International Journal of Applied Science and Engineering Review

IJASER

ISSN: 2582-6271

Vol. 4, Issue.6, Nov-Dec 2023, page no. 45-56

To cite this article: Hajar FARES[1], Nirmine HAJRAOUI[2] and Abderrahmane HAJRAOUI[3] (2023). PROPOSED METHOD FOR DETECTING ACTIVE ATTACKS IN WIRELESS SENSOR NETWORK USING MACHINE LEARNING AND HASH CRYPTOGRAPHIC FUNCTION, International Journal of Applied Science and Engineering Review (IJASER) 4 (5): 45-56 Article No. 175 Sub Id 272

PROPOSED METHOD FOR DETECTING ACTIVE ATTACKS IN WIRELESS SENSOR NETWORK USING MACHINE LEARNING AND HASH CRYPTOGRAPHIC FUNCTION

Hajar FARES[1], Nirmine HAJRAOUI[2], Abderrahmane HAJRAOUI[3]

[1,2]Equipe: systeme de communication et detection, Abdelmalek Essaadi university, Tetouan, Morocco
[3]Department of Telecommunication Laboratory of Remote Sensing and Geographic Information System, ENSA, Tetouan, Morocco

DOI: https://doi.org/10.52267/IJASER.2023.4604

ABSTRACT

Network monitoring and analysis has taken primordial role to understand the functioning of the internet and prevent it from any future probable attacks. Many publications treated the topic of the security as an interesting research domain. Due to the importance and the different applications of wireless sensor networks, the research of finding security solutions is always up but their limited resources (energy consumption, CPU capacity, limited memory…) make the application of classical protocols of security like cryptography, almost impossible. Therefore, recently machine learning is a new field which gets the interest of the majority of researchers. The solutions for providing security services conveyable of in this type of network, are proposed. In this paper we focus in the monitoring of wireless sensor network using machine learning as an intrusion detection system. We address in particular to active attacks. Because of the limitation of machine learning and to provide a high protection against attack we proposed a hash cryptographic function in order to protect the authenticity of information. Our interesting contribution aims three important axes of security: confidentiality, integrity and authentication.

KEYWORDS: Network monitoring, intrusion detection, wireless sensor network, machine learning; active attacks, hash cryptographic function.

1. INTRODUCTION

Wireless sensor network (WSN) is a technology destined for collecting information in order to monitor a specific area. Their facilities of deployment make them very attractive for many applications in various fields, such as military, fire and health monitoring.

International Journal of Applied Science and Engineering Review

IJASER

ISSN: 2582-6271

Vol. 4, Issue.6, Nov-Dec 2023, page no. 45-56

Unfortunately, these sensors nodes have a limited resource: limited battery life, CPU and memory capacities. These limitations are the most challenges to implement the ordinary protocols as cryptography. As the algorithm's complexity of security increase, the power consumption equally increases. This prompted the researches to look for an alternative and effective solution to secure the communication in this type of networks.

Indeed, as the network grows, the task of the network administrator becomes difficult and the need to have a monitoring tool to monitor and alert becomes crucial.

Network monitoring is the use of a system that constantly monitors a computer network for slow or failing components and that notifies the administrator in case of detecting anomalies. Before developing our intervention, an overview of sensor networks, their applications and their current challenges is summarized below.

A sensor network typically consists of hundreds, or even thousands, of small, low-cost nodes distributed over a wide area. The nodes are expected to function in an unsupervised fashion even if new nodes are added, or old nodes disappear (e.g., due to power loss or accidental damage).

