Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606

Volume 07 Issue 01
2024

Research Article
https://doi.org/10.56979/701/2024

Integrating IoT and Machine Learning to Provide Intelligent Security in Smart Homes

Saira Batool[1], Muhammad Kamran Abid[1*], Muhammad Asjad Salahuddin[2], Yasir Aziz[3], Ahmad Naeem[1], and Naeem Aslam[1]

[1]NFC Institute of Engineering and Technology, Multan, Pakistan.
[2]Department of Computer Science, University of Alabama at Birmingham, Birmingham, AL 35294, USA.
[3]Bahauddin Zakariya University, Multan, Pakistan.
[*]Corresponding Author: Muhammad Kamran Abid. Email: kamranabidhiraj@gmail.com

Received: January 23, 2024 **Accepted:** May 01, 2024 **Published:** June 01, 2024

Abstract: The technology is built entirely on the IoT and ML methods and is very desired in the sector of security. This method allows consumers to secure and regulate their homes. The system is used to track the treats in real time with response mechanism that detect with different sensor and send feed security information through internet. Smart home offer intelligent, real-time threat detection and response capabilities by utilizing decision tree, transfer learning logistic regression and SVM models. Smart home collects, preprocessed and trained data from many IoT sensors, such as cameras and motion detectors and then apply Ml models to detect the threads and perform the action according to requirements. A total accuracy of 0.992 indicated the model's strong performance, confirming its suitability for practical use. Decision tree and transfer learning models perform higher Accuracy rates than SVM and logistic regression. These findings highlight the great potential of fusing IoT and machine learning technologies to produce flexible, effective, and scalable security solutions. They also offer a strong foundation for the implementation of dependable and high-performing machine learning models in real-world smart home security systems.

Keywords: IOT; ML; Decision Tree; Logistic Regression; SVM; Transfer Learning; Smart Home.

1. Introduction

According to research, the smart home industry is expected to develop significantly, tripling in size by 2020 due to the appeal of the idea to consumers. Smart homes specific market by product (energy management system, security and entertainment control, access control, and HVAC control), protocol, technology (protocol, communication technology and cellular technology) ,service (customization installation), and geography (Europe, North America, APAC and ROW) forecast and trend to 2020 In addition, a recent market analysis projects that the smart home market will reach US$58.68 billion in 2020, growing by 17% yearly between 2015 and 2020 [1]. The interest in smart houses, both commercially and academically, has increased significantly since the 1980s. Governments and research organization in the UK, US and Japan have all made investments in the study and advancement of smart home service development [2].

With their abundance of linked items, smart homes provide countless opportunities to enhance our quality of life in context of comfort, convenience, and ease. Wireless gadgets in smart homes are outfitted with an array of sensors to keep an eye on the automation or management of the living space, thereby enhancing the quality of life for the occupants [3].

IoT devices can connect to the internet via a variety of methods, including cellular networks Wi-Fi, and Bluetooth, and like 4G and 5G. The market size for IoT is expected to reach 1.5 billion dollars globally by 2027, driven by the growing adoption of connected devices across various industries [4].

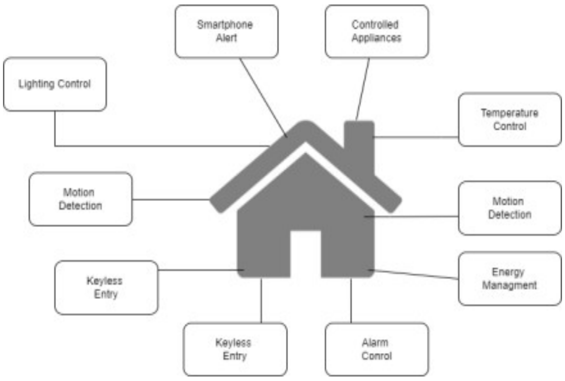

Figure 1. IoT Based Smart home

The Internet of Things (IoT) looks to be a key component of modern information technology and a significant development in this period given the rapid growth of information and communication technology (ICT). IoT integration has definitely improved the comfort and quality of life in smart homes, but it has also brought new risks and weaknesses, especially with regard to privacy and security in the quickly evolving landscape of technologies, the convergence of machine learning (ML) and Internet of Things (IoT) has combined as a transformative force, it can influence numerous aspects of our daily lives. The integration of ML and IoT to give intelligent security solutions within smart homes. The idea of smart homes has been grown in recent years due to machine learning and other technological development have built it possible to create more responsive and intelligent living spaces. Smart homes join or integrate networked devices, actuators and sensors to optimize consumption of energy, improve security, and also customize the living environments [5]. By being able to learn about the patterns, preferences and context of the user through machine learning algorithms combined with smart home systems we can reach new levels of convenience comfort, and efficiency [6].

1.1. Activity Recognition

Smart home technology can learn from sensor data of smart homes and smart appliances. We use it to trace possible patterns of human activity. The smart homes could do this by automatically performing activities such as, turn on/off lights, close/open doors etc. A smart building can include systems such as heating, ventilating, and air conditioning and lighting and temperature controls as per the routine of the inhabitants [7].

1.2. Energy Management

The automation which integrates learning machines would also regulate and strive to lessening the consumption of power as the houses continue to learn the preferences or inclinations concerning the tendencies of the occupants. Refined models of prescriptive may focus on coupling in energy consumption as well as gadgets that enables heating and cooling to minimize wastage and odds related to utility bills [8].

1.3. Security and Anomaly Detection

The application of artificial intelligence creates a way through which smart home systems can track certain signs that may point out some signs of security risks and other abnormalities. These algorithms work by processing sensor data coupled with human behavioral data to differentiate between normal physical exercise and acts of suspicious movement. This enables them to start the appropriate measures, such alarm systems or automated lockdown procedures [9].

The integration of machine learning techniques has the ability to improve the security posture of smart home systems. Machine learning algorithms, powered by the huge amounts of sensor data generated by Internet of Things devices, enable real-time pattern analysis, anomaly detection, and risk prediction.

1.4. Emergence of Smart Home Technologies

A paradigm shift in residential living is marked by the emergence of smart home technologies, which are driven by advancements in data analytic, sensor technology, and networking. Smart homes provide previously unheard-of levels of automation, comfort, and energy efficiency thanks to the integration of thermostats, lighting controls, security cam- eras, entertainment systems, and other technologies into one seamless ecosystem [10]. The following are important smart home technology enablers:

1.4.1. Internet of Things (IoT)

Intelligent or smart home ecosystems are built on the IoT paradigm, which is defined by the physical device's internet-based connectivity. IoT enabled gadgets with sensors and actuators may talk to centralized control systems and each other in order to automate, monitor, and remotely manage home surroundings [11].

1.4.2.Wireless Connectivity

The seamless or ideal connection between smart home devices made possible by technologies like Wi-Fi, Z-Wave Bluetooth, Zigbee, eliminates the need for intricate wiring installations and offers a variety of deployment alternatives [12].

