Towards a Smart Home : Environment Monitoring and Intelligent Anti-Theft Alarming

Sunil Gunasinghage R.W
Department of Computer Systems Engineering
Sri Lanka Institute of Information Technology (SLIIT)
Malabe, Sri Lanka
it20212704@my.sliit.lk

M.M.S. Silva
Department of Computer Systems Engineering
Sri Lanka Institute of Information Technology (SLIIT)
Malabe, Sri Lanka
it20383770@my.sliit.lk

R.K. Kodikara
Department of Computer Systems Engineering
Sri Lanka Institute of Information Technology (SLIIT)
Malabe, Sri Lanka
it20182182@my.sliit.lk

J.S.P.A Ekanayake
Department of Computer Systems Engineering
Sri Lanka Institute of Information Technology (SLIIT)
Malabe, Sri Lanka
it20108922@my.sliit.lk

N.D.U. Gamage
Department of Computer Systems Engineering
Sri Lanka Institute of Information Technology (SLIIT)
Malabe, Sri Lanka
narmada.g@sliit.lk

Poojani Gunathilake
Department of Computer Science & Software Engineering
Sri Lanka Institute of Information Technology (SLIIT)
Malabe, Sri Lanka
poojani.g@sliit.lk

***Abstract* - Recently Smart Home concept has been a popular choice as a solution for emerging security related problems. The primary objective of this research was to create a cyber-threat free fully functioning smart home monitoring and anti-theft alarming system with enhanced physical security mechanisms. The focus of this research was to create a holistic and secure smart home system, combining cutting-edge physical security measures. The study introduced novel Intruder Access Prevention methods rooted in human behavior and voice pattern recognition, while also incorporating blockchain and network traffic analysis to safeguard the homeowner's data. Furthermore, a pioneering voice-controlled monitoring mechanism, utilizing protective energy-saving plug technology, was devised to enhance safety within contemporary households. The human behavior recognition and voice recognition-based intruder access prevention system demonstrated over 80% accuracy in intruder prevention, while user data protection mechanism prevents the communication channel from cyber hackings. Further, the smart plug demonstrates reliable and accurate physical environment monitoring with minimum latency. These results underscore the system's significant contribution to home security, marking a noteworthy advancement in the Smart Home concept.**

Keywords - Smart Home, Cyber-Threat, Real-Time, Machine Learning, Algorithm, Blockchain Technology, Data Integrity

I. INTRODUCTION

The Smart Home concept is the most recent solution invented to resolve security problems emerge in modern homes due to the rising rates of theft and burglary in modern society. Anomaly detection is also a key concept in smart home systems where unusual events are detected. To better protect against threats and reduce false alarms, smart home concept needs to take a much more sophisticated and adaptive approach.

The system examines footage from surveillance cameras to look for aberrant behavior and then notifies the user of any potential dangers. The technology is able to forecast and prevent prospective break-ins by recognizing anomalous behavior in invaders. To implement this scheme, it undertake a meticulous dissection of the CCTV footage through employment of avant-garde deep learning techniques and computer vision algorithms. Also, the enhancement of technology, traditional security measures like locks, alarms, and CCTV camera etc. fail to provide the necessary protection to modern houses. Anomaly sound detection is also a key concept in the smart home systems where, unusual events are detected for better protect against threats and reduce false alarms, smart home concept needs to take a much more sophisticated and adaptive approach. Anomaly sound detection could be introduced as the process of finding data patterns that differ from what is deemed typical or expected. The method of finding unusual sound patterns in a specific setting is known as anomaly sound detection.

Modern houses have become more networked and simpler to control as a direct result of the growth of internet-enabled "smart home" devices and the Internet of Things (IoT). However, the greater connectivity comes with an accompanying increase in the potential of cyber-attacks. To address this issue, the combination of blockchain and machine learning technology has come out as a perfect solution. Blockchain technology, and machine learning algorithms can be used to recognize anormal behaviors and suspicious behaviors, which paves the way to early detection and prevention of cyberattacks. Also, this project designs an intelligent plug that can watch over and manage itself when there is no motion detected close to household electrical appliances. When there isn't any motion detected for a predetermined amount of time, the project's smart plug have the ability to shut off automatically. Also, it provides unique voice recognition, current analysis, LP gas leak analysis, and motion detection features. The Intelligent Plug Base is a device that plugs into a standard power outlet and provides several features that can be useful in households. Fig.1 depicts a high-level diagram for the completed solution.

