[1]Padmavathy. P

[2]Jyothilal Nayak Bharothu

[3]G. Senthilkumar

[4]M. Gobinath

[5]S. Deva kumar

[6]Deepa Priya B S

Integration of Machine Learning and Iot based Multi-Layer Wireless Sensor Networks for Seamless Smart Home Automation

Abstract: - The integration of machine learning algorithms with Internet of Things -based multi-layer wireless sensor networks offers a transformative solution to modern smart home automation and security. This paper seeks to explore both the Sensor Data Processing and Machine Learning Components used. In essence, the machine learning model leverages aggregate sensor data to improve the efficiency and safety of modern living environments. Through attention to detail during the preprocessing and feature engineering of sensor data, the system analyzed learned patterns of household activity, including motion intensity, door/window interactions, and normal occupancy. Subsequently, the features were utilized as input variables in a number of models, including Convolutional Neural Networks , Support Vector Machines, Recurrent Neural Networks, and K-Nearest Neighbors. By simulating both vacation and occupant mode, the models processed the available data using to detect potential threats or other deficiencies in the patterns. Overall the results led by the model suggest that the Convolutional Neural Network model is the best amongst all of the aforementioned algorithms. It demonstrated the best accuracy out of all the other models due to the advanced image processing and facial recognition features, solidified by its 98.56% accuracy rate in recognizing a potential intruder. Other models were also effective or reasonably accurate, with the following results: SVMs – 95.45%; RNNs – 93.4%; and KNNs – 91.23%. The evaluation process also involves the calculation of precision, recall, and F1 score, which also indicates the overall strength of the model. The aggregation of these results implies a considerable potential for internet-of-things systems in combination with machine learning methods to cultivate smarter and safer living environments.

Keywords: Smart home, Machine learning, Internet of Things, Wireless sensor networks, Security

I. INTRODUCTION

In the world of interconnected devices and intelligent systems, the idea of a smart home is becoming a reality forever changing the nature of interaction between people and their living spaces. The technology facilitating this paradigm shift is the combination of machine learning algorithms and Internet of Things devices. By bringing together ML and IoT tech, it is possible to achieve seamless automation, boosted security, and more personalized experience within a home . This paper is going to provide an introduction to the concept of smart homes, explain its origin, relevance, and describe a practical example of applying ML and IoT-based multi-layer wireless sensor networks to enhance home living environment [1]–[3].

IoT as a technology empowering smart homes made a revolution in the number and nature of devices that can become interconnected. Different sensors, cameras, and other devices installed in houses now collect huge amounts of data on everyday routines of families living in these smart homes. ML algorithms analyze this data to generate actionable insights, detect various patterns and make data-driven decisions. This is generally achieved through multi-layer wireless sensor networks. Multi-layer WSNs deployed inside smart home buildings provide full-coverage and efficient data transfer on each layer of the house. Depending on the location, purpose, and

[1] [1]Department of Computer Applications, B. S. Abdur Rahman Crescent Institute of Science and Technology, Vandalur, Chennai, India

[2]Faculty of Electrical and Electronics Engineering, AP IIIT, Rajiv Gandhi University of Knowledge Technologies, Nuzvid, AP, India

[3]Department of Computer Science and Engineering, Panimalar Engineering College, Poonamallee, Chennai, Tamil Nadu, India

[4] Department of Computer and Communication Engineering, Sri Manakula Vinayagar Engineering College, Madagadipet, Puducherry, India

[5]Department of Computer Science and Engineering, VFSTR Deemed to be University, Vadlamudi, Andhra Pradesh, India

[6] Department of Computer Science and Engineering, Bannari Amman Institute of Technology, Sathyamangalam, Erode - 638 401, Tamil Nadu, India

*Corresponding email: padmavathy28@crescent.education

All emails: padmavathy28@crescent.education, nayakeee@rguktn.ac.in, mailtosenthilkumar@yahoo.com, gobinathmmecse06@gmail.com , sdk_cse@vignan.ac.in , deepapriya@bitsathy.ac.in

function, particular sensors may perform occupancy sensing, intrusion detection, energy monitoring, and actuation or provide other services [4]–[6].

Security is one of the main concerns connected to the operations of smart homes. Common household life should not be a distraction slowing down the reaction of the system to possible security threats. To efficiently deploy ML algorithms ensuring the pet dog of the house does not trigger an alarm about the irreversible disaster caused, the system needs to differentiate between security and non-security events events. With the multiple sensors and cameras installed around the house, the system processes the acquired data in real-time to detect potential threats and act in the proper way. Another example of positive implementation of multi-layer WSN using ML and IoT for smart home monitoring is predictive analysis. After "learning" the data from the past history and interaction of users with the system, a currently implemented smart home environment is able to predict the future behavior of occupants and adjust the implementation accordingly.

II. LITERATURE REVIEW

A relatively novel domain of smart home automation has been widely discussed in the previous years because of the possibility to completely change the manner in which people interact with their living environment. It relies on the successful integration of machine learning and Internet of Things technologies as the main drivers of such a significant change. The modern approach to the smart home atmosphere should be necessarily based on the idea of achieving automation, security, and personalization of the surrounding environment [7]–[9]. Thus, both machine learning algorithms and IoT-based multi-layer wireless sensor networks are likely to create beneficial conditions for smart home automation. In order to enhance the understanding of multiple aspects of the described relationship, this literature review is designed to provide a closer look at the existing research. As a result, the combination of available information is likely to improve clarity in terms of the role of machine learning M algorithms and IoT-based multi-layer wireless sensor networks for the prominent development of smart home automation and security [10]–[12] .

