IoT-based Cyber-security of Drones using the Naïve Bayes Algorithm

Rizwan Majeed[1], Nurul Azma Abdullah[2], Muhammad Faheem Mushtaq[3]
Faculty of Computer Science and Information Technology[1, 2]
Universiti Tun Hussein Onn Malaysia (UTHM), Parit Raja 86400, Johor, Malaysia[1, 2]
Department of Artificial Intelligence, The Islamia University of Bahawalpur, 63100 Bahawalpur, Pakistan[3]

***Abstract*—Recent advancements in drone technology are opening new opportunities and applications: in various fields of life especially in the form of small drones. However, these advancements are also causing new challenges in terms of security, adaptability, and consistency. Small drones are proving to be a new opportunity for the civil and military industries. The small drones are suffering from architectural issues and the definition of security and safety issues. The rapid growth of the Internet of things opens new dimensions for drone technology but posing new threats as well. The tiny flying intelligent devices are challenging for the security and privacy of data. The design of these small drones is yet not matured to fulfill the domain requirements. The basic design issues also need security mechanisms, privacy mechanisms, and data transformations. The aspects like intrusion and interception in the domain of the Internet of Drones (IoD) need to be investigated to make these timely drones more secure and more adaptable. In this paper, we have used intelligent machine learning approach to design an IoT aided drone. This approach will provide intelligent cyber security system which will help in detecting network security threats using Blockchain.**

Keywords*—Drone technology; security; internet of things; internet of drones; machine learning; blockchain

I. Introduction

Internet usage is increasing as a powerful tool nowadays because of its unlimited benefits and applications. It is a global trend in which computers and devices are interconnected through some predefined rules and standards. Day-to-day information is carried by these communication networks over the internet. Nowadays, Internet of Things (IoT) is the most widely used network among all networks [1]. IoT is an interconnection of devices that are using the internet to share their information. These devices can be small household objects or can be large industrial machines that are communicating to perform their operations. IoT devices can be used to monitor objects, the performance of machines, bank transactions as well as industrial tasks [2, 3]. There are 90 million IoT objects by the end of 2020 which can be 25 billion in 2021[4]. These IoT objects can communicate intelligently with other devices by consuming low energy. Fig. 1 shows the impact of IoT devices on different areas of life. The manufacturing and health sector has the major share of IoT devices. IoT is most widely used in smart cities, surroundings observing, health, commerce, inventory, and business administration [5].

The main issue with IoT objects is security and privacy. Security means provide authorized access to information and protecting it from unauthorized users. Security includes confidentiality and integrity. IoT-specific security issues include cyber-attacks. With the advancement of technology, security challenges are growing day by day. Cloud technology has increased the risk of unauthorized access to information [6]. This Research [7] Identified cyber security challenges of IoT networks and other sources such as software, hardware, data, and applications. Attacks associated with IoT networks include transmission protocol disaster, denial of service, jamming, spoofing, and messaging attacks.

The advancement of technology and expansion of the economy allows the use of drone technology in many areas of life [8]. Drone technology provides several advantages and benefits for human beings. It helps in day-to-day activities as well as the military and monitoring of weather. However, several privacy and safety concerns are associated with their advantages [9]. At the same time, it also provides openings for cyber-criminals to eavesdrop on drone communication for harmful purposes. Unmanned Aerial Vehicles (UAV) were used in the past with major security threats and extortions. These devices were also used for harmful attacks on communication which increases the chances of distorted warfare. The Internet of Drone Things (IoDT) [10] or Internet of Drones (IoD's) [11] are emerging concepts towards smart commercial drones that can be used for precision agriculture, product delivery, security purposes, etc.

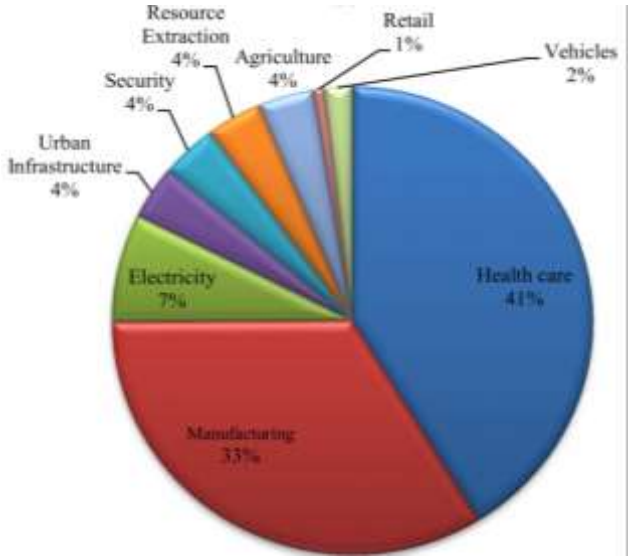

Fig. 1. Financial Influence of IoT Devices.