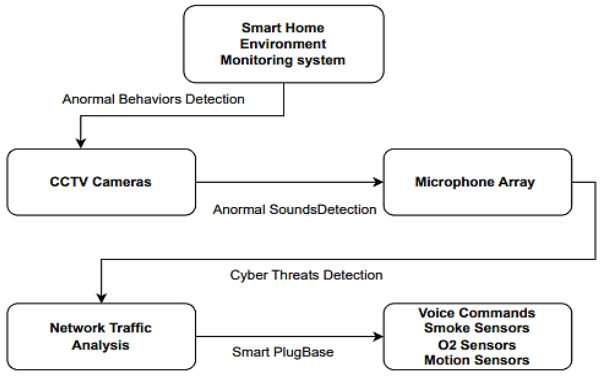

Fig. 1. High Level Diagram for Smart Home Monitoring Sysytem

II. LITERATURE REVIEW

This literature review aims to provide a comprehensive overview of the latest developments in these fields, focusing on environment monitoring and intelligent anti-theft systems. It analyze research papers and scholarly articles to present a comprehensive snapshot of the current state of technology.

The studies listed below provide an in-depth examination of the use of technology for Human Action Recognition (HAR) and abnormal behavior detection, specifically within the realm of video analytics. The "Vision-Based Multi-Modal Framework for Action Recognition" paper presents a system for human action recognition using multimodal data. It follows a three-step process: feature extraction, data fusion, and classification [1]. Multimodal approaches, using CNNs and LSTMs, outperform single-modal methods on public datasets.

In the "Evaluation of Human Action Recognition Methods meant for Video Analytics," the authors assess various HAR techniques, with an emphasis on their application within security and surveillance sectors. Through their analysis, the Histogram of Oriented Gradients (HOG) method emerges as the most accurate in detecting human motion [2]. The study concludes with a call for more standardized datasets and consideration of environmental factors for further accuracy improvements.

The "Computer Vision-based Survey on Human Activity Recognition System, Challenges and Applications" paper provides a comprehensive review of HAR systems and their components. The authors highlight the challenges HAR systems face, such as managing noisy and incomplete data and fluctuations in human activity [3]. They also emphasize potential research areas like multimodal data fusion, deep learning-based feature extraction, and transfer learning across domains, while highlighting the societal and individual benefits of such systems. Collectively, these studies highlight the potential of CNN and LSTM technology in improving security and surveillance systems and underscore the need for ongoing research in this area.

When considering about the voice and sound recognition technology related research, there are still only few research on the practical use of this technology has been found. These research papers broadly center on the theme of enhancing smart home security through the deployment of voice and sound anomaly detection techniques.

Kim et al.'s paper on "Anomaly Voice Detection Using a Stacked Denoising Autoencoder for Smart Homes" focuses on using a stacked denoising autoencoder for feature extraction from audio signals [4]. Through comparative evaluations, the authors demonstrate the superiority of this method over conventional techniques in terms of accuracy and reduced false alarms, affirming its efficacy in noisy environments.

The authors in "Anomaly Detection for Smart Home Security Using Voice Recognition" suggest the use of Deep Neural Networks for classifying sound data to improve security measures in smart homes [5]. Their proposed system has shown promising results, indicating practical potential for real-world application.

The paper "Smart Home Security: Voice-Based Anomaly Detection and Intrusion Prevention follows a similar thematic approach. They advocate for the inclusion of voice data as an additional layer of security in smart homes, highlighting their system's effectiveness with a low false positive rate [6]. Finally, Parameshwaran and Prakash's paper titled "Anomaly Detection of Sounds for Home Security Systems" proposes using sound data and machine learning techniques to detect anomalies. They demonstrate more than 80% accuracy rate and discuss the system's potential in burglar detection and unauthorized entry attempts. While these papers provide valuable insights, they also underscore the need for further extensive research, especially considering the performance of these methods in different scenarios and potential privacy concerns related to audio data collection.