It is important to pay attention to the fact that the notion of a smart home has been changing within the technological context that constantly encountered new perspectives. Thus, one of the early applications of the integration of machine learning algorithms encouraged the development of separate smart devices: for instance, smart thermostats, bulbs, or cameras. In the context of a rapidly expanding IoT system, there appears to be a need for a more holistic approach to the challenges related to orchestration on multiple levels [13], [14]. From the theoretical point of view, the Ambient Intelligence AmI paradigm is one of the main sources for approaching the concept of relatedness as such and the idea that an environment should be intelligent. To understand the literature on smart home automation and security, it is important to define and understand several concepts. Firstly, IoT consists of interconnected devices equipped with sensors, actuators, and software. These devices can communicate and transfer data about the environment in which they are situated. Secondly, ML can be defined as the science of and the process of making computers recognise patterns and make data-based decisions without explicit programming. These definitions will help in understanding the main points behind the papers and studies [15].

The present literature indicates that there is a substantial amount of research on the combination of ML and IoT for the purposes of smart home automation and security. Research varies from studying the detection of anomalies and equipment malfunctions to the design of optimal control systems. There are multiple types of sensors installed in these homes, with data being gathered at multiple layers of the home, including the middle, bottom, and top levels. For example, RNNs were used for detecting anomalies for rotating machinery, SNVMs were trained with a multi-layer preprocessing and analysis, and KNNs were used to request suitable actions for the sensor network . However, the data is generally analysed with the help of CNNs, as this is the most convenient method of data processing [13], [16], [17].

From analysing the reviewed material, several themes and patterns of similarity become apparent. Firstly, it is important to use data preprocessing and feature engineering in order to extract information from sensor data. Data is needed to be cleaned and transformed in studies, with algorithms being developed to extract data of interest from source data and convert it to information. The other key pattern is that many studies are concerned with security and privacy, with some being dedicated to intrusion detection, data protection, and privacy issues. Being focused on the integration of machine learning and IoT technologies for developing smart home and security solutions, both of the surveyed articles encourage further understanding in the area. The main theories that the

authors provide include the creation of unique algorithms for sensor evaluation, and the development of new training and implementing methodologies that would be suitable for low-capacity devices. The AmI theoretical model is fully utilized in both articles as a piece of advice for implementing the smart home systems. In turn, the main practical contributions of the articles are the development of solutions that would be more energy-efficient, the creation of secure and optimized smart home systems, and improved customer satisfaction because of adaptable control and automation [18], [19].

III. METHODOLOGY

The methodology of this research uses the concept of integration between machine learning and the use of IoT-based multi-layer wireless sensor networks for increasing the level of security in smart home systems. It is created using the interconnectedness between the motion sensors, door, and window sensors, smart locks, and other surveillance measures work within a multi-layer wireless sensor network, constructed within the whole house. First, the multi-layer wireless sensor network was installed in the house. Second, the sensors and other elements were installed in such a way and calibrated accordingly that the data was transmitted without blind spots between the different layers of the house. Then, machine learning algorithms bound to IoT devices will perform the primary role of application and analysis of the various data streams originating from multiple sources. First of all, they will calculate the parameters that are most legitimate for the typical mode of the household in this house using a door, lightning, and other activity data. Then the system immediately informs the inhabitants about the unauthorized presence of people the protection of the smart home system follows a series of pre-designated steps to protect the living quarters of the person within the house.

