International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0190
e ISSN: 2584-2854
Volume: 03
Issue:04 April 2025
Page No: 1164 - 1168

Real-Time Cybersecurity Monitoring for Smart Homes With AI

K. Amsamani [1], A. Beneta Mary[2], J. P. Aswini [3], K. Premkumar[4]
[1,2,3,4]Assistant Professor, Department of Computer Science and Engineering, St. Joseph College of Engineering, Sriperumbudur, Chennai. 602117, and India.
Emails ID: *amsamani@stjoseph.ac.in[1], benetamary@stjoseph.ac.in[2], aswini@stjoseph.ac.in[3], premkumar@stjoseph.ac.in[4]*

Abstract
The rapid growth of state-of-the-art housing technologies has revolutionized modern life by automation and monitoring household appliances. However, increasing connectivity and integration of internet devices pose challenges. The report provides a comprehensive framework for real-time cyber security surveillance using artificial intelligence to identify and control threats in the Smart Home environment. The proposed structure uses deep learning methods to analyses network traffic and identify possible penetration. Using machine learning models such as computational learning models (CNS) and repeat neurological networks (RNNS), the computer reaches higher accuracy in detecting cyber threats by minimizing the wrong passivity. In addition, we introduce an adaptive insight that continue to improve its knowledge base to respond to the formation of attack vectors. Test results prove that the surveillance system run by AI significantly improves the ability to detect the threat compared to traditional signature approaches. This research highlights the potential of Artificial Intelligence. This will help provide immediate security solutions for smart home vacations and promote safe and flexible digital environments.

Keywords: *Smart homes, cyber security, real-time monitoring, artificial intelligence, machine learning, analyzing, IOT security.*

1. Introduction
The rapid advancement of technology has brought about various changes in modern life, enhancing the development of globalization, automation, and artificial intelligence (AI). In particular, the improvement of home security and surveillance systems has led to the widespread emergence of smart home systems for domestic and commercial use. With the increase of modern devices like mini computers, natural language processing (NLP), actuators, sensors, and Internet of Things (IoT), homes are being fully automated, increasing both convenience and safety for people. As a result, technology has been developed to automate many tasks that users would otherwise need to perform manually, thereby reducing human labor. Smart Home Security Concerns: Home security is a crucial aspect of smart home technologies. Currently, technologies such as automated doors, surveillance cameras, motion detection, and voice-based security systems are enhancing security. However, as security threats continue to evolve, these technologies pose additional challenges. Unsecured IoT devices can allow hackers to steal personal information. Security passwords and outdated firmware compromise security protocols [1]. If internet security measures, encryption methods, and safe network practices are not adhered to, security vulnerabilities may arise. Due to such security concerns, there is an increasing importance in discovering new methods and security solutions. Specifically, when all internet-connected devices do not adhere to security protocols, hackers create an environment that can easily be exploited. Deficiencies in Current Security System current security systems often operate based on older attacks. This leads to an inability to detect newly emerging threats. Since hackers continue to use new techniques, unsecured IoT devices can be easily compromised. Furthermore, many smart devices lack

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0190
e ISSN: 2584-2854
Volume: 03
Issue:04 April 2025
Page No: 1164 - 1168

the facility for automatic software updates, making them susceptible to security vulnerabilities. The Role of Artificial Intelligence: This study proposes the creation of a real-time cyber security surveillance system based on artificial intelligence. Given the large number of internet-connected devices, advanced security protocols for IoT devices are essential. A system must be developed that can autonomously detect new cyber threats and reduce security issues. Deep Learning and Machine Learning Technologies. In this study, network traffic is analyzed using deep learning techniques to develop a security system capable of accurately detecting new and unknown attacks [2]. By utilizing machine learning models, higher success can be achieved in identifying new threats. Desired Benefits: Ability to automatically detect unprecedented attacks. Reduction of false positives, improving security performance. Improved legacy security systems that can autonomously detect continuously evolving threats. This study highlights the opportunities for developing AI-based solutions for smart home security. An automated security system must be created that enhances legacy security systems and has the capability to autonomously detect new and unknown threats. With the help of artificial intelligence, a secure and reliable home environment can be created for users. To develop security measures that can completely prevent cyber-attacks, the application of artificial intelligence must be increased. This study serves as a significant guide for exploring new ways to ensure security and develop solutions for smart home protection.