Next research papers in focus revolve around bolstering security in smart homes and IoT devices through the innovative deployment of blockchain technology and machine learning algorithms. The paper by Saha and Kar sheds light on the security vulnerabilities of smart homes, elaborating on the potential of blockchain as a security measure [7]. They introduce an approach employing a permissioned blockchain to log device interactions and use machine learning for anomaly detection, arguing it provides superior security and efficiency.

Saleh et al. in "A Blockchain-based Security Framework for IoT-enabled Smart Homes," present a novel blockchain-based framework for securing IoT devices. They underscore the inadequacy of current, centralized security solutions and argue for a decentralized, blockchain-based architecture for heightened security and data privacy [8].

Lastly, Khan et al.'s paper discusses harnessing blockchain for safe, decentralized information storage among IoT devices [9]. They propose a combination of blockchain and machine learning, emphasizing the advantages of their approach, such as enhanced security and reliability for IoT devices. Collectively, these papers highlight the promise of blockchain and machine learning in protecting smart homes and IoT devices. They emphasize the importance of ongoing research due to increasing cyber threats and the need for strong, decentralized security solutions.

Next research papers being considered here share a common focus on the application of Internet of Things (IoT) in anti-theft security for smart homes and vehicles. The first paper, "Anti-Theft Monitoring for a Smart Home," presents an IoT-based system for monitoring potential theft or intrusions in smart homes. The proposed system utilizes various sensors that collect data and relay it to a central device [10]. Then collected data processes and notified the homeowner and monitoring service of any abnormal activity, suggesting a reliable and adaptable solution to home security.

Similarly, the second paper, "Smart Vehicle and Anti-Theft System Using IoT," proposes an IoT-driven security solution for vehicles. The system processes sensor data in the cloud and employs algorithm to detect unauthorized activities [11]. The paper concludes that the suggested system could serve as an effective tool against vehicle theft while offering potential integration with other smart services.

The third paper, "IoT Based Anti-Theft Security System," also applies the IoT framework to improve security in residential and commercial spaces. It introduces an array of sensors to detect unwarranted intrusions, with data analyzed at a central hub that alerts the property owner or monitoring service about any suspicious activity [12]. The system's ability to integrate with other smart devices, as well as remote

door/window control and live video monitoring, solidify its effectiveness and reliability in theft prevention.

These studies collectively demonstrate how the IoT, combined with MLP machine learning algorithm and sensor technology, can provide robust anti-theft solutions for both residential properties and vehicles. Each proposed system presents a scalable and adaptive security solution, proving effective in different theft scenarios and demonstrating potential integration with broader smart home or vehicle services.

In summary, the research on "Smart Home Environment Monitoring and Intelligent Anti-Theft Alarming System" highlights the significant progress and immense opportunities within smart home solutions. Current studies detail various machine learning methods suitable for the envisioned Anti-Theft and Monitoring systems. Specifically, for proposed system, CNN and LSTM algorithms are employed for detecting unusual behaviors, while the MLP algorithm is utilized for anomalous sound detection, attributed to these algorithms' commendable accuracy exceeding 80%. In terms of Cyber Threat Detection, the system leverages the strengths of the Random Forest and Gaussian Naïve Bayes methods to ensure thorough environmental surveillance, advanced analytics, and effective threat counteractions. Further, studies emphasize the need for improved standardization and interoperability across devices to maximize the utility of these systems. Looking ahead, the continuous integration of AI and IoT in home security systems is anticipated to drive significant improvements in terms of system adaptability, precision, and real-time responses, promising a safer and smarter future for home environments.