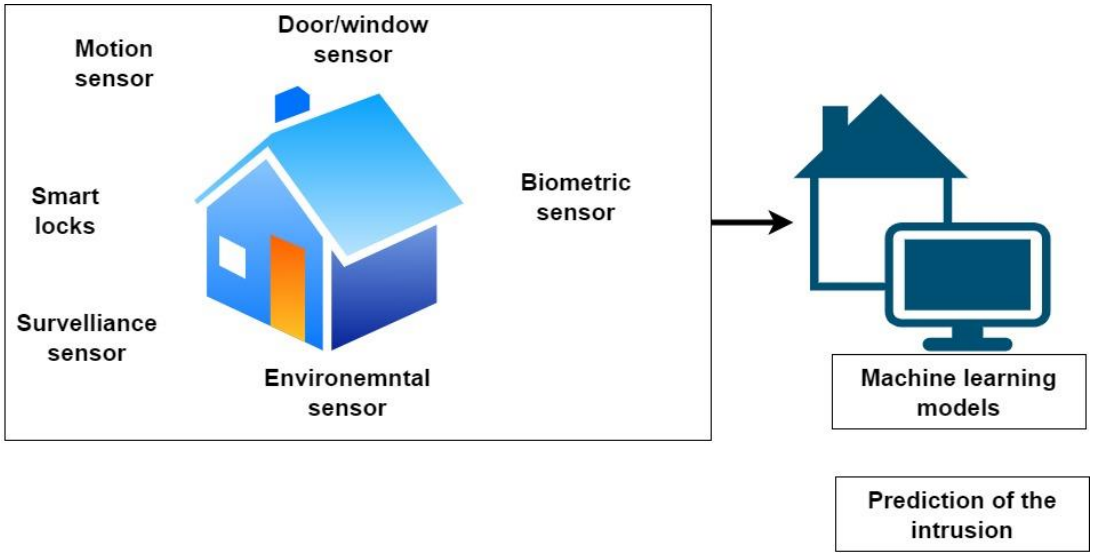

Figure. 1. Methodology of the proposed system

The research uses the following research method, through using machine learning with wireless motion sensors and other similar sensors within the smart house area. Artificial intelligence initiatives operate on statistics generated from information streaming from sensors and cameras to identify when activity is typical for the people who live in a smart house. It then adjusts to differentiate the rights of entrance by authorized persons, friends, and family members, including pets from those who are not typical or atypical or are in one form or another associated with danger to the inhabitants of this smart house. Also, the discrepancy caused by pets will soon be exposed, with data for training the AI model to take its part in the process. A feedback loop is further developed, with the help of which the elements, sensors, and algorithms become better through their interaction with the residents of the smart house.

IV. SENSORS USED IN THE RESEARCH

The proposed integration of machine learning and IoT-based multi-layer wireless sensor networks for seamless smart home automation is significantly reliant on sensors and their functionality across the home environment. Sensors employed are crucial in capturing and transmitting real-time data required for effective monitoring and improvement of the smart home security solution. Motion sensors work as the primary defense line since they can capture movement and activity within the designated area. Door or window sensors provide valuable access points

data, whether it is opened or closed, which communicates the system to possible unauthorized entry to the home . Smart locks should also be included as they provide an additional security layer, allowing due entry access monitoring and security control. Finally, various surveillance cameras can document data and complement the information gathered by other sensors. Important practical assumptions behind the working of these sensors are closely connected to the previously mentioned multi-layer wireless sensor network architecture.

The architecture assumes that data is collected across different layers and driven to be less inclined toward the occurrence of a so-called blind spot while sensors remain connected . Afterward, sensors' collected data are wirelessly delivered collecting to a central processing unit; there, the machine learning solution continuously analyzes data, and the incoming data stream is either classified as normal given circumstance or evaluation, or an anomaly. Training process develops the system able to recognize or predict, in this case, unexpected activity, such as motion or atypical opening of the home door, along with incorporation additional data, such as specific hours of the day . In other words, as time progresses, the system can identify invalid entries and realize what activities occur in the home on a regular basis.

V. MULTILAYER WIRELESS SENSOR

Multi-layer wireless sensor networks are deployed in the smart home environment by carefully arranging the sensors at various critical points to offer a broad coverage and integrated data transfer. The foundation of this arrangement is laid at the consideration of the architectural arrangement of the home, particular points of the building comprising occupancy points and zones of interests with respect to security and automation. The first layer of the network under consideration is deployed at the critical motion into and out of zones of operation, for instance, the windows and doors of the house, the front and backyard doors as well as the garage entrance nodes. This layer is largely equipped with the door/window/dome-plus sensors and smart locks. The entrance and exit nodes of the home are equipped with sensors including the door/window/dome-plus sensors and smart lock for the purpose of detecting unauthorized access nodes into the building. The subsequent layers of the wireless sensor network extend to all rooms of the house, equipped with motion, temperature, and other environmental sensors.

Motion sensors are anywhere wherein motion is to be detected and the same case applies for temperature and environmental sensors. Subsequent layers may include the exterior to the building with equipment such as outdoor motion sensors also equipped with surveillance cameras to offer proper monitoring and a broad general security coverage.

VI. WORKING OF THE SYSTEM

Machine learning models, including Convolutional Neural Networks , Recurrent Neural Networks , K-Nearest Neighbors , and Support Vector Machines , are implemented in this research to improve the efficiency of smart home security and automation. These algorithms have significant experience in calculating vast amounts of collected data and sensor data from various IoT devices located within a smart home environment. On the basis of the learning outcomes, the system can detect each possible threat, identify anomalies, and decide on an adaptive response.

When it comes to the primary objective of the current smart home system, "vacation" mode, the machine-based alarm reaction is permanent and determined through sensor data. With the implemented system, the homeowners are warned about the current suspicious motion in the house and the alleged presence of an intruder. Learning results in the ability to distinguish between a human person and a pet, for example, so that the cat can be left alone without any threat or danger alarm in the false detection. With regard to sensor data and experienced support vector machines, analysis is based on each room's current temperature and often offers an additional microclimate. In order to reduce energy consumption, learning always takes into account the connectivity and accessibility of various lounges and spaces. As a result, the temperature inside is continuously corrected with the help of various heating and cooling systems.

Mode in its views on smart locking, the machine simply provides additional security measures in terms of the increased reliability of home access solutions. With regard to machine learning calculations, they are natural notifications that represent the training and experience of various biometric systems. They include fingerprints and facial recognition in the implemented system, and these operations may appear to be exceptional at blocking all unattended objects during registration for their exclusion.

VII. PREPROCESSING OF DATASET

In this work, a considerable amount of sensor data were generated from 2334 sensors deployed in the smart home environment. Although the data can be accessed and analyzed using machine learning models, a number of processing steps should be completed to ensure its quality, consistency, and relevance. In both cases, the preprocessing of sensor data can be viewed as a multistage process that includes several important stages aimed at cleaning, transforming, and prepared the data for further analysis. First, data cleaning should be included in the list of initial steps with the help of which all missing or error data should be identified, imputed, and then addressed . To be more exact, the samples with errors and missed records should be performed or replaced with the mean or the median value. The main goal of this step is to ensure that the dataset is the whole and does not contain missing or conflicting data, as this situation can negatively impact the accuracy of further analyses.