A major challenge in drone security is the generation of heavy computation and communication load for drones and other IoT devices [12]. The execution of computation-intensive and latency-sensitive security procedures becomes tough to ask for heavy drone data streams due to limited resources of drones such as limited memory, restricted computation, limited radio bandwidth, and limited battery resources. A secure authentication procedure for Drones and other IoT devices to identify the secure nodes and mitigate the identity-based attacks such as spoofing, etc. [13]. A robust access control method is required to prevent the unauthorized need to access the IoT resources [14-17]. A secure offloading technique is required that enables drones to perform computational-intensive tasks while interacting with the storage resources of the server and other edge devices [11].

Currently, there is no efficient platform exists for secure and smart industrial drones. Previously, industrial drones are being flown with a camera and a GIS sensor without having any platform support for drone security and data privacy, which could result in hacking of drones, and interception or loss of drone data [18]. Secure drone flight and privacy of drone data are needed to provide safe and secure surveillance of smart buildings. Additionally, machine intelligence (such as machine learning) support is also needed for drone data analytics along with the support of mobile and Web apps to visualize and disseminate the results [11]. There is a need to investigate and design a secure and intelligent mechanism for the authentication procedure for IoT devices, access control method, and secure offloading [19].

In the modern architectures of drones, the industrial drones are transmitting raw sensor data directly to a cloud platform whereas, the telecommunication channels are not secure. Here, absence of platform support for secure drone data transmission, the possibility exists that a drone with a security hole may be left unattended. A mechanism to manage and upgrade drone-side security and data privacy is necessary. Previously, machine learning has been used to provide secure mechanisms for wireless networks. However, there is a need for blockchain and machine-learning-based intelligent security systems to provide a secure channel for data transmission to the edge side for drones. Previously, blockchain is being used in IoT systems for secure authentication of devices [20], but the security mechanism for secure access control and secure offloading is still an open challenge.

This study will play a significant role in making these tiny flying devices intelligent, smart, and secure. However, the absence of a platform to ensure security and intelligence for these small drones is a bottleneck that makes it difficult to use these tiny drones for commercial, business, or industrial purposes. The proposed research will improve the basic design of small drones to ensure safety from cyber security threats, data privacy threats, and data interception threats. The proposed research is presenting an improved layered architecture that adds new layers from the implementation of security mechanisms and data analysis mechanisms in the traditional architecture of drones. Such, layered architecture will help to handle security and data analytics separate from the other conventional operations of drone handling mechanisms. Additionally, the proposed improvement in layered architecture will not only help in simple implementation but also will support easy regeneration for future enhancements. Furthermore, the secure drone flight and privacy of drone data will help in providing safe and secure surveillance of smart buildings and the raw-sensors data will safely reach IoT Hub for detailed data analytics. Finally, the support for machine intelligence (such as machine learning) will help in improved drone data analytics along with the support of mobile and Web apps to visualize and disseminate the results.

The rest of the paper can be organized as follows: Section 2 explains the research methodology of this research. Section 3 discusses the result and discussion based on the proposed methodology. Section 5 mentioned the conclusion and future work of this research.

II. Research Methodology

This research mainly focused to improve the basic design drones in order to ensure the security threats of drones such as data interception, data privacy and common cybersecurity threats. In the proposed approach, new layers are added in the layer architecture to help the implementation of security and data analysis mechanisms in the traditional drone's architecture. The improvement of layer architecture will support the easy regeneration for future enhancements. Fig. 2 shows the addition of security and privacy layer with the updating in the data processing layer through the components of machine intelligence.

A. Drone Layer

The first layer of industrial drones is the drone layer where camera needs to attach with the mini drone or quadcopter. In this layer, smart sensors are used such as altitude sensor, radar, GPS sensor and camera. The purpose of this layer to sense, record and transmit the recorded information y drones to the next layer. DJI phantom 3 drone are deployed that consist of communication link and custom remote controller.