1.4.3. Sensor Technology

The creation of small, inexpensive sensors that can detect a range of environmental factors, including motion, light, temperature, and humidity, is the result of advancements in sensor technology. These sensors provide real time data that informs automation, decision-making and decision support system acting as the eyes and ears of smart home system [13].

1.4.4. Cloud computing and data analytics

Platforms for cloud computing offer scalable storage and processing power to handle and examine the massive volumes of data produced by smart home appliances [14].

1.4.5. Interconnected Nature of Smart Homes

Smart homes are networked, signifying the smooth integration of ML and the IoT to revolutionize residential living experiences. Real time data collection from various equipment and settings is accomplished in smart homes through the usage of IoT devices and sensors. Smart homes are able to adapt to changing conditions, learn from human preferences, and optimize functioning [15].

1.4.6. Integration of IoT Sensors

With the ability to collect an abundance of real time environmental data, integrated IoT sensors in smart homes serve as the ecosystem as eyes and ears. From motion detectors and smart appliances to temperature and humidity sensors, these sensors continuously collect data on the environment around the home and the activities of its occupants [16].

The MQTT dataset from Kaggle used for the machine learning algorithms. One lightweight publish-subscribe messaging protocol used for IoT (Internet of Things) and M2M (Machine to Machine) communication is called MQTT (Message Queuing Telemetry Transport). Simple, effective, and appropriate for limited devices and low bandwidth, high latency, or unstable networks, it is meant to be simple to use. MQTT datasets are used by scientists for a broad range of purposes, which include real time decision making, edge computing, longitudinal studies, QoS optimization, security evaluation, protocol specific analysis, and privacy protection. [17].

1.5. Significance of the Study

Smart homes are networked is crucial to many different fields, particularly when it comes to ML and the IoT. Innovations in this field of technology foster innovation and allow for the development of intricate systems, protocols, and algorithms that enhance security, maximize energy efficiency, and streamline automation in smart home settings. Through the use of ML techniques, large quantities of IoT generated data may be analyzed, allowing smart homes to anticipate requirements, adjust to user preferences, and deliver personalized experiences that raise the bar for residential living. Moreover, knowing the intricate integration of smart technology in homes, centered designs and less complex interfaces can be created, where the owners of these homes are capable of efficiently interacting with their home environment. On a normal basis, mundane tasks may be predicted and controlled in advance comprehensively through the use of machine learning algorithms applied in smart homes to enhance comfort and satisfaction among occupants. These algorithms are trained with the principles of human behavior, their choices, and daily habits. Designers and developers who give focus on the user experience and accessibility can ensure that the smart home technologies are easily understandable and easier to use; thereby, making it inclusive and accommodating the different needs and expectations of the occupants.

2. Literature Review

Enhancing security is one of the many advantages of integrating IoT and ML technology in smart homes. This can be developing other smart home gadgets or tools and service which will adaptable environments and digital systems, smart home technology goal to enhance the everyday living. However, because Internet of Things devices are frequently targets of assaults, smart home technology has security issues. Through anomaly detection and access control, machine learning algorithms may improve security in smart homes [18]. Technology adoption depends on consumers accepting and integrating smart home technology into their daily life, which calls for a user- centered approach to smart home design. Through generalization of user behavior and adapting to their tendencies, the application of machine learning (ML) algorithms may be incorporated into smart home security systems for optimal user experience, [19]. The elements used to build a smart home are generally from several sectors, including technology, places, and services. Thus, the incorporation of ML algorithms into smart home security systems can contribute to the enhancement of the general architecture structure of smart homes [20]. The ML algorithms use for smart home security system work more accurate to emerging risks and threats in the future. [21]. Motivation for integrating IoT and ML for enhanced security in smart homes:

- Improved security posture: IoT and Ml collectively subject to cyberattacks, abnormalities identify by ML algorithms, after detecting abnormalities ML techniques stop unwanted or illegal access, made smart home more secure [22].
- Adaptive security measures: I comparison to traditional rules-based protections, by using AI/ ML algorithms for determining scopes of selections conditions, system restrictions may be adapted depending on user or device patterns served.
- Usability: Security system that is tailored to learn behavior and automatically account for different preferences which in result would provide a well-behaved smart home [23].
- Cost effective solutions: Low computational demands can be useful for creating the security much more affordable using ML algorithms that work quite well, and thereby making them suitable to deploy on IoT devices as they are low processing power systems.
- Real-time monitoring: Real-time security danger and area of concern identification is possible with the use of ML algorithms, which allows smart home devices to respond quickly to areas that need attention.
- Less false alerts: By enhancing the underlying models, machine learning-based systems and algorithms lessen user strain and boost the overall effectiveness of smart home security solutions. This helps to decrease the quantity of false alerts created. Access constraints and data randomization might safeguard user privacy. Machine learning techniques [24] [25].

2.1. Challenges Facing Smart Home Technology

Issues with Standardization and Interoperability: A Smart Home Technology the smooth integration of devices and systems is hampered by compatibility problems and a lack of industry standards. Cyber security Risks: Hacking, malware, and data breaches can affect smart home devices, putting users' security and privacy at risk. Installation and Configuration Complexity: Many consumers find that setting up and configuring smart home devices may be difficult and time-consuming, which can have an impact on adoption rates [26]. Cost and affordability: The initial outlay of funds necessary for smart home technology continues to be a turnoff for certain customers, which prevents a broad adoption. Ownership and Data Privacy: There are moral and legal issues raised by worries about ownership and data privacy as well as the possible misuse of personal data gathered by smart home devices.

2.1.1.An overview of IoT uses in smart homes

People as interactions with their living surroundings have been completely transformed by IoT applications in smart homes. These are a few of the most important Internet of Things uses in smart homes.

1. Control and Automation of the Home: With the use of linked devices and sensors, such as security cameras, smart lighting controls, and thermostats, homeowners may automate and manage many parts of their homes from a distance.
2. Efficiency and Management of Energy: In order to support energy conservation and sustainability initiatives, Internet of Things (IoT) devices track patterns in energy consumption and use clever algorithms to optimize utilization [27].
3. Monitoring and Safety at Home: Sensors, cameras, and alarms are all combined in IoT enabled security systems to provide alerts and monitoring and alerts, enhancing home security and residents' peace of mind [28].

2.1.2. Limitations of IoT based smart homes

IoT-based smart homes come with a host of security, privacy, and functional problems. These are serious problems. Some of the primary barriers and limitations include the following:

1. Latency and Data Security: Both data latency and security are issues that IoT and ML deal for home automation. The data security and data latency problems can improve through fog computing
2. Interoperability and Integration: Latency and data security are two issues that IoT-based smart home automation has to handle. Fog computing and standard protocols can be used to improve data security and address latency problems.
3. Vulnerabilities and assaults: Hackers can utilize smart home devices for a variety of malicious goals, including distributed denial of service (DDoS) assaults, data theft, and device hijacking. These devices are open to several data breaches.
4. User Data Protection: The smart home tools develop significant concerns about privacy and user data protection. Unwanted approach to monitoring or accessing equipment and the data breaches both are privacy issues related with smart homes [29] [30].
5. Privacy and data protection: Concerns regarding privacy and user data protection are brought up by the inter connectedness of smart home appliances [31].