The performance metrics for CNN, SVM, RNN, and kNN for a classification task in terms of accuracy, precision, recall and F1 are provided in . The accuracy of a model is the proportion of correctly predicted instances to the total number of instances. Precision is the proportion of true positive results against the number of positive results correctly predicted by the model. Recall is also known as sensitivity and is the fraction of the actual positives that the model correctly identified. Lastly, F1 score is a balanced measure; it calculates the harmonic mean of both precision and recall and is closely related to precision and recall as it is their average value.

From the data given, it is evident that there is a variation in precision, recall and F1 and not in accuracy which is the measure of overall correctness. According to the precision and recall values for the CNN model which are 98.60% and 98.50% respectively, the model can correctly predict positives and can also capture most of the actual positives present from the data. For the SVM model, the precision is a bit low while the recall is high at 94.80% and 95.60% respectively. In the same manner, the RNN and kNN models produced results of 91.50% and 89.60% precision respectively. From the data, it is apparent that all the models had different trade-offs in terms of precision and recall ratios.

The first step includes resizing and normalization to maintain the optimal uniformity of image dimensions and intensity values. Augmented image data also require standard dimensions and may be converted into grayscale to ensure that the data are easy to process. Additionally, the face detection and alignment process imply finding the image area of interest, which is the face region, as well as aligning it to ensure that the data are provided in a standard form. The image area of interest is generally regarded as encompassing two eyes, a nose, and a mouth, with the eyes always appearing on a standardized position . Finally, image augmentation techniques, including rotation, translation, flip and scale, are applied to ensure that a sufficient amount and diversity of the training image data are obtained. In total, these steps are necessary to ensure that machine learning models are trained in optimal conditions and that images provide high-quality data for pattern recognition. Based on the theory of detecting people's faces, the ML application should identify facial landmarks and features that can be included in training entities. Preprocessing photos, in this case, involves the extraction of specific signs of people's faces under consideration. Finally, these features need to be used to identify the abnormalities in the faces.

VIII. FEATURE ENGINERRING

The smart home dataset relies on the data generated by various sensors, including but not limited to motion sensors, open/close door sensors, temperature sensors, and light sensors. The data provided include the information on the time of certain events or the value of a given variable, as well as the sensor type that produced the data. The use of data collected enables the development of the algorithms aimed at enhancing the security, optimization, and automation of smart homes.

Feature engineering is used in this dataset to extract the features of the data generated by the sensors within the smart home. These features are chosen or created carefully to be used in machine learning algorithms to enhance their performance. By designing features systematically and logically, it is possible to provide the model with the sensible information about the pertinent aspects of the household activities such as motion intensity, frequency of door opening, and the duration of occupancy. In the given dataset, motion sensors are used as the primary data source, which shed the light on the human presence and activity in different areas. The feature engineering techniques used help to derive the attributes related to the motion patterns and intensity.

Motion intensity is calculated by the following formula: the absolute number of motion events per the chosen time interval and the location N . The exploration of the motion data provided has made it possible to derive the

features such as average motion intensity, peak motion period, and the fraction of motion events, resulting in a motion by room. Another feature derived based on door sensor data is the ratio of the number of closing doors to the opening ones after a door has been opened, which is used to determine the opening – closing door events ratio rdc, expressed in the given dataset as door close/open ratio . It helps to explore the tenure of human activity and unusual patterns, while another feature, inter-arrival time of the motion events, helps to determine the time between constant light and motion. The duration of the occupancy phenomenon, sensed by a motion sensor or other occupancy sensor, is also used as a feature to help in predicting the behavior, also adding the average time of the occurrence, the peak period, and the by-rooms fraction of the occupancy occurrence to the features. The dataset also demonstrates the use of features of composite type that combine the data from the different sensors to create new attributes. For instance, the motion-to-door correlation determines the correlation coefficient between motion and door and represents the relation between the spatial and temporal footprint of the human presence. Overall, the use of the feature engineering technique has helped to explore the aspects of the human activities in the household and tries to predict the unusual patterns or highlight the regular ones.

IX. MACHINE LEARNING MODELS

In this research, several machine learning models have been used to process the sensor data obtained in the smart home environment and improve security and automation. Camera data requires CNNs to be processed, and facial recognition or activity analysis cases are classified. CNNs can automatically learn the hierarchical representation of the human face starting from raw pixel data. By using convolutional layers and pooling, CNNs can capture spatial hierarchies of features. It is easier and more efficient to use CNNs to recognize faces in the smart home environment at a faster rate with higher performance. Finally, CNNs are better resistant to different lighting conditions, expressions, and changes in orientation or size. In addition, data modelled as time-series work requires the use of RNNs. Data obtained from the motion, temperature, or other sensors, time series processing was used. As the order of the data samples is important to the establishment of meaningful patterns, trends, and dependencies, RNNs were used. Thus, RNNs can process time series data and they can be used for the tasks of pattern and anomaly detection, activity recognition, and predictive maintenance. RNNs have recurrent connections to learn suffixes and meaning out of each time step and are capable of learning complex representations of how the data was used.