B. Edge Processing Layer

This layer forwards the IoT raw data and drone data to the security and privacy layer where it verify the data come from authenticated devices. The IoT gateways are used in this layer for wireless communication that provides a fast transmission of the information. This layer is responsible for data flooding, protecting and cashing. For the purpose of cloud communication, it uses the Azure IoT gateway.

C. Security and Privacy Layer

This layer is responsible to provide the authentication to the devices and secure the access control through the machine learning algorithms. In this layer, some privacy threats are occurred such as physical, behavior and location privacy threat. Third party is secretly monitored and capture the drone information that effects the personal information of someone compromised. In behavior privacy, the unauthorized person can monitor someone's activities and behavior. Threats using location privacy involves to capture the location by authorized persons. These threats can be managed through the protocols and authentication schemes. Furthermore, machine learning algorithms are used by device authentication to alert and detect the security attacks.

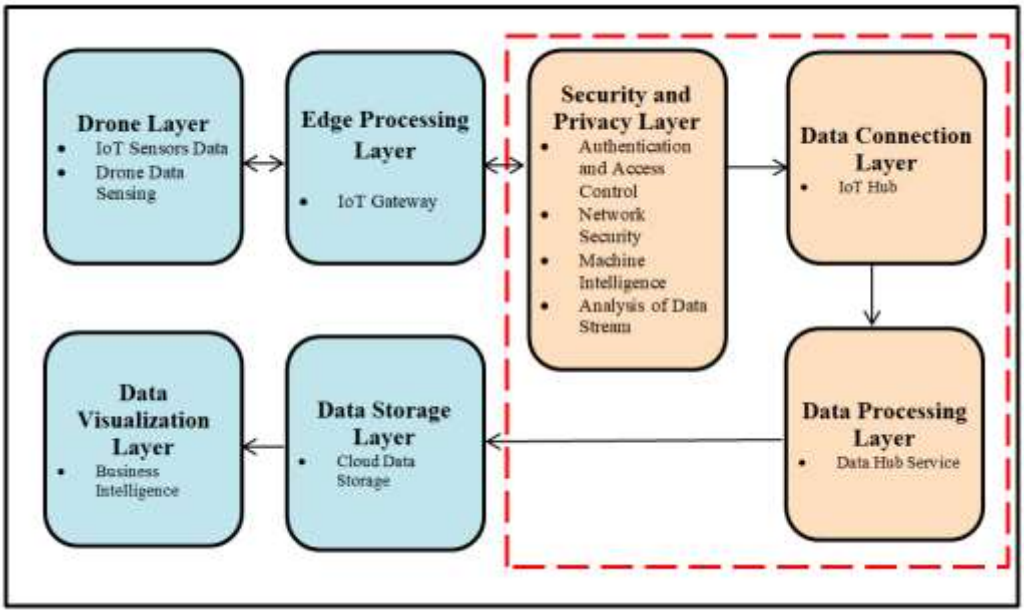

Fig. 2. Proposed Architecture.

D. Device Connection Layer

The security and privacy layer play an vital role to provide the communication link to a cloud based IoT Hub at the base station and new module is added in this layer for security automation and orchestration which ensures the connection between the authenticated devices. In the IoT network, message passing between cloud system and IoT devices is allowed by the IoT hub. IoT security and devices is provided by Blockchain mechanism in real-time.

E. Data Processing Layer

In order to analyze the drone data in stream, IoT hub data is passed to the data processing layer. In this layer, two new modules are developed such as machine intelligence that carried out the intelligent data analysis and data hub service that helps in simple and smooth cloud data storage. Naïve Bayes model are used in this layer that is intelligent machine learning algorithm. Flight data of drone is used for training and testing.

F. Data Storage Layer

Drones generate the data storage results for the cloud-based NoSQL database. It contains the IoT sensors data with the drone and network information. The purpose to use NoSQL database provides less storage schema of information that makes easily retrieve and access data in a short time.

G. Data Visualization Layer

This layer allows the monitoring of data with multiple services and tools. In our proposed work, Microsoft Azure services are used for storage and hub services. The data visualization layer shows the predictions made by proposed intelligent model about the security level of a drone and identified with the intelligent Naïve Bayes model.

III. Results and Discussion

In this section, results produced by the model as well as the experiment are explained. The performance is evaluated using precision, recall, and cost which are arithmetical methods to estimate performance. This experiment is performed on real-time data of drones, KDD'99 dataset. The proposed machine learning model such as Naïve Bayes is applied for good performance.