2.1.3. Machine Learning Applications in IoT

Predictive maintenance with the use of real-time data collected from sensors, machine learning applications in the Internet of Things, including predictive maintenance, foresee equipment breakdowns and provide timely remedies. This method assists in: 1. Lowe expenses 2. Improve output 3. Boost the use of machinery 4. Cut down on idle time 5. Enhance the durability of equipment Proper imple- mentation of predictive maintenance systems may lead to very accurate predictions, frequently above 90% [32]. Generally, the procedure entails the subsequent actions: 1. Gathering data in real time from sensors 2. Sending information to a centralized, cloud-based data storage system 3. Using algorithms and machine learning to analyze data 4. Estimating the potential time of failure 5. Planning ahead for maintenance duties.

2.1.4. Overview of ML techniques in IoT systems

Machine learning techniques in IoT systems for smart homes include: Predictive maintenance Anomaly detection, personalization, Environmental monitoring, resource optimization These methods facilitate better decision making, minimize downtime, and maximize resource efficiency. For Internet of Things applications in smart homes, a few of the frequently utilized machine learning algorithms include.

2.1.4.1. Random Forest

Random Forest is an ensemble learning technique that uses many decision trees to provide accurate predictions about the class labels of incoming data. Random Forest is well known for its ability to handle complex and high dimensional data with resilience and accuracy in classification tasks. It has been used by IoT systems to detect botnet attacks, improve malware recognition for IoT devices, and generate rules for detecting anomalies in real time. It has also been used by predictive maintenance systems to predict equipment failures and provide timely fixes. In this cases, Random Forest has generated high diagnosis percentage of up to 99.6% [33-35].

2.1.4.2. Support vector Machine

SVM are powerful supervised learning algorithms that are often applied to classification and regression issues. Support vector machines (SVMs) are flexible and effective in high- dimensional spaces by finding the optimum hyperplane that divides data points of different classes with the largest margin. SVMs have a range of kernel functions to handle non-linear data. Interestingly, SVMs have shown useful in several domains, including text categorization, picture recognition, bioinformatics, and financial forecasting [36].

2.1.4.3. Decision Tree

A machine learning approach called decision trees may be used to a variety of IoT applications, such as cybersecurity, anomaly detection, and healthcare monitoring. Decision trees are flexible prediction models that pick-up knowledge from reasoning and observations. They are helpful for classification issues and are used to represent and classify occurrences. IoT systems have processed medical data, identified abnormalities in smart surroundings, and implemented security fixes for vital IoT systems using decision trees. The algorithm makes decisions easier to comprehend and explain by illustrating every conceivable outcome through the use of a branching mechanism [37].

Table 1. Machine learning models accuracy comparison

Reference	Techniques	Accuracy	Limitations
[37]	(GBM), (RF), and Multi-Layer Perceptron Neural Network (MLP)	97.95% for binary classification on network data 98.39% with IoT information	Existing ML based NIDSs have limited ability to adapt to changing network environments.
[38]	Reprocessing techniques like Normalization and Data set Scaling were utilized	Logi-CB 85.6 % Logi-XGB, Logi-GBC Logi-ABC achieved of 80.2%, 77.8%, and 80.7%	Works for hybrid developed methods.
[39]	Logistic Regression,K-Nearest Neighbors, and SVM	Detection models generated By traditional and ensemble classification ML method show outstanding overall performance with accuracy over 98.8%	Limitation of Hardware resources in smart home devices. Various OS of current OS of current smart home devices
[40]	Logistic regression, Random Forest, Extreme Gradient Boosting, and Light Gradient Boosting Machine classifiers	Proposed intrusion detection model achieves 99.92% accuracy.	LGBM library of ML used for proposed intrusion detection model.
[41]	Feature selection and hyper parameter tuning Machine and Deep learning techniques	N/A	classification minimized compared to state-of-the-art solutions Proposed scheme outperformed only MLDL schemes
[42]	ML algorithms outperform DL models for some devices/attacks	N/A	Existing IDS are inefficient in IoT due to limited computation capability, mobility, and large scale of the network. ML models outperform DL models for some devices /attacks in Smart home.
[43]	Preprocessing techniques: Normalization and Scaling of Dataset. Feature engineering algorithms for extracting features for text data	algorithm achieved The highest accuracy of 85.66% in detecting attacks and anomalies In an IoT environment in a smart home.	Limited to internal network intrusion detection. Trains only on external data and traffic.
[434]	Deep learning methods are to build data features. Fuzzy technique is used to analyze attack.	The detection rate for denial of service attack and remote illegal access is 94%	The proposed method only improves the detection rate of attacks.
[45]	Deep learning Method	Deep learning models are Optimal for estimating prediction performance and	Only Deep learning-based technique

3. Methodology

One lightweight publish-subscribe messaging protocol used for IoT (Internet of Things) and M2M (Machine to Machine) communication is called MQTT (Message Queuing Telemetry Transport). Simple, effective, and appropriate for limited devices and low-bandwidth, high-latency, or unstable networks, it is meant to be simple to use [46]. Strong security measures are provided by security evaluations and vulnerability investigations, user privacy and a protect systems. Researchers maximize protocol utilization and increase interoperability with the investigation of MQTT message payloads as well as communication patterns. Planning and adaption for the long run are aided by longitudinal studies that monitor changes in smart home behavior over time. In the end, innovations that improve the effectiveness, intelligence, and user experience of future smart home settings are driven by MQTT datasets

In datasets number of sensors for measuring light intensity, humidity, and temperature is displayed on the datasets. Name of the sensor, address, IP address, room, time (random or periodic), subject, and data profile are all given. The datasets have 8 columns. Sensor, Address, IP. Room, Time' Topic Data Profile.

3.1. Machine Learning Model

3.1.1. Logistic Regression model

Logistic regression is a binary classification technique that estimates the probability of a given input falling into one of two classes. Our instance includes the" occupied" and" unoccupied" classes. [48].

1. Occupancy Detection: Occupancy detection is a feature of smart homes; logistic regression may be used to predict whether or not a certain room or area will be occupied based on information from various sensors. The developed logistic regression model extended for drawing conclusions based on occupancy sensor data, motion detectors, and other appropriate sensors the historical data of occupancy, with regard to the system's ability to determine whether or not a room was occupied at the time the data was collected. Subsequently, this data facilitates the adjustment of light intensity and opens channels for energy, temperature, and security system control [49] [50].
2. Energy Management: A useful technique for predicting trends in energy use in smart homes is logistic regression. A logistic regression technique may look at characteristics like the time of day, the environment, and tenant behavior to determine energy demand levels and identify opportunities for savings or efficiency [51] [52].
3. Behavior Analysis: It is possible to examine how occupants behave in a smart home setting using logistic regression. Logistic regression analysis techniques are used to identify patterns and abnormalities in data collected from various sensors, including door sensors, motion sensors, and smart home devices.