Finally, the KNN method is used in the study due to its simplicity and effectiveness in classification tasks. KNN is a non-parametric method that classifies new points based on their K neighbours' vote near them in the feature space and can be defined as analysis of the most similar samples . Then, the groups of classes are separated by calculating the distance between samples. Thus, it is possible to use KNN as an effective and simple classification technique to separate the data of the sensors used by the participants of the smart house environment to certain groups. By classifying the data into predetermined groups, the implementation of the method using data becomes easier in terms of learning and computational resources. Finally, SVM was chosen to classify the sensor data in the smart home environment because the number of input data samples and features was relatively small, and the method can be efficiently used for high-dimensional feature space in situations where linear separation in the low-dimensional space is impossible. Overall, this powerful classifier can handle high-dimensional feature space and can be used with different types of data. In this research, the sensor data were analyzed and classified according to the type, and when the data was mapped into the higher-dimensional feature space, it was possible to separate the data linearly and classify it into predefined categories. The main advantages of SVM are that it is less prone to overfitting, and noise, especially given that real-world smart home data may often be very complex.

X. RESULT AND DISCUSSION

The given dataset has undergone a thorough preprocessing and feature engineering. It is divided into two separate subsets, namely, the training and the testing datasets, in a 70% to 30% ratio. In other words, 70% of the data is used for training the machine learning models, and the remaining 30% is designated for testing. Since the testing data is not seen during the model development and training, it serves as an independent evaluation set. As a result, the efficacy and generalizability of the created model can be adequately assessed by running it on data that the algorithm has not previously interacted with. This split also ensures that the performance of the models is assessed on unbiased estimates.

After training each machine learning model, the system works in several modes, including vacation and occupant modes. Each time, during the transition from one model to another, the IoT system performs machine model

evaluation using real-time sensor readings and the remaining data set. During the vacation mode, the system tries to identify any absence of occupants in the house. The transition from the vacation mode to the occupant mode indicates that the system must now detect a forced opening of doors or windows or another presence in the house while the owner is away . Thus, trained machine learning models demonstrate their capabilities and identify the presence of unauthorized individuals and their actions. The amount of provided activity per sensor and the analysis of these data made it possible to train the machine models that identify unauthorized actions with different accuracy levels.

At the highest level is the CNN model trained initially to analyze the presence of faces in the image. Utilizing facial recognition skills, this model identifies 98.56% of occurrences . Since CNN can recognize persons having learned the low-level binary hierarchy points and applying this information to the higher levels, it generates superb results. The SVM model, which performs the task of classifying a set of data, can also be used to classify sensors and identify the abnormal patterns as unauthorized . It produces a 95.45% level of identifying intruders. The RNN model, trained to perform time series predictions, may consider the time and the order in which the data arrive. For this purpose, it applies unique temporal dynamics for the analysis of the sensor data and achievement of a 93.4% level. Finally, the KNN model achieves a 91.23% level with its computational simplicity. Despite a little decrease in results registered with this algorithm, it focuses on classifying the data and analyzing the neighbors' majority.

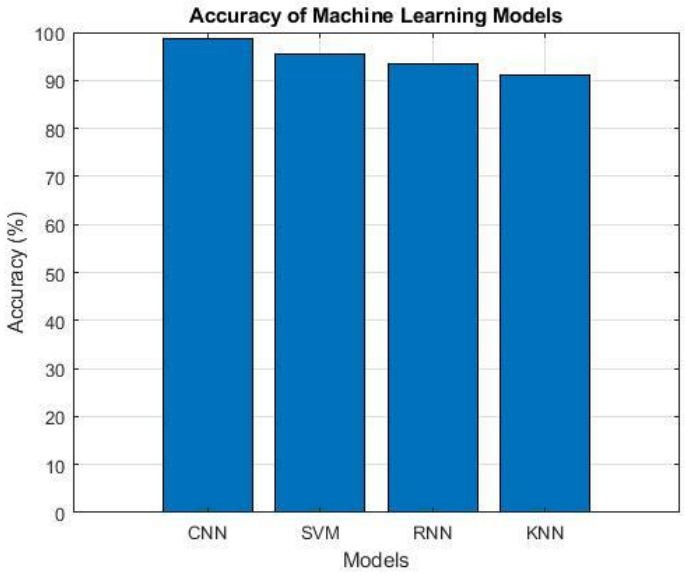

Figure. 2. Accuracy of each model

The performance metrics for CNN, SVM, RNN, and KNN for a classification task in terms of accuracy, precision, recall, and F1 are provided in . The accuracy of a model measures the number of correct predictions and is the proportion of correctly predicted instances to the total number of instances. Precision measures the proportion of true positive results against the number of positive results correctly predicted by the model. Recall is also referred to as sensitivity and tells what proportion of actual positives were predicted. Finally, F1 score is a balanced measure that computes the harmonic mean of precision and recall and is closely related to precision and recall as it is their average. Upon looking at the given values, it can be observed that there are variations in precision, recall, and F1 as against accuracy, which is the measure of overall correctness. The CNN model shows that the precision and recall are also high at 98.60% and 98.50%, showing that it can correctly predict positives and can also capture most of the actual positive instances. In the case of the SVM model, precision is a little lower at 94.80%, which is compensated by the higher recall of 95.60%. Similarly, the RNN and KNN models with 91.50% and 89.60% precision, respectively, were seen to have distinct trade-offs in the context of precision and recall measures.