A. Naïve Bayes Model Results

The proposed Naïve Bayes model provides an overall accuracy of 96.3%. The confusion matrix of the trained Naïve Bayes model depicts true and predicted classes of data provided to the model as shown in table 6.2. Class precision for the DOS, Jamming, and Spoofing category is 96%, 99%, and 93% respectively. Similarly, class recall is also shown in the confusion matrix for three categories. Fig. 3 shows the drone routing id and route length information.

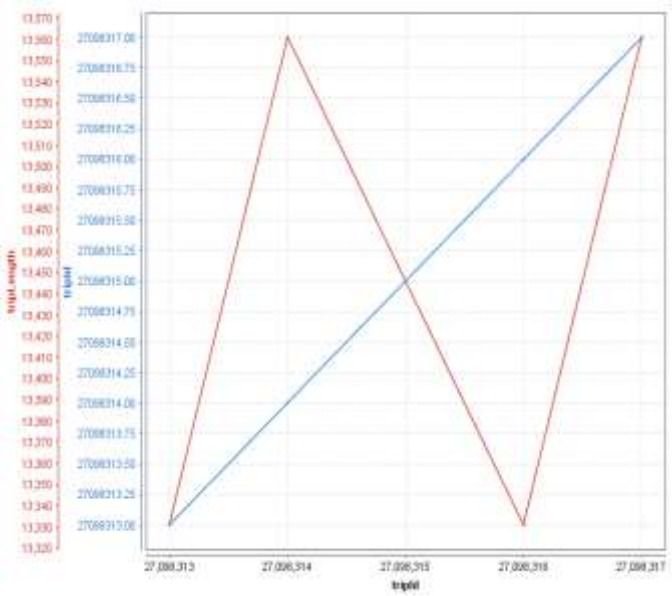

Fig. 3. Trip Id and Trip Length of Drone.

In the graph, trip id is plotted on x-axis and route length of drone is plotted on y axis. Blue and red lines represent this information in a line graph.

Fig. 4 shows the trip id, pattern id and stop length of DJ phantom 3 drone which is used in the experiment. Fig. 5 shows the true positive and false positive rate in training dataset. Fig. 5(a) shows the histogram and 5(b) shows the ROC curve of this training data. -15 is used as a threshold value to separate the normal communication from the malicious traffic.

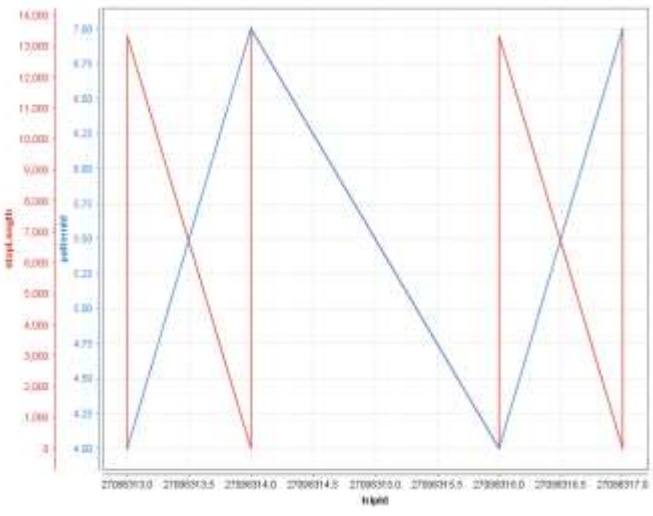

Fig. 4. Drone Flight Information.