III. METHODOLOGY

The proposed mechanism and the components mainly consist of four sub systems which are anormal behavior detection and response, anormal sound detection and response, securing the smart home from cyber threats by analyzing the network traffic and to enable an electric hazard-free environment in a modern house. The research design for developing a cyber-threat-free fully functioning smart home monitoring and anti-theft system with enhanced physical security through behavior pattern and voice pattern monitoring, energy-saving capabilities, and protective plug bases involve a combination of qualitative and quantitative approaches. Fig. 2 depicts a system diagram for the whole solution component.

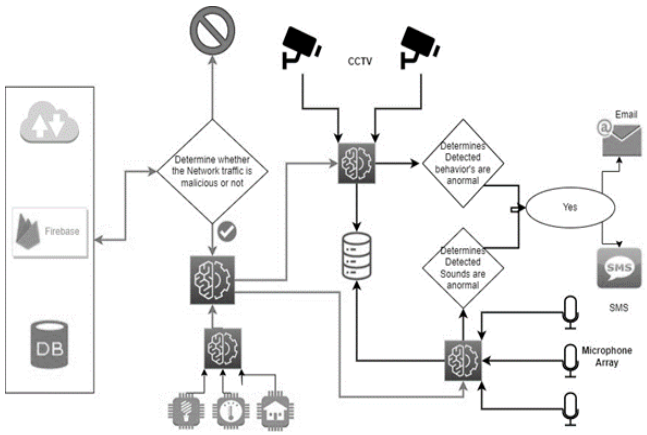

Fig. 2. System Diagram for Smart Home Monitoring System

A. Abnormal Behavior Detection System

The Abnormal Behavior Detection System was developed by following a step-by-step approach that combines AI technology with CCTV cameras to improve security and safety Firstly, a wide range of CCTV footage that represents both normal and abnormal behaviors was gathered with high diversity. To protect people's privacy, any personal information was removed from the footage. Next, the collected footage was annotated and labeled by the research team, marking instances of normal and abnormal behaviors. This step helped in creating a reliable dataset for training the AI model, ensuring that the annotations were consistent and accurate. These algorithms allowed the model to efficiently analyze video frames and sequences and here, most commonly deep learning algorithms, CNN was selected and combined with frame capturing to build the AI model.

The model was trained using the labeled dataset, and pre-trained models were utilized to improve its performance. Emphasis was placed on optimizing the AI model for real-time performance, enabling it to process CCTV footage quickly and promptly detect abnormal behaviors. This ensured that security measures could be taken in a timely manner. Throughout development, ethics were prioritized. To preserve privacy and comply with legislation, transparency, consent, and data processing were prioritized. Accuracy, recall, precision, and F1-score were used to evaluate the AI model.

The model was tested on a separate dataset to ensure accurate detection of abnormal behaviors without generating excessive false alarms. The importance of ongoing monitoring and improvement was also recognized. Feedback from users and administrators in real-world scenarios was gathered, allowing for the identification of any limitations or biases. Based on this feedback, the AI model was regularly updated and refined to enhance its performance and adapt to evolving security challenges.

B. Abnormal Voice detection system

A step-by-step approach was followed to create a system that detects abnormal voice patterns using MLP classifier and microphone arrays. First, a diverse set of voice recordings that included both normal and abnormal voice patterns was gathered. A wide range of scenarios and voice characteristics, including different accents, speech patterns, and background noises, were captured. Privacy regulations were respected, and the necessary consent for using the recordings was obtained.

Next, a microphone array system was set up with multiple microphones strategically placed in the recording environment. High-quality audio from different angles and locations was captured using this setup. The microphones were calibrated for consistent and accurate sound recording. The voice recordings underwent preprocessing to improve their quality. Background noise was removed, volume levels were normalized, and unwanted artifacts were eliminated. This ensured a clean dataset ready for analysis. Relevant acoustic features such as pitch, intensity, spectral characteristics, and temporal patterns were extracted from the recordings. These features provided valuable information for the solution to identify abnormal voice patterns.