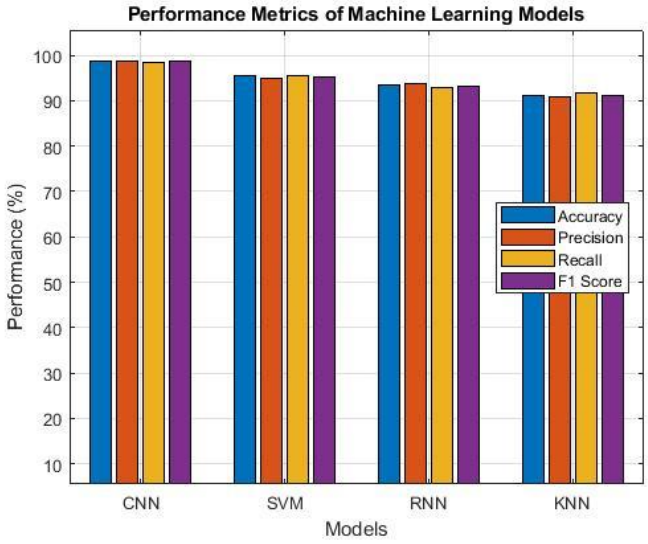

Figure 3. Confusion matrices of each model

The confusion matrix shown in figure 4, CNN model shows that its performance is outstanding, suggesting a high number of true positives and true negatives compared to false positives and false negatives . In other words, the CNN model seems to show exceptional performance in detecting the presence but also the absence of intruders since machine learns to differentiate between the cases of finding an intruder and those in which the potential intruder is not detected. A similar conclusion can be made regarding the SVM model, which, however, performed slightly worse compared to the CNN model. Indeed, the number of false positives and false negatives was slightly larger when the separate testing set was allowed against the model. The same concerns the RNN model which was successful in real-life training and testing but showed interesting performance in the test results. The same can be said about the KNN, as the results of the tests showed that this model may not only experience difficulties and thus anomalies in the future if the studies are continued but that it may also not perform very well in terms of classification. The CNN seems to be the most preferable option, as it could successfully detect intrusions with high accuracy. Its number of true positives and true negatives is the highest among all, while the number of false positives and false negatives is the lowest. It also seems to be very effective in terms of recognizing facial structure and, therefore, detecting intruders. The CNN model is the most successful in this case, and it should be recommended in the context of smart home applications.

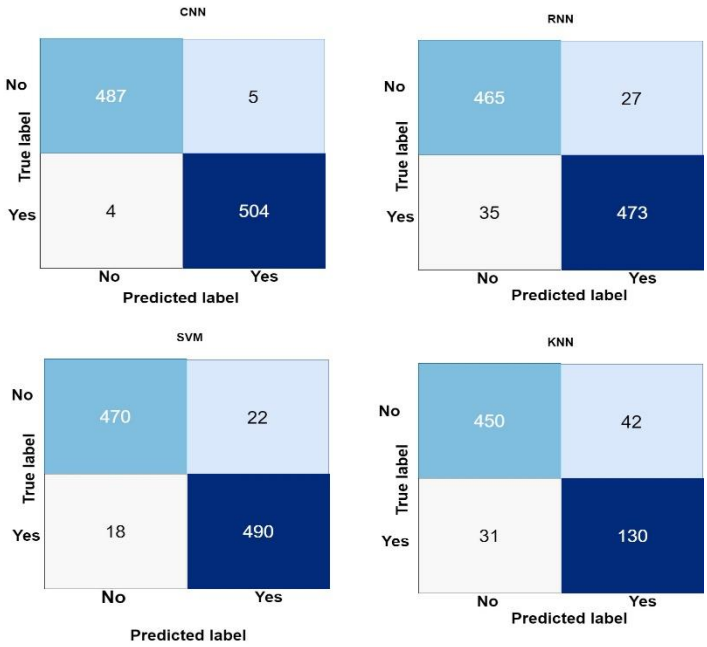

Figure. 4. Confusion matrices of each model

XI. CONCLUSION

The research has proved the efficiency of combining IoT-based multi-layer wireless sensor networks with machine learning algorithms for achieving seamless smart home automation and quality security control. Thanks to the well-prepared preprocessing and features of the sensors' data and advanced algorithms, such as CNNs, SVMs, RNNs, and KNNs, the system is efficient in intrusion detection, the difference between ordinary household processes and threats, and energy efficiency. With the help of confusion matrices, which helped to compare models used in the study, it was discovered that the CNN model is able to recognize intrusion in the most accurate way possible because of the qualities of face recognition and patterns identifying it possesses. Therefore, it is possible to conclude that the study has achieved its goals successfully. In the future, compared studies may be developed to help in the evaluation of the model on a larger scale and for real use in households. More research has to be focused on the problems of data security and privacy and the ways to improve the resistance of systems to the cyber-attacks. In this way, the results of this research are meaningful and contribute to the development of smart houses.

REFERENCES

[1] S. K. Bhoi *et al.*, "FireDS-IoT: A Fire Detection System for Smart Home Based on IoT Data Analytics," *Proceedings - 2018 International Conference on Information Technology, ICIT 2018*, pp. 161–165, 2018, doi: 10.1109/ICIT.2018.00042.

[2] C. Rodríguez-gallego, F. Díez-muñoz, A. Gabaldón, M. Dolón-poza, and I. Pau, "A collaborative semantic framework based on activities for the development of applications in Smart Home living labs," *Future Generation Computer Systems*, vol. 140, pp. 450–465, 2023, doi: 10.1016/j.future.2022.10.027.