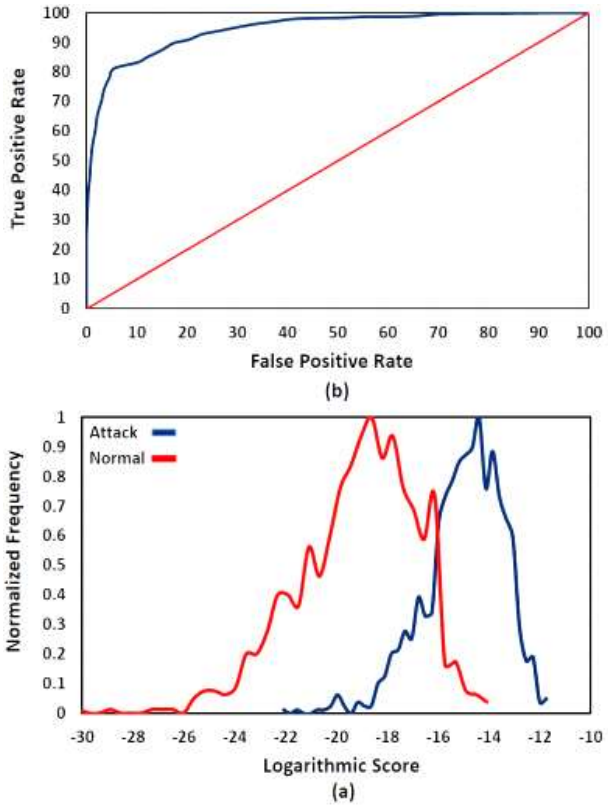

Fig. 5. Threshold Categorization of Training Data i.e. (a) Histogram, (b) ROC.

Fig. 6 shows the training data categorization with -64 threshold value. This training data is generated by the experimentation. Fig. 6(a) shows the histogram and 6(b) shows ROC cure. The ROC curve for the spoofing attach identification is shown in Fig. 7.

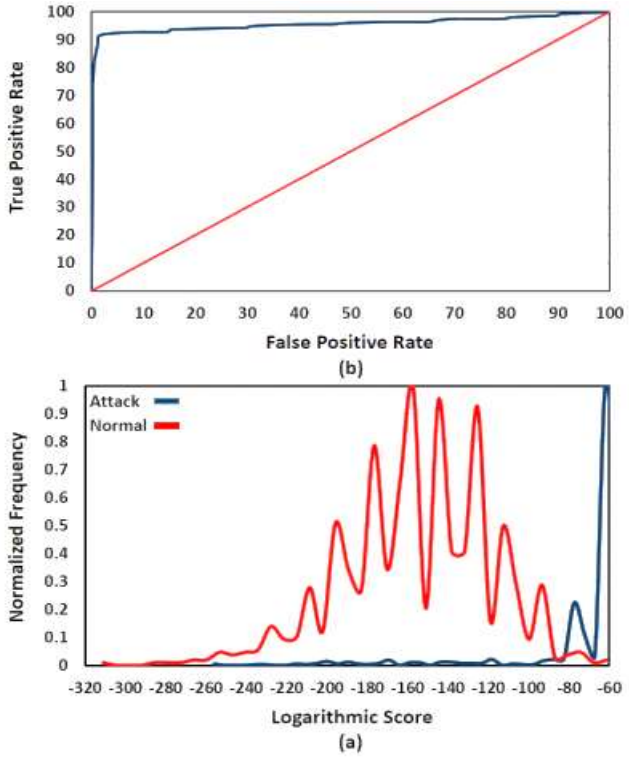

Fig. 6. Threshold Categorization of Training Data with -64 Threshold Value.

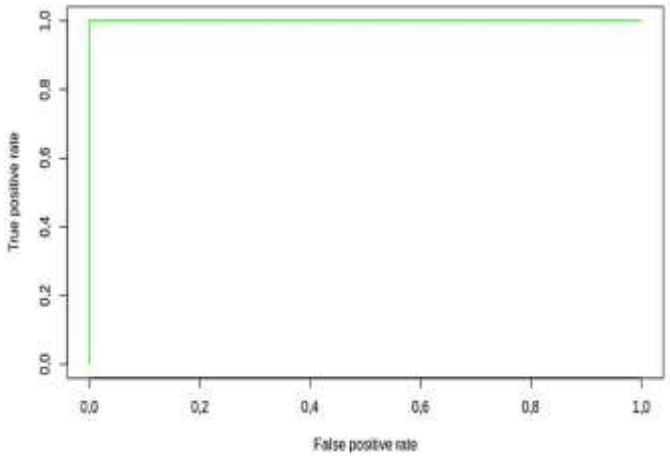

Fig. 7. Spoofing Attack Identification ROC Curve.

The confusion matrix for the Naïve Bayes classifier indicates the accuracy of the proposed machine learning algorithm shown in Fig. 8. True classes are shown as columns and predicted classes are shown as rows. Classification of data is performed by using three classes DOS attack, Jamming, and Spoofing. In this classification process, 96.3% accuracy is achieved which is the best for the cyber security decision-making process.