3.2. Smart Home Activity Recognition

Smart home gadgets proceed to human behaviors by using task detection, which enhances security convenience, and energy efficiency.

3.3. SVM

SVM are essential for smart homes, especially for task such as activity recognition, anomaly detection, occupancy monitoring, problem diagnostics and energy management. SVM models employ sensor data to identify activities, optimize energy use, detect abnormalities, identify issues in the smart home environment, and classify occupancy status.

3.4. Decision Tree

Decision Tree are hierarchical tree structures in which a decision based on a feature is represented by each internal node, a decision's consequence is represented by each branch, and a class label is represented by each leaf node. Recursive partitioning of the feature space serves as the foundation for the decision-making process.

3.5. Transfer Learning

Applying skills or models which have been learned on one task or domain to improve efficiency or productivity in associated activity or domain within a smart home system is known as" transfer learning" in regards to intelligent homes [53].

- Sensor Fusion and Context Awareness: When used along with transfer learning and deep learning, details received from different sensors such as temperature, light and movement detectors can efficiently be used in an intelligent house. The effective and desired goals of sensors can be raised and enhanced whenever models are trained to identify the exercises taking place bound to intelligent homes. As an example, one developed from data gathered by motion detectors may contain details to recognize certain actions such as watching television and preparing food.
- Adaptive Behavior and Customization: Transfer learning enhances the capacity for smart home systems to be more tailored to the preferences and role of the particular user. The consumption models for smart homes founded on the sum of data which is collected by the electronic devices of different users might be developed in order to match the personalized offers to each consumer and his usage schedule.

- Anomaly Detection and Security: Through the models trained from similar context or data sets, the transferred learning is for use in improving security as well as detecting anomalies in home automation systems. In order to analyze data and detect possible abnormalities specific to the case of smart homes, it is possible to reuse methodologies that were developed in different domains such as cybersecurity or manufacturing with the models as modified so that they identify different types of abnormality.
- Adaptation to Changing Environments: Home automation systems can adapt to changing user preferences and evolve with the times thanks to transfer training. If systems were developed based on historical data from similar electronic home environments, they could be exported and modified to fit new users, gadgets, and environmental conditions.

4. Results and Discussion

4.1. Evaluation Metrics development

4.1.1.Decision Tree

The method of classification performs effectively in general, correctly recognizing the majority of cases across a variety of cyber-attacks and innocuous traffic, according to the examination of the confusion matrix. These insights emphasize the need for further development of the model, possibly through increased feature engineering or additional training data, to improve its accuracy and dependability in detecting a broader spectrum of cyber threats.

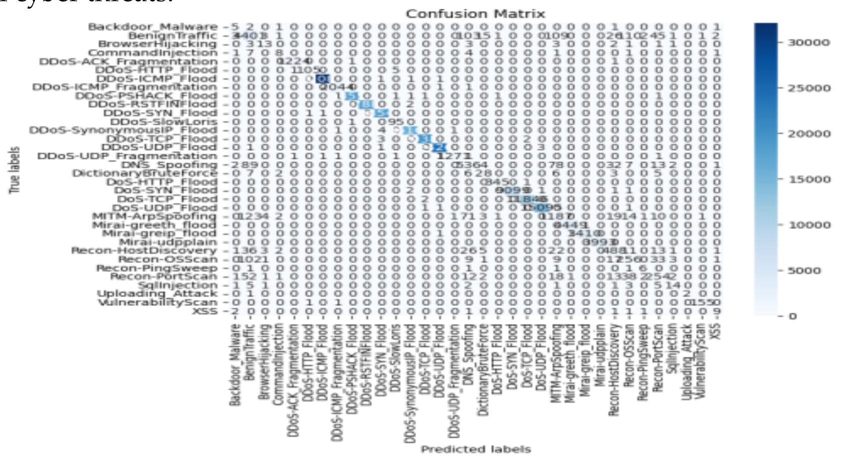

Figure 2. Decision Tree Confusion matrix

4.1.2. Logistic Regression

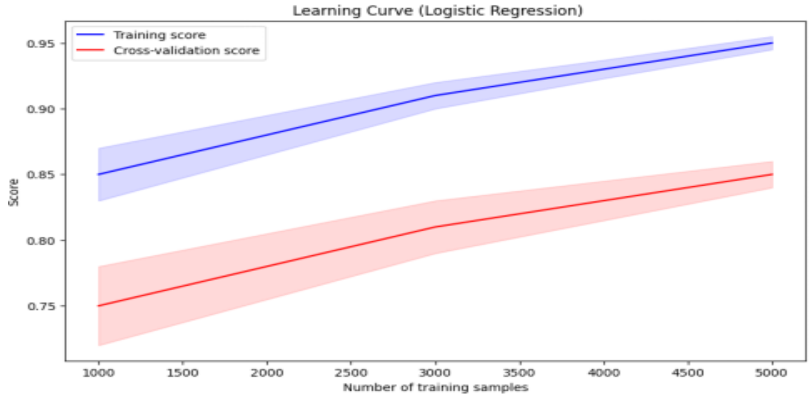

Figure 3. logistic Regression Confusion Curve

The link between the quantity of samples used for training and the model's performance as indicated by the training score and cross-validation score is displayed in the curve of learning for a logistic regression model. The amount of training samples, which ranges from 1,000 to 5,000, is shown by the x-axis, while the model's score is displayed on the y-axis. The training score is represented by the blue line, and when more samples are added, the accuracy increases. The shaded area shows the confidence interval. The cross-validation score is shown by the red line; it is likewise rising but is constantly less than the training score, suggesting some degree of over fitting. Given that both scores are trending upward, it is possible that adding more training data can enhance model performance even more and narrow the difference between cross-validation and training scores.

4.1.3. Transfer Learning

The transfer learning model's learning curve illustrates how the model's performance changes as the number of training samples increases, from 1,000 to 5,000. The blue line shows the training score, which starts high at roughly 0.96 and rises slightly to roughly 0.98. A small confidence interval indicates consistent performance. As more samples are added, the cross-validation score, represented by the red line, begins lower at roughly 0.85 and rises to about 0.95, with its confidence interval decreasing to reflect more stable estimates. A little amount of over fitting is shown by the difference between the training and cross-validation scores, but as the number of samples increases, this difference closes, indicating better generalization.