[3] R. Kaur *et al.*, "Machine learning and price-based load scheduling for an optimal IoT control in the smart and frugal home," *Energy and AI*, vol. 3, p. 100042, 2021, doi: 10.1016/j.egyai.2020.100042.

[4] L. Ferreira, T. Oliveira, and C. Neves, "Consumer ' s intention to use and recommend smart home technologies : The role of environmental awareness," *Energy*, vol. 263, no. PC, p. 125814, 2023, doi: 10.1016/j.energy.2022.125814.

[5] K. P. Prakash *et al.*, "A comprehensive analytical exploration and customer behaviour analysis of smart home energy consumption data with a practical case study," *Energy Reports*, vol. 8, pp. 9081–9093, 2022, doi: 10.1016/j.egyr.2022.07.043.

[6] H. Khajeh, H. Laaksonen, and M. G. Sim, "A fuzzy logic control of a smart home with energy storage providing active and reactive power flexibility services," vol. 216, no. November 2022, 2023, doi: 10.1016/j.epsr.2022.109067.

[7] J. Zhen and M. Khayatnezhad, "Optimum pricing of smart home appliances based on carbon emission and system cost," *Energy Reports*, vol. 8, pp. 15027–15039, 2022, doi: 10.1016/j.egyr.2022.11.058.

[8] R. Fritz, K. Wuestney, G. Dermody, and D. J. Cook, "International Journal of Nursing Studies Advances Nurse-in-the-loop smart home detection of health events associated with diagnosed chronic conditions : A case-event series," *International Journal of Nursing Studies Advances*, vol. 4, no. May, p. 100081, 2022, doi: 10.1016/j.ijnsa.2022.100081.

[9] S. G. Liu, R. Liu, and S. Y. Rao, "Secure and efficient two-party collaborative SM9 signature scheme suitable for smart home," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 7, pp. 4022–4030, 2022, doi: 10.1016/j.jksuci.2022.05.008.

[10] S. H. Alsamhi *et al.*, "Machine Learning for Smart Environments in B5G Networks: Connectivity and QoS," *Computational Intelligence and Neuroscience*, vol. 2021, 2021, doi: 10.1155/2021/6805151.

[11] P. Jafarpour, M. Setayesh, and M. Shafie-khah, "Resiliency assessment of the distribution system considering smart homes equipped with electrical energy storage , distributed generation and plug-in hybrid electric vehicles Comfort Mode of Smart Home Saver Mode of Smart Home Energy Partner Mode of Smart," vol. 55, no. June, 2022, doi: 10.1016/j.est.2022.105516.

[12] K. Poh *et al.*, "ScienceDirect ScienceDirect Optimizing Energy Consumption on Smart Home Task Scheduling Optimizing Energy Consumption on Smart Home Task Scheduling using Particle Swarm Optimization using Particle Swarm Optimization," *Procedia Computer Science*, vol. 220, pp. 195–201, 2023, doi: 10.1016/j.procs.2023.03.027.

[13] A. Nawaz, A. Rizwan, R. Ahmad, and D. Hyeun, "Internet of Things An OCF-IoTivity enabled smart-home optimal indoor environment control system for energy and comfort optimization," *Internet of Things*, vol. 22, no. October 2022, p. 100712, 2023, doi: 10.1016/j.iot.2023.100712.

[14] L. Matindife, Y. Sun, and Z. Wang, "A Machine-Learning Based Nonintrusive Smart Home Appliance Status Recognition," *Mathematical Problems in Engineering*, vol. 2020, 2020, doi: 10.1155/2020/9356165.

[15] L. Zhang, Y. Tang, T. Zhou, C. Tang, H. Liang, and J. Zhang, "ScienceDirect Research on flexible smart home appliance load participating in demand side response based on power direct control technology," *Energy Reports*, vol. 8, pp. 424–434, 2022, doi: 10.1016/j.egyr.2022.01.219.

[16] A. Lara, V. Mayor, R. Estepa, A. Estepa, and J. E. Díaz-verdejo, "Internet of Things Smart home anomaly-based IDS : Architecture proposal and case study," *Internet of Things*, vol. 22, no. January, p. 100773, 2023, doi: 10.1016/j.iot.2023.100773.

[17] D. Buil-gil *et al.*, "Computers in Human Behavior The digital harms of smart home devices : A systematic literature review," *Computers in Human Behavior*, vol. 145, no. March, p. 107770, 2023, doi: 10.1016/j.chb.2023.107770.

[18] S. Mehra, A. Khatri, P. Tanwar, and V. Khatri, "Intelligent Embedded Security control system for Maternity ward based on IoT and Face recognition," *Proceedings - IEEE 2018 International Conference on Advances in Computing, Communication Control and Networking, ICACCCN 2018*, pp. 49–53, 2018, doi: 10.1109/ICACCCN.2018.8748516.

[19] K. Alfaverh, F. Alfaverh, and L. Szamel, "Plugged-in electric vehicle-assisted demand response strategy for residential energy management," *Energy Informatics*, vol. 6, no. 1, 2023, doi: 10.1186/s42162-023-00260-9.

[20] S. K. Bhoi *et al.*, "FireDS-IoT: A Fire Detection System for Smart Home Based on IoT Data Analytics," *Proceedings - 2018 International Conference on Information Technology, ICIT 2018*, pp. 161–165, 2018, doi: 10.1109/ICIT.2018.00042.