The model was trained using preprocessed voice recordings. The model's parameters were optimized to improve its performance, employing techniques like cross-validation and grid search. To evaluate the model, the dataset was split into training, validation, and testing sets. The model

was trained on the training set and its performance was assessed on the validation set. Based on this evaluation, the model was fine-tuned. Finally, the model was evaluated on the testing set to measure its accuracy, sensitivity, specificity, and other relevant metrics. This determined how well the model could detect abnormal voice patterns.

For real-time implementation, the trained AI model was deployed in a system that could process audio streams captured by the microphone array in real-time. The system was optimized for low latency, enabling prompt detection of abnormal voice patterns and immediate alerts or actions if necessary. Throughout the process, ethical considerations were prioritized. Privacy regulations were followed, and informed consent was obtained for using voice recordings. Clear policies were established to ensure responsible and ethical use of the system, addressing privacy, data storage, and potential biases.

System efficiency was tracked in real-world circumstances to improve it. The AI model and infrastructure were updated based on user input, new data, and voice analysis breakthroughs. This improved system accuracy, adaptability, and efficacy. This technology was used to create a real-time voice pattern detection system. This technology could help people identify atypical voice traits and provide timely support or action.

C. Cyber Threat Detection System

A step-by-step approach was followed to develop a strong cyber threat detection system that utilizes Random forest, Gaussian native Bayes, MLP and ensures secure data communication between smart home devices using blockchain technology. Firstly, thorough research was conducted, and the specific requirements for the cyber threat detection system were analyzed. Existing research on cyber threats, AI techniques, secure data communication, and blockchain technology in the context of smart homes was studied.

Next, relevant datasets containing examples of cyber threats, network traffic patterns, and security events related to smart home devices were collected. The data was carefully prepared by cleaning it, normalizing it, extracting important features, and ensuring the anonymity of sensitive information.

An AI model specifically designed for threat detection was developed. Suitable AI techniques, such as machine learning algorithms or deep learning models, were selected, and the model was trained using the preprocessed dataset. The model's parameters were optimized, and its performance was evaluated using various metrics. To ensure secure data communication between smart home devices, a blockchain-based framework was implemented. This framework utilized cryptographic techniques, such as encryption, digital signatures, and public-key infrastructure, to protect the confidentiality, integrity, and authenticity of the data within the blockchain network. Smart contracts or decentralized applications were created on the blockchain to facilitate secure data sharing and communication among the devices.

The trained AI model was integrated with the blockchain framework, enabling real-time cyber threat detection and secure data communication within the smart home network. Interfaces for data exchange between the AI model and the blockchain network were established, and protocols for analyzing network traffic, identifying threats, and securely communicating relevant information through the blockchain were defined.

Thorough testing and evaluation of the integrated system were conducted. The accuracy of cyber threat detection, real-time response capabilities, scalability, and the effectiveness of secure data communication using the blockchain were assessed. Tests were performed in simulated environments or real-world smart home setups, considering different threat scenarios and network conditions. Throughout the development and deployment process, ethical considerations were prioritized, and compliance with privacy regulations and data protection laws was ensured. Privacy-enhancing techniques, such as data anonymization and secure multiparty computation, were implemented to address privacy concerns.

Finally, a process for continuous monitoring and improvement of the system was established. The system's performance, adaptability, and resilience to evolving cyber threats and network conditions were regularly monitored. User feedback and expert insights were collected to identify any weaknesses, false alarms or misses, and areas for enhancement. The AI model, blockchain framework, and security measures were kept up to date based on the latest threat intelligence and advancements in AI and blockchain research.

By following this methodology, a cyber threat detection system that combines AI and secure data communication using blockchain was successfully developed. This system enhances security and privacy in smart homes by detecting threats in real-time and facilitating trusted communication between devices.

D. Intelligent Plug Base

A step-by-step approach was followed to create an intelligent plug base that operates through voice commands and includes smoke detectors, fire detectors, and oxygen meters. Firstly, the requirements and objectives of the intelligent plug base system were carefully analyzed. The desired functionalities, performance criteria, and safety standards for each component, including voice command functionality, motion detectors, fire detectors, current meters, and oxygen meters, were defined.