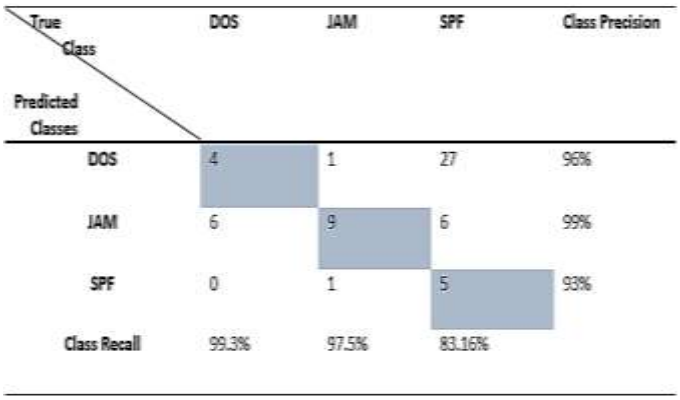

Fig. 8. Confusion Matrix for Naive Bayes Classifier.

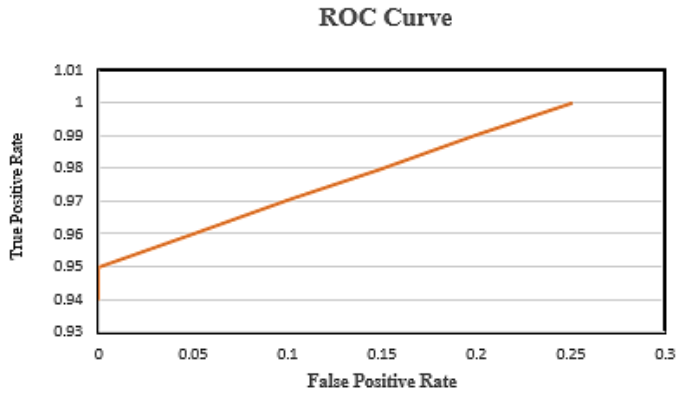

Fig. 9. ROC Curve for Intrusion-Detection Model.

In Fig. 9, the ROC curve of our proposed Naïve Bayes model is shown the number of true positive instances and the number of false-positive instances predicted by the Naïve Bayes model. True positive cases are shown on y and false-positive are shown on the x-axis. The area under ROC is 0.996. Fig. 10 shows the Roc curve for multiple cyber-attacks.

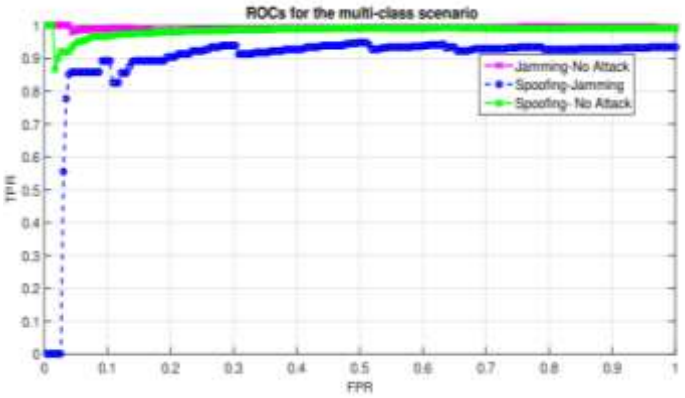

Fig. 10. ROC Curve for Multiple Cyber Attacks.

IV. Conclusion and Future Work

This paper proposes IoT-based cyber-security of drones using the Naïve Bayes algorithm. This model uses IoT sensors data, drones, and network information to generate patterns of security levels and identified the security attacks using these patterns. With this pattern, the model was able to identify attacks in the dataset. This model is tested with two datasets and achieves higher accuracy in real-time security attack detection. The accuracy achieved by the model is 96.3% which is higher and acceptable as compared to previous machine learning approaches. Precision recall and cost are calculated to estimate the performance. The Naïve Bayes model works by predicting items using two layers of processing in which independence between information items is assumed which shows a drawback in this suggested model. In the future, this problem will be addressed using a more efficient algorithm.

Acknowledgment

The authors would like to thank the Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia (UTHM), Johor, Malaysia for supporting this research.

References

[1] Nayyar, A., Nguyen, B. L., and Nguyen, N. G., “The Internet of Drone Things (IoDT): Future Envision of Smart Drones”, International Conference on Sustainable Technologies for Computational Intelligence. Springer, Singapore. pp. 563-580, 2020.