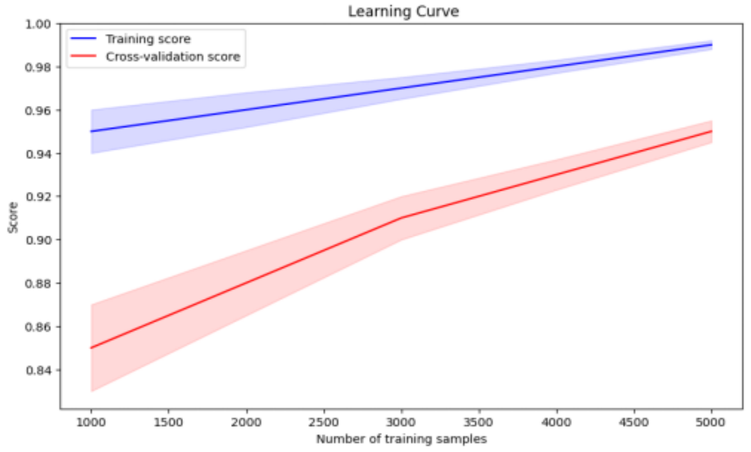

Figure 4. Transfer Learning curve

4.2. Accuracy comparison

The bar chart provides the comparison between four machine learning models it shown the accuracy of results, which model perform more accurate than other the decision algorithm provides more accuracy percentage than SVM, Logistic regression and transfer learning. The decision tree has 0.9928 accuracy while SVM have 0.9028 logistic regression have 0.9328 and transfer learning have 0.9904 accuracy.

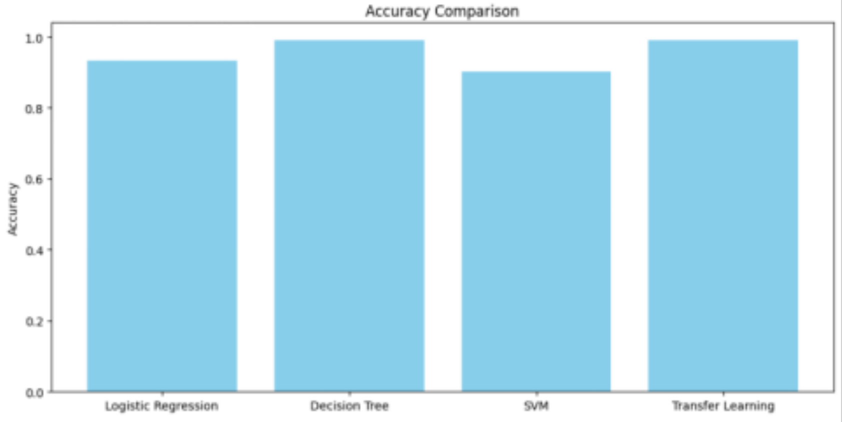

Figure 5. Accuracy Comparison bar chart shows the accuracy between logistic regression, Decision Tree , SVM and transfer learning

4.3. Precision Comparison

The bar chart shows the models precision results of logistic regression, decision tree, SVM and transfer Learning. Decision tree algorithm precision is more than other, decision tree has 0.992 precision while others SVM have o.9128 logistic regression has 0.9428 and transfer learning have 0.9908.

The precision of machine learning models Logistic Regression, Decision Tree, Support Vector Machine, and Transfer Learning is compared in the accompanying line figure. The models with the highest precision, Decision Tree and Transfer Learning, each at roughly 0.99, show that they are much superior in terms of accurately detecting pertinent cases. On the other hand, with a precision of roughly 0.91, the SVM model has the lowest precision, and Logistic Regression does marginally better, at roughly 0.94.

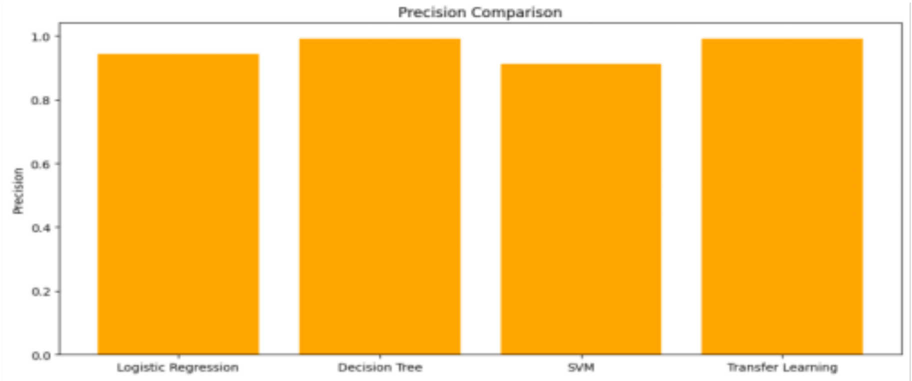

Figure 6. Precision/ Comparison bar chart shows the accuracy between logistic regression, Decision Tree, SVM and transfer learning

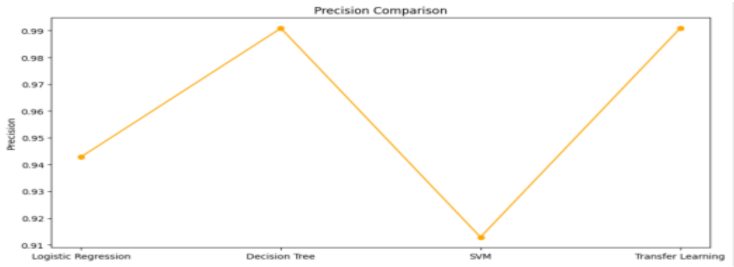

Figure 7. precision graph shows the accuracy between logistic regression, Decision Tree, SVM and transfer learning

4.4. F1 Score Comparison

Good balance between recall and precision is indicated by excellent F1 scores for all models. Decision Tree and Transfer Learning have somewhat higher scores, near 1.0, although SVM and Logistic Regression both have F1 ratings of about 0.9.

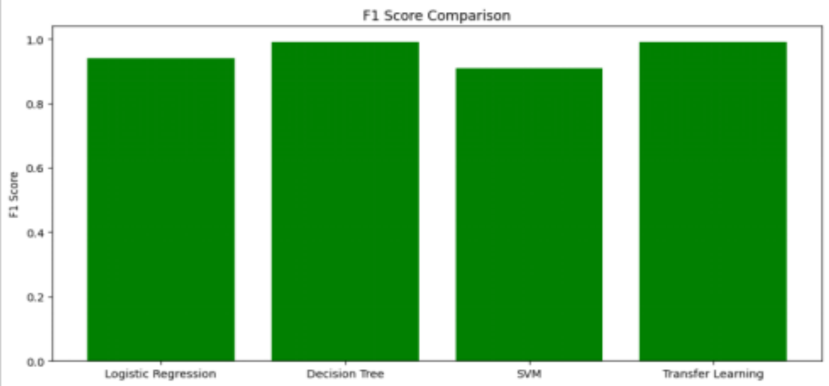

Figure 8. F1 Score bar chart between logistic regression, Decision Tree, SVM and transfer learning.

Table 2. Table shown the Overall model performance

ML Model	Accuracy	Precision	F1 Score
Decision Tree	0.9928	0.992	0.992
SVM	0.9028	0.9128	0.9092
Transfer Learning	0.9904	0.9908	0.9906
Logistic Regression	0.9328	0.9428	0.9328

4.5. Metric Distribution

In this experimental design we used threefold designs that debug the proportion of the training sets to the test sets and then obtained the corresponding values of metric with the shown figure 12. The model obtained a accuracy score 0.992, a precision score of 0.992, a F1 score of 0.992, respectively. The outcomes clearly shown how demonstration is effectively remarkable.