[21] C. Rodríguez-gallego, F. Díez-muñoz, A. Gabaldón, M. Dolón-poza, and I. Pau, "A collaborative semantic framework based on activities for the development of applications in Smart Home living labs," *Future Generation Computer Systems*, vol. 140, pp. 450–465, 2023, doi: 10.1016/j.future.2022.10.027.

[22] R. Kaur *et al.*, "Machine learning and price-based load scheduling for an optimal IoT control in the smart and frugal home," *Energy and AI*, vol. 3, p. 100042, 2021, doi: 10.1016/j.egyai.2020.100042.

[23] L. Ferreira, T. Oliveira, and C. Neves, "Consumer ' s intention to use and recommend smart home technologies : The role of environmental awareness," *Energy*, vol. 263, no. PC, p. 125814, 2023, doi: 10.1016/j.energy.2022.125814.

[24] K. P. Prakash *et al.*, "A comprehensive analytical exploration and customer behaviour analysis of smart home energy consumption data with a practical case study," *Energy Reports*, vol. 8, pp. 9081–9093, 2022, doi: 10.1016/j.egyr.2022.07.043.

[25] H. Khajeh, H. Laaksonen, and M. G. Sim, "A fuzzy logic control of a smart home with energy storage providing active and reactive power flexibility services," vol. 216, no. November 2022, 2023, doi: 10.1016/j.epsr.2022.109067.

[26] J. Zhen and M. Khayatnezhad, "Optimum pricing of smart home appliances based on carbon emission and system cost," *Energy Reports*, vol. 8, pp. 15027–15039, 2022, doi: 10.1016/j.egyr.2022.11.058.

[27] R. Fritz, K. Wuestney, G. Dermody, and D. J. Cook, "International Journal of Nursing Studies Advances Nurse-in-the-loop smart home detection of health events associated with diagnosed chronic conditions : A case-event series," *International Journal of Nursing Studies Advances*, vol. 4, no. May, p. 100081, 2022, doi: 10.1016/j.ijnsa.2022.100081.

[28] S. G. Liu, R. Liu, and S. Y. Rao, "Secure and efficient two-party collaborative SM9 signature scheme suitable for smart home," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 7, pp. 4022–4030, 2022, doi: 10.1016/j.jksuci.2022.05.008.

[29] S. H. Alsamhi *et al.*, "Machine Learning for Smart Environments in B5G Networks: Connectivity and QoS," *Computational Intelligence and Neuroscience*, vol. 2021, 2021, doi: 10.1155/2021/6805151.

[30] P. Jafarpour, M. Setayesh, and M. Shafie-khah, "Resiliency assessment of the distribution system considering smart homes equipped with electrical energy storage , distributed generation and plug-in hybrid electric vehicles Comfort Mode of Smart Home Saver Mode of Smart Home Energy Partner Mode of Smart," vol. 55, no. June, 2022, doi: 10.1016/j.est.2022.105516.

[31] K. Poh *et al.*, "ScienceDirect ScienceDirect Optimizing Energy Consumption on Smart Home Task Scheduling Optimizing Energy Consumption on Smart Home Task Scheduling using Particle Swarm Optimization using Particle Swarm Optimization," *Procedia Computer Science*, vol. 220, pp. 195–201, 2023, doi: 10.1016/j.procs.2023.03.027.

[32] A. Nawaz, A. Rizwan, R. Ahmad, and D. Hyeun, "Internet of Things An OCF-IoTivity enabled smart-home

optimal indoor environment control system for energy and comfort optimization," *Internet of Things*, vol. 22, no. October 2022, p. 100712, 2023, doi: 10.1016/j.iot.2023.100712.

[33] L. Matindife, Y. Sun, and Z. Wang, "A Machine-Learning Based Nonintrusive Smart Home Appliance Status Recognition," *Mathematical Problems in Engineering*, vol. 2020, 2020, doi: 10.1155/2020/9356165.

[34] L. Zhang, Y. Tang, T. Zhou, C. Tang, H. Liang, and J. Zhang, "ScienceDirect Research on flexible smart home appliance load participating in demand side response based on power direct control technology," *Energy Reports*, vol. 8, pp. 424–434, 2022, doi: 10.1016/j.egyr.2022.01.219.

[35] A. Lara, V. Mayor, R. Estepa, A. Estepa, and J. E. Díaz-verdejo, "Internet of Things Smart home anomaly-based IDS : Architecture proposal and case study," *Internet of Things*, vol. 22, no. January, p. 100773, 2023, doi: 10.1016/j.iot.2023.100773.

[36] D. Buil-gil *et al.*, "Computers in Human Behavior The digital harms of smart home devices : A systematic literature review," *Computers in Human Behavior*, vol. 145, no. March, p. 107770, 2023, doi: 10.1016/j.chb.2023.107770.

[37] S. Mehra, A. Khatri, P. Tanwar, and V. Khatri, "Intelligent Embedded Security control system for Maternity ward based on IoT and Face recognition," *Proceedings - IEEE 2018 International Conference on Advances in Computing, Communication Control and Networking, ICACCCN 2018*, pp. 49–53, 2018, doi: 10.1109/ICACCCN.2018.8748516.

[38] K. Alfaverh, F. Alfaverh, and L. Szamel, "Plugged-in electric vehicle-assisted demand response strategy for residential energy management," *Energy Informatics*, vol. 6, no. 1, 2023, doi: 10.1186/s42162-023-00260-9.