Next, the intelligent plug base was designed to seamlessly incorporate all the necessary components. Factors such as size, form factor, and placement were considered to ensure efficient integration. The circuitry and hardware required to support component functionalities and enable communication between them were developed. Prototypes of the intelligent plug base were then created to test its functionalities. Rigorous testing was performed on each component, including the motion detectors, fire detectors, current meters, and oxygen meters, to ensure accurate readings and reliable performance. The voice command functionality was also tested to ensure accurate recognition and response to voice commands.

Voice recognition and natural language processing technologies were incorporated to enable voice command functionality. These technologies allowed the system to accurately interpret voice commands and execute the appropriate actions. The voice recognition model was trained using a diverse dataset to improve accuracy and account for different accents, speech patterns, and languages. Connectivity options, such as Wi-Fi or Bluetooth, were implemented to facilitate communication between the

intelligent plug base and other smart home devices or control interfaces. Interoperability with a central control hub or smart home system was ensured for seamless integration and remote monitoring/control capabilities.

Safety monitoring was prioritized in the system. Real-time monitoring of motions, smoke, fire, current level, and oxygen levels was enabled, triggering appropriate actions when abnormal conditions were detected. Immediate alerts, such as audible alarms or notifications, were generated by the intelligent plug base to warn users of potential safety hazards. A user-friendly interface was designed to interact with the intelligent plug base. This included voice prompts, LED indicators, and a mobile application that allowed users to monitor the plug base remotely. Customizable settings, alert management, and access to historical data were provided to enhance the user experience.

By following this methodology, an intelligent plug base system that incorporates voice command functionality, motion detectors, fire detectors, current, and oxygen meters, was successfully developed. The system ensures seamless integration of components, undergoes rigorous testing, meets safety standards, and prioritizes user satisfaction.

IV. Results and Discussion

The research was methodically divided into several targeted sub-objectives to ensure a comprehensive and detailed approach. The first sub-objective centered on enhancing the physical security of contemporary dwellings. The aim was to deter unauthorized access by furnishing homes with sophisticated intrusion detection systems, capable of promptly identifying, flagging, and notifying homeowners of illicit breaches.

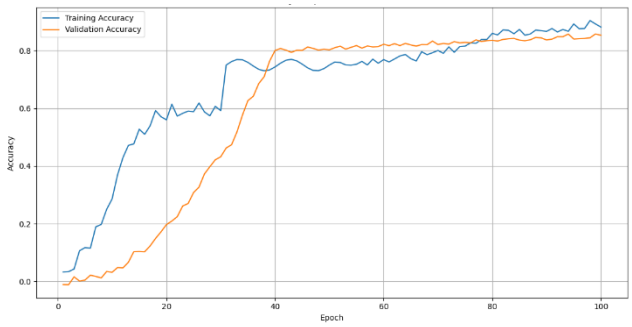

Fig. 3. Overall Accuracy Comparison Diagram of Intruder Access Prevention System

This intruder access prevention system monitors the people who attend the home through the front and back doors through the cameras fixed along those doors and if that person performed any abnormal action such as relatively fast or slow movements and if that person covered the face with any object, this system informs the owner of the home on that action via an email or a SMS on real time. The action identification has been done through frame capturing and the covered faces can be detected through the Convolutional neural network (CNN) implementation which is a deep learning approach as well. And, as an efficient memory utilizing approach, this system stores the nearest 10 seconds related to that considered abnormal activity as a proof inside a local hard drive where other CCTV systems store all the footages which cost high and consume more memory. Above Fig. 3 defines the accuracy comparation of intruder access prevention component.

The second sub-objective involved the deployment of voice recognition technology. By leveraging advanced features in this domain, the intention was to develop a system proficient at identifying and detecting inconsistencies in sound patterns, providing an additional layer of defense against potential threats. This system live monitors the sounds around the sensitive environments through the microphones installed on those places and it notify the owner of the home if there was any sort of abnormal sound detected via an email and SMS real time with the location of the place where sound generated as well. In this system it has been used libraries such as librosa and numpy to build the sound identification code and the datasets have been created manually as well. This system is one of the unique systems as no one had heard about this kind of system in homes. Here Fig. 4 depicts the accuracy comparison of anomaly sound detection component.