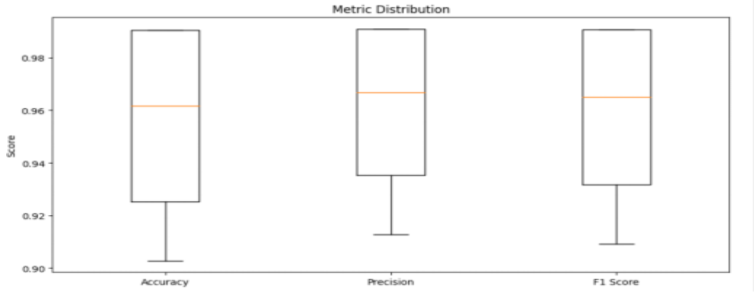

Figure 9. Box-whisker plot for three-fold accuracy precision and F1 score experimental design

4.6. Performance metric comparison

The performance measures (Accuracy, Precision, and F1 Score) for four machine learning models Logistic Regression, Decision Tree, SVM, and Transfer Learning are compared in this bar chart. The performance measures (Accuracy, Precision, and F1 Score) for four machine learning models Logistic Regression, Decision Tree, SVM, and Transfer Learning are compared in this bar chart. Outperforming all other models in every metric assessed, Decision Tree and Transfer Learning are the most efficient models. Not the best, but good enough Logistic regression performs adequately, falling short of Decision Tree and Transfer Learning in terms of performance. Out of the four models that were assessed, SVM had the lowest performance despite being consistent.

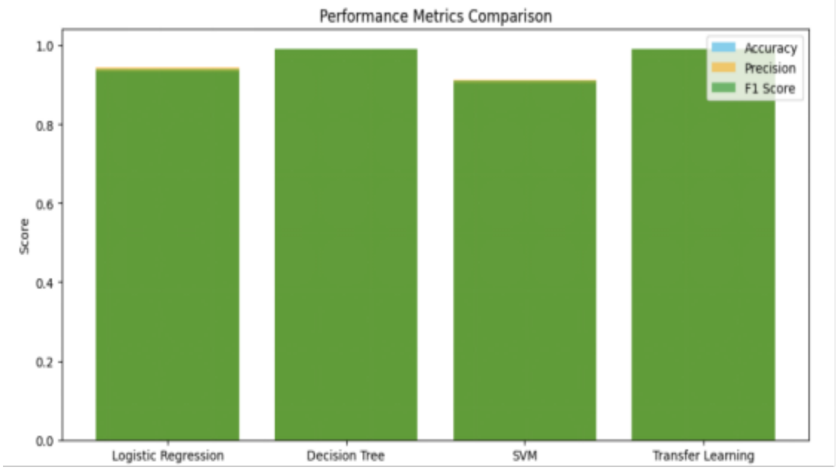

Figure 10. Performance comparison across models

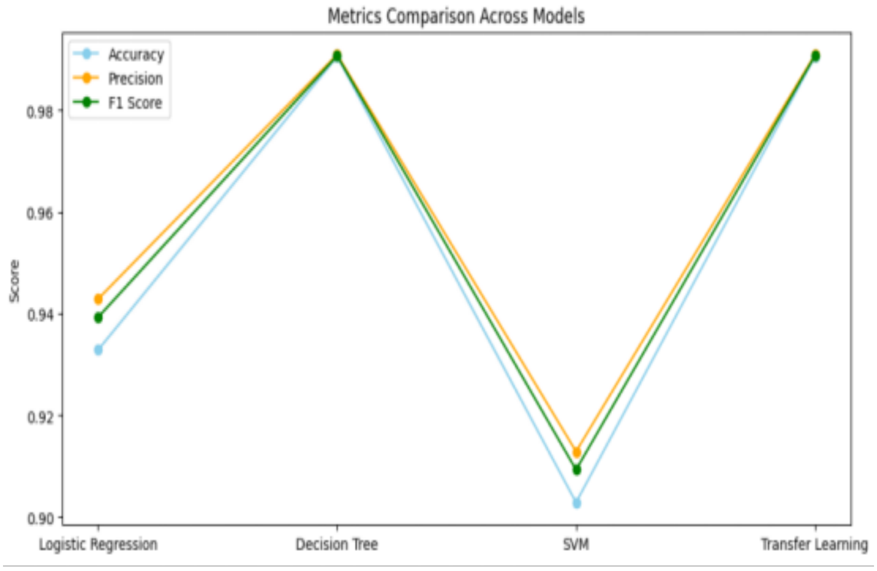

Figure 11. Performance comparison across models

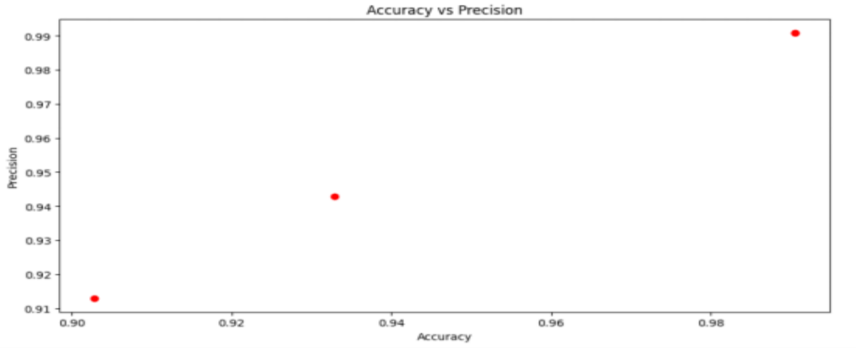

Figure 12. Accuracy and Precision Comparison

4.7. Comparison Accuracy Vs precision

Three distinct machine learning approaches are compared in terms of precision and accuracy using a scatter plot. Based on these two criteria, each red dot shows how well a model is performing. A thorough plot analysis is provided below: At X-axis (accuracy) it shows how accurate the models are; it ranges from 0.90 to about 0.99 A higher percentage of accurate predictions is shown by higher values. Y-axis (Precision)it Represents the models' precision, with a range of 0.91 to 0.99. Greater numbers denote a higher percentage of accurate positive predictions among all the model's positive predictions. Red dots, or data points are accuracy and precision of a model's performance is indicated by each red dot. The prior analysis is graphically confirmed by this figure, which shows that SVM is the least effective model for the problem at hand, Logistic Regression is mediocre, and Decision Tree or Transfer Learning models are excellent.