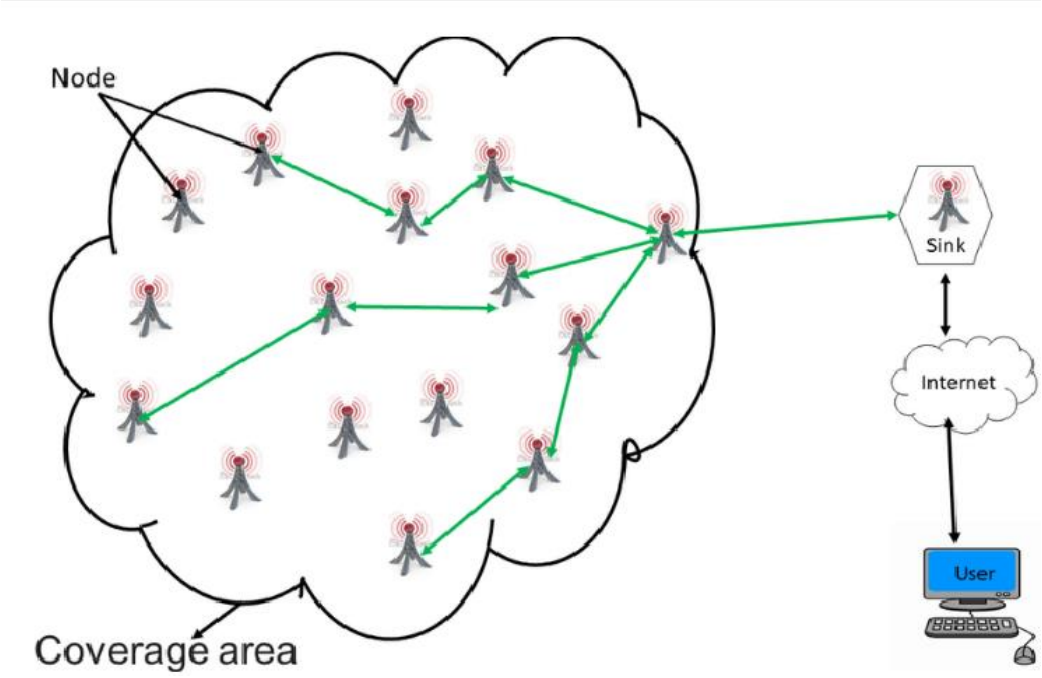

Figure 1: wireless sensor network

International Journal of Applied Science and Engineering Review

IJASER

ISSN: 2582-6271

Vol. 4, Issue.6, Nov-Dec 2023, page no. 45-56

A sensor node [12] uses its sensor(s) in order to measure the fluctuation of current conditions in its adjacent environment. These measurements are converted, via an ADC unit, into relative electric signals which are processed via the node's processor. Via its transceiver, the node can wirelessly transmit the data produced by its processor to other nodes or/and to a selected sink point, referred to as a base station.

Various applications of WSNs [12] are currently either already in mature use or still in infant stages of development. Generally, WSN applications are classified according to the nature of their use into eight main categories which namely are: military, healthcare, environment,
agriculture, security, smart home, industrial, or urban applications.

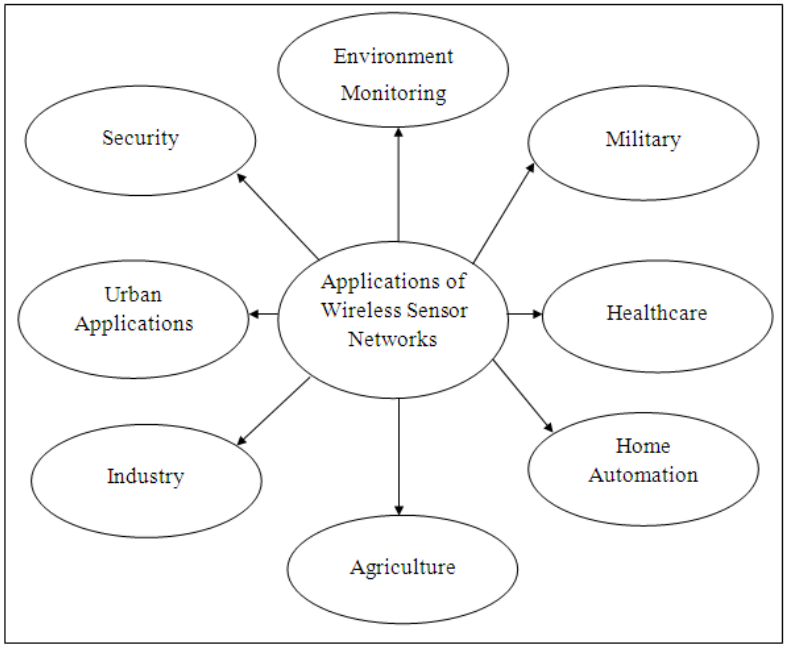

Figure 2: wireless sensor network applications

Any procedure of security designed for a wireless sensor network must take in consideration the constraints and the limitations of this type of network.
We can cite several restrictions [28] such as:

- Low capability of computation,
- Small memory,
- Limited resources of energy
- Unstable topology