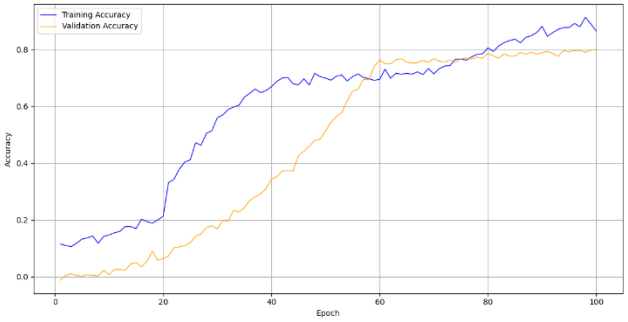

Fig. 4. Overall Accuracy Comparison Diagram of Anomaly Sound Detection System

The third sub-objective focused on establishing a secure data communication framework. In an era where data breaches have become alarmingly commonplace, ensuring secure transmission of information within the smart home ecosystem was of paramount importance. The machine learning-based secure data communication framework demonstrated robust performance in ensuring the privacy and integrity of the data transmitted within the smart home ecosystem. Machine learning algorithms were deployed to identify abnormal data patterns that might indicate potential security breaches. The system was capable of flagging suspicious activities in real-time, enabling rapid responses to potential threats. Also, the machine learning algorithms utilized checksums and data hashing techniques to guarantee the integrity of the data during transmission. This prevented any unauthorized tampering or modifications of data packets. By mitigating the risk of data breaches, homeowners' sensitive information remained well-protected, instilling confidence in the system's reliability. Below Fig. 5 depicts the accuracy comparison of Cyber threat detection component.

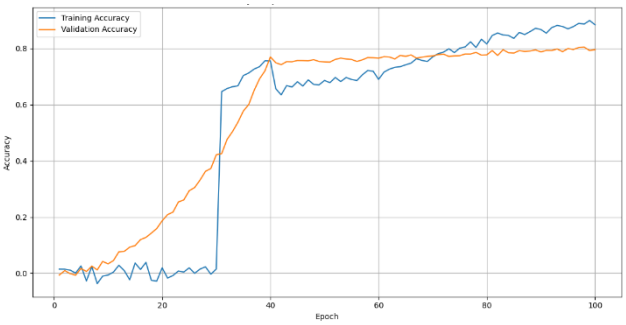

Fig. 5. Overall Accuracy Comparison Diagram of Cyber Threat Detection

The final sub-objective involved creating an environment free from electrical hazards in contemporary homes. This objective included implementing protective measures to mitigate typical household electrical risks, and through the integration of energy-conserving practices and safeguarded plug bases, a safe and sustainable living environment was to be fostered. Here this plug base can be controlled through voice commands and monitor some important parameters such as people, gas concentration, electric voltage and also the oxygen level around the environment via sensors and it cut off its supply of electricity if it detected any people not available near the plug for a certain period of time which can be customized, any detection of leakage of LP gas or lower down of the oxygen level and also if it detected any abnormality in voltage of power provided. Here Fig. 6 depicts the comparison of accuracy of the intelligent plug base.

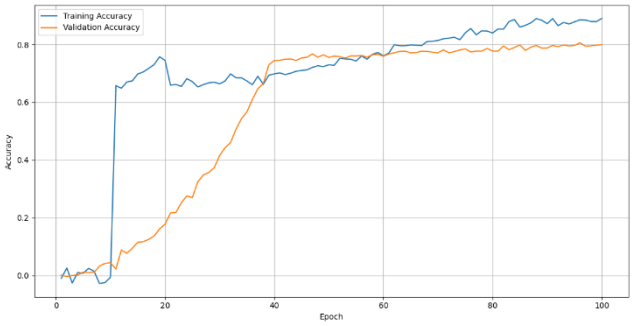

Fig. 6. Overall Accuracy Comparison Diagram of Intelligent Plug Base

To transform these strategic objectives into practical solutions, an exhaustive research journey was embarked upon. The effectiveness of the developed system was affirmed, highlighting its capability to efficiently identify sound pattern anomalies, detect unauthorized access attempts, and ensure secure data communication within the smart home, thereby enhancing the safety of its inhabitants.

