC)* (pp. 00925-00929). IEEE.

[23] Apthorpe, N., Reisman, D., Sundaresan, S., Narayanan, A., & Feamster, N. (2017). Spying on the smart home: Privacy attacks and defenses on encrypted iot traffic. *arXiv preprint arXiv:1708.05044*.

[24] Apthorpe, N., Huang, D. Y., Reisman, D., Narayanan, A., & Feamster, N. (2018). Keeping the smart home private with smart (er) iot traffic shaping. *arXiv preprint arXiv:1812.00955*.

[25] Pinheiro, A. J., de Araujo-Filho, P. F., Bezerra, J. D. M., & Campelo, D. R. (2020). Adaptive Packet Padding Approach for Smart Home Networks: A Tradeoff Between Privacy and Performance. *IEEE Internet of Things Journal*, *8*(5), 3930-3938.

[26] Engelberg, A., & Wool, A. (2021). Classification of Encrypted IoT Traffic Despite Padding and Shaping. *arXiv preprint arXiv:2110.11188*.

[27] Vakili, M., Ghamsari, M., & Rezaei, M. (2020). Performance analysis and comparison of machine and deep learning algorithms for iot data classification. *arXiv preprint arXiv:2001.09636*.

[28] Dong, S., Li, Z., Tang, D., Chen, J., Sun, M., & Zhang, K. (2020, October). Your smart home can't keep a secret: Towards automated fingerprinting of iot traffic. In *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security* (pp. 47-59).

[29] Jovanov, E. (2019). Wearables meet IoT: Synergistic personal area networks (SPANs). *Sensors*, *19*(19), 4295.

[30] ElMoaqet, H., Ismael, I., Patzolt, F., & Ryalat, M. (2018, September). Design and integration of an IoT device for training purposes of industry 4.0. In *Proceedings of the 2nd International Symposium on Computer Science and Intelligent Control* (pp. 1-5).

[31] Irawan, Y., & Wahyuni, R. (2021, February). Electronic Equipment Control System for Households by using Android Based on IoT (Internet of Things). In *Journal Of Physics: Conference Series* (Vol. 1783, No. 1, p. 012094). IOP Publishing.

[32] Sehrawat, D., & Gill, N. S. (2019, April). Smart sensors: Analysis of different types of IoT sensors. In *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)* (pp. 523-528). IEEE.

[33] Adi, P. D. P., & Kitagawa, A. (2019). ZigBee Radio Frequency (RF) performance on Raspberry Pi 3 for Internet of Things (IoT) based blood pressure sensors monitoring. *International Journal of Advanced Computer Science and Applications (IJACSA)*, *10*(5), 18-27.

[34] Basu, M. T., Karthik, R., Mahitha, J., & Reddy, V. L. (2018). IoT based forest fire detection system. *International Journal of Engineering & Technology*, *7*(2.7), 124-126.

[35] Palaiokrassas, G., Karlis, I., Litke, A., Charlaftis, V., & Varvarigou, T. (2017, July). An IoT architecture for personalized recommendations over big data oriented applications. In *2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)* (Vol. 2, pp. 475-480). IEEE.

[36] Jang, S. Y., Lee, Y., Shin, B., & Lee, D. (2018, October). Application-aware IoT camera virtualization for video analytics edge computing. In *2018 IEEE/ACM Symposium on Edge Computing (SEC)* (pp. 132-144). IEEE.

[37] Aliero, M. S., Qureshi, K. N., Pasha, M. F., & Jeon, G. (2021). Smart Home Energy Management Systems in Internet of Things networks for green cities demands and services. *Environmental Technology & Innovation*, *22*, 101443.

[38] Stolojescu-Crisan, C., Crisan, C., & Butunoi, B. P. (2021). An IoT-based smart home automation system. *Sensors*, *21*(11), 3784.

[39] Khalfalla, O. A., Ali, S. A., Altrjman, C., & Mubarak, A. S. (2022). Smart Home Appliance Control in the IoT Era. In *International Conference on Forthcoming Networks and Sustainability in the IoT Era* (pp. 392-397). Springer, Cham.

[40] Inyangat, F. X. (2022). *Smartphone agro-IoT application for smallholder farmers* (Doctoral dissertation, Busitema University).

[41] Alghuried, A. (2017). A model for anomalies detection in internet of things (IoT) using inverse weight clustering and decision tree. *Masters's Thesis, Dublin Institute of Technology, Dublin, Ireland*.

[42] Charbuty, B., & Abdulazeez, A. (2021). Classification based on decision tree algorithm for machine learning. *Journal of Applied Science and Technology Trends*, *2*(01), 20-28.

[43] Aksoy, A., & Gunes, M. H. (2019, May). Automated iot device identification using network traffic. In *ICC 2019-2019 IEEE International Conference on Communications (ICC)* (pp. 1-7). IEEE.

[44] Lin, W., Wu, Z., Lin, L., Wen, A., & Li, J. (2017). An ensemble random forest algorithm for insurance big data analysis. *Ieee access*, *5*, 16568-16575.

[45] Abdulkareem, N. M., & Abdulazeez, A. M. (2021). Machine learning classification based on Radom Forest Algorithm: A review. *International Journal of Science and Business*, *5*(2), 128-142.

[46] Dogru, N., & Subasi, A. (2018, February). Traffic accident detection using random forest classifier. In *2018 15th learning and technology conference (L&T)* (pp. 40-45). IEEE.

[47] Wang, H., Xu, P., & Zhao, J. (2021). Improved KNN Algorithm Based on Preprocessing of Center in Smart Cities. *Complexity*, *2021*.

[48] Gawri, B., Kasturi, A., Neti, L. B. M., & Hota, C. (2022, January). An efficient approach to kNN algorithm for IoT devices. In *2022 14th*

International Conference on COMmunication Systems & NETworkS (COMSNETS) (pp. 734-738). IEEE.

[49] Hu, Y., Huber, A., Anumula, J., & Liu, S. C. (2018). Overcoming the vanishing gradient problem in plain recurrent networks. *arXiv preprint arXiv:1801.06105*.

[50] Staudemeyer, R. C., & Morris, E. R. (2019). Understanding LSTM--a tutorial into long short-term memory recurrent neural networks. *arXiv preprint arXiv:1909.09586*.

[51] Bai, L., Yao, L., Kanhere, S. S., Wang, X., & Yang, Z. (2018, October). Automatic device classification from network traffic streams of internet of things. In *2018 IEEE 43rd conference on local computer networks (LCN)* (pp. 1-9). IEEE.

[52] Datta, T., Apthorpe, N., & Feamster, N. (2018, August). A developer-friendly library for smart home iot privacy-preserving traffic obfuscation. In *Proceedings of the 2018 Workshop on IoT Security and Privacy* (pp. 43-48).