5. Conclusion

In order to improve security in smart homes, this study investigated the integration of machine learning algorithms with Internet of Things (IoT) devices. Specifically, decision tree models were used to detect threats intelligently and in real time. IoT sensors were installed, data was collected and preprocessed, engineering features were selected and applied, decision tree model was built, evaluated, and the final decision tree model was deployed onto a smart home system. Overall, the results demonstrated that the integration of the IoT application and decision tree models effectively provides high and automatic alerts on potential security threats, which can act as a powerful approach to identify and prevent malicious behavior and unauthorized access. This is because the decision tree model has high interpretability, meaning users' confidence and trust will be highly boosted in the system, which analyzes data in real time so that possible breaches such as DDoS-HTTP Flood, Backdoor Malware and DoS-Slow Loris may be detected promptly. In addition to the decision tree, the research also compared other models such as Transfer Learning, Support Vector Machine (SVM), and Logistic Regression, illustrating the opportunity and drawbacks of each in the subject of smart home security. The Decision model led to an astonishing accuracy of almost 0.992 in the distinguishing number. But, coming to the transfer learning model which also works in a similar way as that of a decision tree but is slightly complex and involves the use of a couple of extra parameters. According to experimental result the decision tree and transfer learning both have higher accuracy than SVM and logistic regression. This outstanding score indicates its capacity to acknowledge examples and authenticates its potential for real world use.

6. Future Work

The accuracy of smart home security systems may be further upgrade by merging more sophisticated ML in the time ahead, including ensemble approach, deep learning. To further offer a more complete security solution, consider looking into the integration of other IoT devices and sensors. It's also important to create methods for adaptive learning and constant updates so that the security system may change to meet new threats.

References

1. M. G. Salimon, H. Goronduste, and H. Abdullah, “User adoption of smart homes technology in malaysia: Integration tam 3, tpb, utaut 2 and extension of their constructs for a better prediction,” J. Bus. Manag, vol. 20, no. 4, pp. 60–69, 2018.
2. M. Chan, E. Campo, D. Est`eve, and J.-Y. Fourniols, “Smart homesˆacurrent features and future perspectives,” Maturitas, vol. 64, no. 2, pp. 90–97, 2009.
3. S. H. Park, S. H. Won, J. B. Lee, and S. W. Kim, “Smart home–digitally engineered domestic life,”Personal and Ubiquitous Computing, vol. 7, pp. 189–196, 2003.
4. D. Karlsson and A. Lindstr¨om, “Automated learning and decision: Making of a smart home system,” 2018.
5. G. Suciu, A. Vulpe, S. Halunga, O. Fratu, G. Todoran, and V. Suciu, “Smart cities built on resilient cloud computing and secure internet of things,” in 2013 19th international conference on control systems and computer science, pp. 513–518, IEEE, 2013.
6. B. Quinto and B. Quinto, “Introduction to machine learning,” Next-Generation Machine Learning with Spark: Covers XGBoost, LightGBM, Spark NLP, Distributed Deep Learning with Keras, and More, pp. 1–27, 2020.
7. D. Cook and S. K. Das, Smart environments: technology, protocols, and applications, vol. 43. John Wiley & Sons, 2004.
8. J. C. Augusto, H. Nakashima, and H. Aghajan, “Ambient intelligence and smart environments: A state of the art,” Handbook of ambient intelligence and smart environments, pp. 3–31, 2010.
9. P. Rashidi and D. J. Cook, “Keeping the resident in the loop: Adapting the smart home to the user,” IEEE Transactions on systems, man, and cybernetics-part A: systems and humans, vol. 39, no. 5, pp. 949–959, 2009.
10. D. Mocrii, Y. Chen, and P. Musilek, “Iot-based smart homes: A review of system architecture, software, communications, privacy and security,” Internet of Things, vol. 1, pp. 81–98, 2018.
11. I. Lee and K. Lee, “The internet of things (iot): Applications, investments, and challenges for enter- prises,” Business horizons, vol. 58, no. 4, pp. 431–440, 2015.
12. L. Atzori, A. Iera, and G. Morabito, “The internet of things: A survey,” Computer networks, vol. 54, no. 15, pp. 2787–2805, 2010.
13. R. Krishnamurthi, A. Kumar, D. Gopinathan, A. Nayyar, and B. Qureshi, “An overview of iot sensor data processing, fusion, and analysis techniques,” Sensors, vol. 20, no. 21, p. 6076, 2020.
14. M. M. Sadeeq, N. M. Abdulkareem, S. R. Zeebaree, D. M. Ahmed, A. S. Sami, and R. R. Zebari, “Iot and cloud computing issues, challenges and opportunities: A review,” Qubahan Academic Journal, vol. 1, no. 2, pp. 1–7, 2021.
15. M. I. Jordan and T. M. Mitchell, “Machine learning: Trends, perspectives, and prospects,” Science, vol. 349, no. 6245, pp. 255–260, 2015.
16. S. Balakrishna, M. Thirumaran, and V. K. Solanki, “Iot sensor data integration in healthcare using semantics and machine learning approaches,” A handbook of internet of things in biomedical and cyber physical system, pp. 275–300, 2020.
17. A. Cornel-Cristian, T. Gabriel, M. Arhip-Calin, and A. Zamfirescu, “Smart home automation with mqtt,” in 2019 54th International Universities Power Engineering Conference (UPEC), pp. 1–5, IEEE, 2019.
18. N. Balta-Ozkan, O. Amerighi, and B. Boteler, “A comparison of consumer perceptions towards smart homes in the uk, germany and italy: reflections for policy and future research,” Technology Analysis & Strategic Management, vol. 26, no. 10, pp. 1176–1195, 2014.
19. S. Sepasgozar, R. Karimi, L. Farahzadi, F. Moezzi, S. Shirowzhan, S. M. Ebrahimzadeh, F. Hui, and L. Aye, “A systematic content review of artificial intelligence and the internet of things applications in smart home,” Applied Sciences, vol. 10, no. 9, p. 3074, 2020.
20. D. Marikyan, S. Papagiannidis, and E. Alamanos, “A systematic review of the smart home literature: A user perspective,” Technological Forecasting and Social Change, vol. 138, pp. 139–154, 2019.
21. M. Alloghani, D. Al-Jumeily, J. Mustafina, A. Hussain, and A. J. Aljaaf, “A systematic review on supervised and unsupervised machine learning algorithms for data science,” Supervised and unsupervised learning for data science, pp. 3–21, 2020.
22. K. M. Harahsheh and C.-H. Chen, “A survey of using machine learning in iot security and the challenges faced by researchers,” Informatica, vol. 47, no. 6, 2023.
23. M. Talal, A. Zaidan, B. Zaidan, A. S. Albahri, A. H. Alamoodi, O. S. Albahri, M. Alsalem, C. K. Lim, K. L. Tan, W. Shir, et al., “Smart home-based iot for real-time and secure remote health monitoring of triage and priority system using body sensors: Multi-driven systematic review,” Journal of medical systems, vol. 43, pp. 1–34, 2019.