International Journal of Applied Science and Engineering Review

IJASER

ISSN: 2582-6271

Vol. 4, Issue.6, Nov-Dec 2023, page no. 45-56

Indeed, the limited power and signal loss during propagation impose fundamental constraints on the operational life time [27] and can cause difficulty in use of security and protection in WSNs

The present study focuses on machine learning as a monitoring tool to detect especially active attacks and a hush cryptographic function to provide a high level of security. This paper was discussed under the following subheading:

- Introduction
- Attacks in WSN
- Machine learning as intrusion detection system
- Contribution and experiment
- Limitations
- Conclusion

2. ATTACKS IN WIRELESS SENSOR NETWORK

Generally, we can classify attacks according to many criteria such as: insider/outsider attacks and active/passive attacks:
Outsider attack, is a malicious node harms the WSN without being part of it.

Insider attack: is a malicious node harms the WSN as an element of the WSN
Active attacks [14]: the unauthorized attacker monitors, listens to and modifies the data stream in the packet exchange within the network including routing attacks, eavesdropping and creation of a false stream etc.

Passive attacker [14] act as a normal node and may do several functions like: collects information from the WSN and unauthorized attackers monitor and eavesdroppers from communication channel.

Authors in [2,3,4,5,6,7,8,9] discussed in details different types of malicious attacks in WSN.

Based on the figure below [24], there are different type of attacks implemented differently according to the layers, while Dos attack shares all layers.

International Journal of Applied Science and Engineering Review

IJASER

ISSN: 2582-6271

Vol. 4, Issue.6, Nov-Dec 2023, page no. 45-56

Malicious attacks in WSN				
Physical layer	**Data link layer**	**Network layer**	**Transport layer**	**Application layer**
Dos Jamming Eavesdropping Node replication Node tampering	Dos Exhaustion Denial of sleep	Dos Selective forwarding Eavesdropping Spoofing Wormhole sybil	Dos Flooding Session hijacking Exhaustion	Dos Repudiation Selective forwarding

Table 1: malicious attacks in WSN

According to many researches, DoS attacks is the most dangerous threats that menace the security in a wireless sensor network.

Dos attack seeks to shut down a system or a network and making it applies to any layer. It works by flooding the sensor node with traffic or providing information that causes the node to fail. Generally, in any network, for it will be called secure, each protocol of security must respect the three axes defined by: confidentiality, integrity, and authentication.

• **Confidentiality [25]:** some field of WSN like (healthcare or military) make sensors transmits critical information. The need of protecting data from attacks is guaranteed with confidentiality by hiding packet with encryption using a secret key known only between sender and receiver.
• **Integrity [25]:** data forwarded from a node should arrive at its exact destination without any small change in the transmitted data
• **Authentication [25]:** refers that authorized node must be able to access to data when needed.
Since the appearance of WSN and their various applications in many fields, many researches try to find an optimal way to secure the communication between nodes and secure data. The current procedure of defenses [15] are: key management, routing security, data aggregation security, and radio channel access security, monitoring and traffic analysing.

3. MACHINE LEARNING AS INTRUSION DETECTION SYSTEM:

Recently machine learning technology gets the interest of many researches in several field of applications. [24] It provides an excellent result against all types of malicious activity. Machine learning algorithms works under the order of a datasets already predefined. It allows to analyse the traffic of a network according of nodes behaviours and classify it as Normal or Attack in order to prevent any possible future attack.

International Journal of Applied Science and Engineering Review

IJASER

ISSN: 2582-6271

Vol. 4, Issue.6, Nov-Dec 2023, page no. 45-56

The table below provide a summary of literature.

References	Type of attack	Learning model	Machine learning algorithm	Accuracy (%¨)
[16]	a. Selective forwarding b. Black hole	supervised	SVM	80≤ x≤100
[17]	a. Wormhole b. Blackhole c. Selective forwarding	supervised	SVM	80≤ x≤100
[18]	a. Black hole	supervised	Markov model	94≤ x≤96
[19]	a. Black hole	Supervised /unsupervised	K-means	99
[20]	a. Flooding	Reinforcement learning	Fuzzy Q logic	83≤ x≤96
[21]	a. Flooding	supervised	Decision tree	83≤ x≤96
[22]	a. Hello flood b. sinkhole c. sybil	supervised	Naïve Bayes	98≤ x≤99