[2] R. Koslowski and M. Schulzke, "Drones along borders: border security UAVs in the United States and the European Union", International Studies Perspectives, vol. 19, pp. 305-324, 2018.

[3] Trevor Hastie, R. T., Jerome Friedman. *The Elements of Statistical Learning*. 2009.

[4] C. Lin, D. He, N. Kumar, K.-K. R. Choo, A. Vinel, and X. Huang, “Security and privacy for the internet of drones: Challenges and solutions”, IEEE Communications Magazine, vol. 56, no.1, pp. 64-69, 2018.

[5] R. Lombreglia, “The Internet of things,” Boston Globe, pp. 76–83, 2005.

[6] M. F. Mushtaq, U. Akram, I. Khan, S. N. Khan, A. Shahzad and A. Ullah, “Cloud Computing Environment and Security Challenges: A Review” International Journal of Advanced Computer Science and Applications, vol. 8, no. 10, 2017.

[7] W. Zhou, Y. Jia, A. Peng, Y. Zhang and P. Liu, "The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved," in IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1606-1616, April 2019, doi: 10.1109/JIOT.2018.2847733.

[8] B. Bera, S. Saha, A. K.. Das, N. Kumar, P. Lorenz, and M. Alazab, “Blockchain-Envisioned Secure Data Delivery and Collection Scheme for 5G-Based IoT-Enabled Internet of Drones Environment”, IEEE Transactions on Vehicular Technology, 2020.

[9] Kerns, A.J., Shepard, D.P., Bhatti, J.A. and Humphreys, T.E. (2014), Unmanned Aircraft Capture and Control Via GPS Spoofing. J. Field Robotics, 31: 617-636.

[10] M. Gharibi, R. Boutaba, S. L. Waslander “Internet of Drones”, IEEE Access, 2016.

[11] Z. Feng, N. Guan, M. Lv, W. Liu, Q. Deng, X. Liu, and W. Yi, “Efficient drone hijacking detection using onboard motion sensors,” in Design,Automation&TestinEuropeConference&Exhibition(DATE), 2017. IEEE, 2017, pp. 1414–1419.

[12] Z. Lv, "The security of Internet of drones", Computer Communications, vol. 148, pp. 208-214, 2019.

[13] M. Shahroz, M. F. Mushtaq, M. Ahmad, S. Ullah, A. Mehmood, G. S. Choi, "IoT-based smart shopping cart using radio frequency identification", IEEE Access, vol. 8, pp. 68426-68438, 2020.

[14] R. Altawy and A. M. Youssef, "Security, Privacy, and Safety Aspects of Civilian Drones: A Survey", ACM Trans. Cyber-Phys. Syst. Vol. 1, No. 2, 2017.

[15] M. F. Mushtaq, S. Jamel, S. R. B. Megat, U. Akram, M. M. Deris, "Key Schedule Algorithm using 3-Dimensional Hybrid Cubes for Block Cipher", International Journal of Advanced Computer Science and Applications, Vol. 10, no. 8, pp. 427-442, 2019.

[16] R. Majeed, N. A. Abdullah, I. Ashraf, Y. B. Zikria, M. F. Mushtaq and M. Umer, "An Intelligent, Secure, and Smart Home Automation System", Scientific Programming, 2020.

[17] M. F. Mushtaq, S. Jamel, K. M. Mohamad, S. K. A. Khalid, and M. M. Deris, "Key Generation Technique based on Triangular Coordinate Extraction for Hybrid Cubes," J. Telecommun. Electron. Comput. Eng., vol. 9, no. 3–4, pp. 195–200, 2017.

[18] F. A. Narudin, A. Feizollah, N. B. Anuar, and A. Gani, "Evaluation of machine learning classifiers for mobile malware detection," Soft Computing, vol. 20, no. 1, pp. 343–357, 2016.

[19] D. Hussain, M. A. Khan, S. Abbas, R. A. Naqvi, M. F. Mushtaq, A. Rehman and A. Nadeem, "Enabling Smart Cities with Cognition Based Intelligent Route Decision in Vehicles Empowered with Deep Extreme Learning Machine", Computers, Materials & Continua, 2020.

[20] V. Chang, P. Chundury, and M. Chetty, "Spiders in the sky: User perceptions of drones, privacy, and security", Proceedings of the 2017 CHI conference on human factors in computing systems, 2017.