V. Conclusion

The article discusses the pressing issue of ensuring the security and protection of contemporary smart houses from potential intrusions, cyber vulnerabilities, and electrical dangers. The presented method entails the implementation of a comprehensive smart home system that places significant emphasis on monitoring the home environment and deterring burglary.

The study demonstrates the efficacy of data-driven insights in detecting and preventing unwanted access attempts through the application of sophisticated machine learning algorithms. The utilization of machine learning techniques in the realm of cyber threat identification exemplifies a proactive strategy in safeguarding the digital components of intelligent life. The integration of intelligent plug bases serves to underscore the dedication to ensuring safety and promoting electrical stability.

The adaptability of the solution is emphasized when considering its ability to continuously learn from developing patterns and threats through machine learning algorithms. Ongoing advancements are anticipated through collaborations with professionals in the fields of cybersecurity and electrical engineering. In summary, the study underscores the importance of improving security and efficiency in smart houses, anticipating a future in which these dwellings provide both convenience and strong safeguarding measures.

References

[1] B. D. Romaissa, O. Mourad and N. Brahim, "Vision-Based Multi-Modal Framework for Action Recognition," in *2020 25th International Conference on Pattern Recognition (ICPR)*, Milan, Italy, 2021.

[2] S. R. Rashmi, S. Bhat and V. C. Sushmitha, "Evaluation of human action recognition techniques intended for video analytics," in *2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon)*, Bengaluru, India, 2017.

[3] A.M.F and S. Singh, "Computer Vision-based Survey on Human Activity Recognition System, Challenges and Applications," in *2021 3rd International Conference on Signal Processing and Communication (ICPSC)*, Coimbatore, India, 2021.

[4] D. Kim, C. Hwang and T. Lee, "Stacked-autoencoder based anomaly detection with Industrial Control System," *Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing*, p. 191, 2021.

[5] Y. Sun, J. Yang and C.-H. Hsu, "Anomaly Detection for Smart Home Security Using Voice Recognition," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3218-3226, 2019.

[6] A. Ghandeharioun and R. W. Picard, "Smart Home Security: Voice-Based Anomaly Detection and Intrusion Prevention," *IEEE Transactions on Multimedia*, vol. 19, no. 4, pp. 807-819, 2017.

[7] S. Saha and S. Kar, "Securing Smart Homes with Blockchain Technology," in *IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Halifax, NS, Canada, 2018.

[8] S. M. A. Saleh, M. T. Ibrahim, M. A. Razzaque and M. F. Mridha, "A Blockchainbased Security Framework for IoT-enabled Smart Homes," in *2019 IEEE 6th International Conference on Industrial Engineering and Applications (ICIEA)*, Tokyo, Japan, 2019.

[9] A. T. Khan, K. Salah and K. Alzahrani, "A Machine Learning Approach for IoT Security Using Blockchain," in *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, Limerick, Ireland, 2019.

[10] T. Nagamani, W. H. Beniga, K. S. Dhanish and A. S. Benitta, "Anti-Theft Monitoring for a Smart Home," in *2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT)*, Tirunelveli, India, 2022.

[11] A. Nagy, M. Abdelftah and B. M. Yousef, "Smart Vehicle and Anti-Theft System Using IoT," *International Journal of Engineering Inventions*, pp. 1-5, 2020.

[12] M. Musab, S. Kaloria, A. Chhipa, A. Sharma and F. Mansoori, "IOT Based Anti-Theft Security System," *International Journal for Research Trends and Innovation*, vol. 7, no. 6, pp. 106-109, 2022.

[13] I. R. Parameshwaran and R. Prakash, "Anomaly Detection of Sounds for Home Security Systems," *IEEE Sensors Journal*, vol. 18, no. 22, pp. 9233-9242, 2018.