Table 2: summary of the literature

To evaluate the performance of machine learning in detecting attacks, all studies already cited use the notion of accuracy [26] defined with the parameters “TP, TN, FP, FN” (see the table of symbols below) by the following relation:

Accuracy= (TP+TN) / (TP+TN+ FP+ FN)

ISSN: 2582-6271

Vol. 4, Issue.6, Nov-Dec 2023, page no. 45-56

TP	True-Positive	Number of instances correctly classified as an attack
TN	True-Negative	Number of samples correctly classified as normal
FP	False-Positive	Misclassification of normal samples as attack samples
FN	False- Negative	Misclassification of attacks as normal samples

Table 3: list of symbols

Even if the accuracy is high, in some critical applications such as healthcare or military this accuracy must be close to perfect. These limitations conduct us to search other tool to perform the security.

4. CONTRIBUTION AND EXPERIMENT:

4.1 -Preparation of the platform

Our contribution aims to provide the three important axes for a secure communication: confidentiality, integrity and availability.

The scenario proposed is designed to use simultaneously two approaches for allowing a high level of security against attacks: machine learning for analysing traffic in real time and classifying the traffic under two categories: ATTACK and NORMAL. And a cryptographic hush function for securing channel communication.

First of all, python simulation environment is loaded on the operation system.

After the successful installation of python platform, we are started by creating our network with 200 nodes. We assume that the base station is secured and has a sufficient storage and computational.

4.2 -Experiment:

Network traffic routing was carried out with AODV protocol based in sel-synchronization and does not require a fixed infrastructure. Datasets [26] used consists of 16 features sizes and 312106 rows. It's main goal is to detect DoS attacks in a wireless sensor networks by analysing the traffic with 4 different machine learning [24] (Random Forest, Decision Tree, Naïve Bayes and Logistic Regression) and 8 different deep learning models [24] (Multilayer Perception "MLP", Convolutional Neural Network "CNN", long short-term memory "LSTM", Gated Recurrent Unit "GRU", CNN –LSTM, LSTM- CNN, CNN –GRU and GRU –CNN).

This dataset was loaded from the URL:

International Journal of Applied Science and Engineering Review

IJASER

ISSN: 2582-6271

Vol. 4, Issue.6, Nov-Dec 2023, page no. 45-56

https://www.kaggle.com/code/prakadesh/intrusion-detection-system-with-ml-dl-563807#Exploring-the-dataset .

Node_id	Rest_Energy	Trace_Level	Mac_Type_Pckt	Source_IP_Port	Des_IP_Port	Packet_Size	TTL	Hop_Count	Broadcast_ID	Dest_Node_Num	Dest_Seq_Num	Src_Node_ID	Src_Seq_Num	Class
79	600.000000	5	0	79.255	1.255	48	30	1	1	100	0	79	4	normal
78	599.979723	5	800	79.255	1.255	48	30	1	1	100	0	79	4	normal
76	599.979722	5	800	79.255	1.255	48	30	1	1	100	0	79	4	normal
75	599.979722	5	800	79.255	1.255	48	30	1	1	100	0	79	4	normal
118	599.979722	5	800	79.255	1.255	48	30	1	1	100	0	79	4	normal

Figure 3: view of a part of traffic analyzing [26]

To provide a high protection against active attacks and secure data a light cryptographic method is proposed using a hush cryptographic function [23] which provides a several advantages for a secure communication. A cryptographic hashing function makes possible to generate different values called digital signature for each communication attempt. This digital signature has a fixed and reduced size which does not waste memory storage.

The hush cryptographic function also stands out for its speed of execution, which makes it very useful for security in real-time applications.

The hash cryptographic function [23] is executed under the following algorithm:

- The node sender calculates a hash value from their message
- Encrypts it with their own key (the digital signature).
- Sent the message to the node recipient with the hash value encrypted.
- The node recipient generates a hash value from the received message using the same hash function.
- Furthermore, it decrypts the received hash value with the official key
- Compares the two values.

ISSN: 2582-6271

Vol. 4, Issue.6, Nov-Dec 2023, page no. 45-56

• If the two values matches, the node recipient can assume that the message was not manipulated during transmission.

There many proposals hush functions authors in [29] are make a comparative study between MD5 and the family of SHA used in wireless sensor network. They analyzed these hush functions in terms of execution time, message size and energy consumption.