24. D. Myridakis, S. Papafotikas, K. Kalovrektis, and A. Kakarountas, "Enhancing security on iot devices via machine learning on conditional power dissipation," Electronics, vol. 9, no. 11, p. 1799, 2020.
25. A. Ullah, S. M. Anwar, J. Li, L. Nadeem, T. Mahmood, A. Rehman, and T. Saba, "Smart cities: The role of internet of things and machine learning in realizing a data-centric smart environment," Complex & Intelligent Systems, vol. 10, no. 1, pp. 1607–1637, 2024.
26. M. Attaran, "The internet of things: Limitless opportunities for business and society," Journal of Strategic Innovation and Sustainability Vol, vol. 12, no. 1, p. 11, 2017.
27. K. Maswadi, N. B. A. Ghani, and S. B. Hamid, "Systematic literature review of smart home monitoring technologies based on iot for the elderly," IEEE Access, vol. 8, pp. 92244–92261, 2020.
28. D. B. Adriano, W. A. C. Budi, et al., "Iot-based integrated home security and monitoring system," in Journal of physics: conference series, vol. 1140, p. 012006, IOP Publishing, 2018.
29. H. Touqeer, S. Zaman, R. Amin, M. Hussain, F. Al-Turjman, and M. Bilal, "Smart home security: challenges, issues and solutions at different iot layers," The Journal of Supercomputing, vol. 77, no. 12, pp. 14053–14089, 2021.
30. U. Tahir, M. K. Abid, M. Fuzail, and N. Aslam, "Enhancing iot security through machine learningdriven anomaly detection," VFAST Transactions on Software Engineering, vol. 12, no. 2, pp. 01–13, 2024.
31. M. K. Abid, M. Qadir, S. Farid, and M. Alam, "Iot environment security and privacy for smart homes," Journal of Information Communication Technologies and Robotic Applications, vol. 13, no. 1, pp. 15–22,
32. 2022.
33. A. Kanawaday and A. Sane, "Machine learning for predictive maintenance of industrial machines using iot sensor data," in 2017 8th IEEE international conference on software engineering and service science (ICSESS), pp. 87–90, IEEE, 2017.
34. S. Ayvaz and K. Alpay, "Predictive maintenance system for production lines in manufacturing: A machine learning approach using iot data in real-time," Expert Systems with Applications, vol. 173, p. 114598, 2021.
35. Muhammad Kaleem , Muhammad Azhar Mushtaq , Uzair Jamil , Sadaqat Ali Ramay , Tahir Abbas Khan , Siraj Patel , Rizwan Zahidy , Sayyid Kamran Hussain. (2024). New Efficient Cryptographic Techniques For Cloud Computing Security. Migration Letters, 21(S11), 13–28. Retrieved from https://migrationletters.com
36. Hussain, S.K., Ramay, S.A., Shaheer, H., Abbas T., Mushtaq M.A., Paracha, S., & Saeed, N. (2024). Automated Classification of Ophthalmic Disorders Using Color Fundus Images, Volume: 12, No: 4, pp. 1344-1348 DOI:10.53555/ks.v12i4.3153
37. C. Cortes and V. Vapnik, "Support-vector networks," Machine learning, vol. 20, pp. 273–297, 1995.
38. A. Fryan, L. Hamad, M. I. Shomo, M. B. Alazzam, M. A. Rahman, et al., "Processing decision tree data using internet of things (iot) and artificial intelligence technologies with special reference to medical application," BioMed Research International, vol. 2022, 2022.
39. M. Wang, N. Yang, and N. Weng, "Securing a smart home with a transformer-based iot intrusion detection system," Electronics, vol. 12, no. 9, p. 2100, 2023.
40. M. Almutairi, "Smart home iot privacy and security preservation via machine learning techniques.," Computers, Materials & Continua, vol. 75, no. 1, 2023.
41. X. Li, H. Ghodosi, C. Chen, M. Sankupellay, and I. Lee, "Improving network-based anomaly detection in smart home environment," Sensors, vol. 22, no. 15, p. 5626, 2022.
42. D. Rani, N. S. Gill, P. Gulia, F. Arena, and G. Pau, "Design of an intrusion detection model for iot-enabled smart home," IEEE Access, 2023.
43. N. Butt, A. Shahid, K. N. Qureshi, S. Haider, A. O. Ibrahim, F. Binzagr, and N. Arshad, "Intelligent deep learning for anomaly-based intrusion detection in iot smart home networks," Mathematics, vol. 10, no. 23, p. 4598, 2022.
44. T. Gazdar, "A new ids for smart home based on machine learning," in 2022 14th International Confer- ence on Computational Intelligence and Communication Networks (CICN), pp. 393–400, IEEE, 2022.
45. A. Rahim, Y. Zhong, T. Ahmad, and U. Islam, "An intelligent approach for preserving the privacy and security of a smart home based on iot using logitboost techniques," Journal of Hunan University Natural Sciences, vol. 49, no. 4, 2022.
46. X. Hu, Q. Zhang, X. Yang, and L. Yang, "An intrusion detection method fused deep learning and fuzzy neural network for smart home," in International Conference on Intelligent Computing, pp. 627–637, Springer, 2022.
47. M. Syamala, C. Komala, P. Pramila, S. Dash, S. Meenakshi, and S. Boopathi, "Machine learning- integrated iot-based smart home energy management system," in Handbook of Research on Deep Learn- ing Techniques for Cloud-

Based Industrial IoT, pp. 219–235, IGI Global, 2023.

48. Y. Liu and S. Li, "A review of hybrid cyber threats modelling and detection using artificial intelligence in iiot," Computer Modeling in Engineering & Sciences, 2023
49. M. Ramzan, Z. U. R. Zia, M. K. Abid, N. Aslam, and M. Fuzail, "A review study on smart homes present challenges concerning awareness of security mechanism for internet of things (iot)," Journal ofComputing & Biomedical Informatics, 2024.
50. H. Nasir, A. Ayaz, S. Nizamani, S. Siraj, S. Iqbal, and M. K. Abid, "Cloud computing security via intelligent intrusion detection mechanisms," International Journal of Information Systems and Computer Technologies, vol. 3, no. 1, pp. 84–92, 2024.
51. Tandon, R., Sayed, A., & Hashmi, M. A. (2023). Face mask detection model based on deep CNN technique using AWS. International Journal of Engineering Research and Applications www.ijera.com, 13(5), 12-19.
52. M. K. Abid, Z. U. R. Zia, and S. Farid, "Security and privacy for future healthcare iot," Journal of Computing & Biomedical Informatics, vol. 4, no. 01, pp. 132–140, 2022.
53. Abbas, M., Arslan, M., Bhatty, R. A., Yousaf, F., Khan, A. A., & Rafay, A. (2024). Enhanced Skin Disease Diagnosis through Convolutional Neural Networks and Data Augmentation Techniques. Journal of Computing & Biomedical Informatics, 7(01).
54. Zhong, X. J., Liu, S. R., Zhang, C. W., Zhao, Y. S., Sayed, A., Rajoka, M. S. R., ... & Song, X. (2024). Natural Alkaloid Coptisine, Isolated from Coptis chinensis, Inhibits Fungal Growth by Disrupting Membranes and Triggering Apoptosis. Pharmacological Research-Modern Chinese Medicine, 100383.