According to the study did by authors [29], they demonstrated that SHA-224 is the best hush cryptographic function for implementing authentication in a wireless sensor network (See the table below)

Hush function	**Output message size (byte)**	**Execution time (second)**
MD-5	128	---
SHA-1	160	0,1355
SHA-224	224	0,1263

Table: hush functions comparison

• As compared with the previous works, this approach propose a scheme for allowing a high potential of security. It doesn't only detect the attacks predefined in the dataset used but can also detect any other tentative attacks thanks to the hash cryptographic function used

5. LIMITATIONS:

Despite the good results obtained, there is always some limitations [28, 30] which stood like an obstacle and make us thinking for searching and improving our proposition. This limitations duo on the one hand, to the specificity of the network and the constraints already cited and on the other hand to the protocol of security used.

The most considerable limitations of machine learning can be summarized as follow:

• The huge amount of data used to learn and predict, which need too much calculation and contradicts with the specification of the network used

• The deviation and unreliable results obtained duo to the false patterns learned, if the data used contains: more/small data or isn't clean and contains noise

ISSN: 2582-6271

Vol. 4, Issue.6, Nov-Dec 2023, page no. 45-56

6. CONCLUSION:

A great deal of research has addressed security in WSN due to the importance that has in several area and applications but the specification of this type of networks like the limited resources (limited energy, CPU capacity, limited memory, unstable topology…) make some challenges to use the classical protocols of security despite of the performance and the efficiency that provides.

Despite the efficiency of this proposed solution, there is always some challenges that conduct us to search and find other solutions.

Recently Machine learning offers several services in network security to detect vulnerabilities or malicious attacks regardless of some limitations already cited.

So, we always search to reinforce this approach taking into account the relationship between the operation time and the amount of energy consumption.

REFERENCES

[1] Ahmad, R.; Wazirali, R.; Abu-Ain, T. Machine Learning for Wireless Sensor Networks Security: An Overview of Challenges and Issues. *Sensors* 2022, *22*, 4730.

[2] Karakaya A, Akleylek S. A survey on security threats and authentication approaches in wireless sensor networks. In2018 6th international symposium on digital forensic and security (ISDFS) 2018 Mar 22 (pp. 1-4). IEEE.

[3] Zou, Y. and Wang, G., 2015. Intercept behavior analysis of industrial wireless sensor networks in the presence of eavesdropping attack. *IEEE Transactions on Industrial Informatics*, *12*(2), pp.780-787.

[4] Hamza, T., Kaddoum, G., Meddeb, A. and Matar, G., 2016, September. A survey on intelligent MAC layer jamming attacks and countermeasures in WSNs. In *2016 IEEE 84th Vehicular Technology Conference (VTC-Fall)* (pp. 1-5). IEEE.

[5] Reindl, P., Nygard, K. and Du, X., 2010, December. Defending malicious collision attacks in wireless sensor networks. In *2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing* (pp. 771-776). IEEE.

[6] Tayebi, A., Berber, S.M. and Swain, A., 2015. Wireless sensor network attacks: An overview and critical analysis with detailed investigation on jamming attack effects. *Sensing Technology: Current Status and Future Trends III*, pp.201-221.

[7] Ward, J.R. and Younis, M., 2015, October. A cross-layer defense scheme for countering traffic

ISSN: 2582-6271

Vol. 4, Issue.6, Nov-Dec 2023, page no. 45-56

analysis attacks in Wireless Sensor Networks. In MILCOM 2015-2015 IEEE *Military* Communications Conference (pp. 972-977). IEEE.

[8] Karuppiah, A.B., Dalfiah, J., Yuvashri, K. and Rajaram, S., 2015, February. An improvised hierarchical black hole detection algorithm in Wireless Sensor Networks. In International confernce on innovation information in computing technologies (pp. 1-7). IEEE.

[9] Alajmi, N.M. and Elleithy, K.M., 2015, May. Selective forwarding detection (SFD) in wireless sensor networks. In 2015 Long Island Systems, Applications and Technology (pp. 1-5). IEEE.

[10] Edeh Michael Onyema1, Ugorji Calistus Chidi2, Nduanya Ujunwa Ifeoma3, Clare Onyewuchi4, Ohwo Stephen Oke5, Ikedilo, Obiora Emeka6. Prospects and Limitations of Machine Learning in Computer Science Education. *Benin Journal of Educational Studies, Volume 27, Issue 1, 48-62; 2021*

[11] Stefano, P.,mathias, P. Reinforcement learning and Tourette syndrome. International review of neurobiology.112.131-153

[12] Kandris, D. Applications of Wireless Sensor Networks. Encyclopedia. Available online: https://encyclopedia.pub/entry/17294 (accessed on 03 November 2023).

[13] Virmani, Deepali, et al., "Routing Attacks in Wireless Sensor Networks: A Survey", arXiv preprint arXiv: 1407.3987 (2014).

[14] Mohammadi, Shahriar, and HosseinJadidoleslamy, "A comparison of link layer attacks on wireless sensor networks", arXiv preprint arXiv:1103.5589 (2011).

[15] Hajraoui, N., Raissouni, N. and Fares, H., 2021. A THREAT ANALYSIS ALLOWING PROGRESS IN THE SECURITY OF WIRELESS HETEROGENEOUS SENSOR NETWORKS.

[16] Kaplantzis, S., Shilton, A., Mani, N. and Sekercioglu, Y.A., 2007, December. Detecting selective forwarding attacks in wireless sensor networks using support vector machines. In *2007 3rd* International Conference on Intelligent Sensors, Sensor Networks and *Information* (pp. 335-340). IEEE. [14]

[17] Sharma, A.K. and Parihar, P.S., 2013. An effective dos prevention system to analysis and prediction of network traffic using support vector machine learning. *International Journal of* Application or Innovation in Engineering & Management, *2*(7), pp.249-256.

[18] E.U.Warriach and K.Tei, " fault detection in wireless sensor networks: A machine learning approach" in 16th IEEE international conference on computational science and engineering (CSE), 2013;pp. 758-765

ISSN: 2582-6271

Vol. 4, Issue.6, Nov-Dec 2023, page no. 45-56

[19] G. Kaur and M. Singh, "Detection of black hole in wireless sensor network based on data mining" in Proc. 5th IEE international conference confluence the next generation information technology summit; 2014; pp. 457-461

[20] S. Shamshirband, A. Patel, N. B. Anuar, M. L. M. Kiah, and A. Abraham, "Cooperative game theoretic approach using fuzzy Q learning for detecting and preventing intrusions in wireless sensor networks", Engineering Applications of Artificial Intelligence, vol. 32, pp. 228-241; 2014

[21] Kim, Mihui, Inshil Doh, and Kijoon Chae. "Denial-of-service (dos) detection through practical entropy estimation on hierarchical sensor networks." In 2006 8th International Conference Advanced Communication Technology, vol. 3, pp. 5-pp. IEEE, 2006.

[22] Sa, M., & Rath, A. K. (2011, February). A simple agent-based model for detecting abnormal event patterns in distributed wireless sensor networks. In Proceedings of the 2011 International Conference on Communication, Computing & Security (pp. 67-70).

[23] www.ionos.fr/digitaleguide

[24] Ahmad, R.; Wazirali, R.; Abu-Ain, T. Machine Learning for Wireless Sensor Networks Security: An Overview of Challenges and Issues. *Sensors* **2022**, *22*, 4730

[25] Gunduz, Sedef, Bilgehan Arslan, and Mehmet Demirci. "A review of machine learning solutions to denial-of-services attacks in wireless sensor networks." In 2015 IEEE 14th International Conference on Machine Learning and Applications (ICMLA), pp. 150-155. IEEE, 2015.

[26] Dener, Murat, Celil Okur, Samed Al, and Abdullah Orman. "WSN-BFSF: A New Dataset for Attacks Detection in Wireless Sensor Networks." IEEE Internet of Things Journal (2023).

[27] Hu, Zhihua, and Baochun Li. "Fundamental performance limits of wireless sensor networks." *Ad Hoc and Sensor Networks* 81101 (2004).

[28] Nayak, P., Swetha, G.K., Gupta, S. and Madhavi, K., 2021. Routing in wireless sensor networks using machine learning techniques: Challenges and opportunities. *Measurement*, *178*, p.108974.

[29] Nunoo-Mensah, H., Boateng, K.O. and Gadze, J.D., 2015. Comparative analysis of energy usage of hash functions in secured wireless sensor networks. International Journal of Computer Applications, 109(11), pp.20-23.

[30] Jabbar, H. and Khan, R.Z., 2015. Methods to avoid over-fitting and under-fitting in supervised machine learning (comparative study). *Computer Science, Communication and Instrumentation Devices*, *70*(10.3850), pp.978-981.