2. System Architecture - Detailed Description

The central security monitoring system has been developed as a multi-layered security system. Its main objective is to protect the IOT devices in the Smart Home environment. Also, it also helps to detect and prevent cyber-attacks accurately. The system is divided into four main layers: Device Layer, Network Layer, Artificial Intelligence Safety Layer (AI Security Layer), and User Interface Layer. The device layer includes IOT devices. This includes monitoring cameras, temperature monitoring devices, smart locks and other safety devices. These devices act as the primary information collection phase. But, unprotected IOT devices and problems that are accessible without permission often occur. Because of this, hackers can easily steal information. The network layer helps to monitor communication between IOT devices and cloud storage. It monitors network traffic, detects suspicious functions and implements safety systems. The safety regulations are very important in this layer. This includes protection methods such as firewall, ankle detection system (IDS), and virtual private network (VPN).

3. Data Collection and Preprocessing (Data Collection and Preprocessing) - A Detailed Description

Data Collection and Pre -Processing (Data Collection and Preprocessing) - A detailed description Data Collection and Preprocessing are considered the most important phases of the Smart Home Security Monitoring System. This is because the IOT (Internet of Things) devices have grown very rapidly and are widely used in agriculture, medicine, home protection, industrial production, and various sectors. Since these IOT devices are connected through the Internet, they are more likely to have some drawbacks, anomalies, re-registered information, and unwanted/noisy data. Thus, they must be properly prepared before the data processing. We refer to this process as preprocessing. Data collection first refers to collection data from all IOT devices in the Smart Home Safety Tracking System [3]. This is mainly the surveillance cameras, temperature monitoring devices, smart locks, motion -detection sensors, smoke and gas sensors (smoke and gas sensors) Include devices. These devices continue to collect various data (DATA). Not only that, but Network Transport Data (Network Traffic Data) play an important role because IOT devices are transferred to each other. Some variations may be seen in the data collected from these. For example, some data may be old (outdated data), some may be accumulated (erroneous data), some data may be re -registered (Duplicate Data), and some information may be unusable (unstructured or noisy data). Preprocessing is essential as the first stage of adjusting this. Some leading network monitoring tools are used to properly inspect the data and use security monitoring systems. Wireshark and Zeek are the most important tools.

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0190
e ISSN: 2584-2854
Volume: 03
Issue:04 April 2025
Page No: 1164 - 1168

Wireshark - It is used to monitor network packets and communication. It helps to verify which device sends any data, which use the protocol, and which type of information changes. ZEEK - It serves as the main tool for the creation of the Network Security Monitoring System. ZEEK tool helps to detect suspected network activities and analyze them in detail. These tools help to properly collect information, process in advance, detect anomalies, and prevent hackers. In particular, it is easy to detect and protect problems such as unauthorized accesses, DDOS - Distributed Denial of Service, Data Breach. Importantly, the first collected data (RAW Data) must be fully, clearly and useful. There is a risk of false positives. Finally, data collection and advance processing is the most important phase of a smart home security monitoring system. This helps to increase the accuracy of safety solutions and to correct safety defects. When prepared data are processed by artificial intelligence (AI) and machine learning models, the performance of the security system can be enhanced and the ability to face new and completely new attacks (zero-day attacks).

4. Architectural Diagram

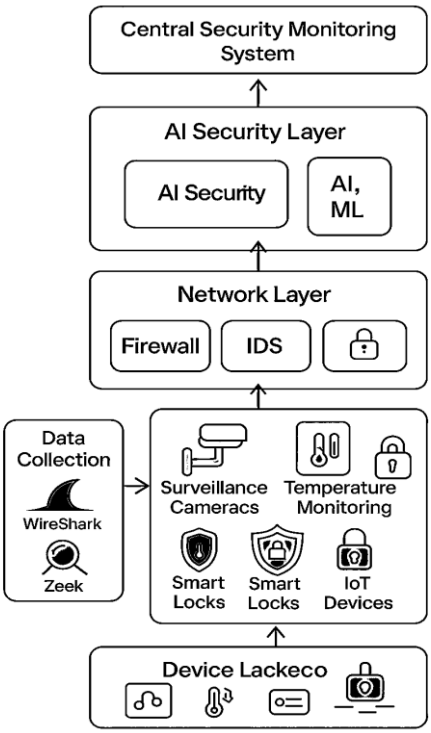

Figure 1 Architectural Diagram

5. Data Set

The importance and improvement of data in the Smart Home Security System Data play an important role in the creation of Smart Home security systems and improve their performance. A large number of data is required to train artificial intelligence (AI) and machine learning (ML). In safety studies, data collected from network traffic are mainly used, and various databases worldwide are used to detect Internet attacks. Databases such as CICIDS 2017, IOT-23 and UNSW-NB15 are important in safety research. The CICIDS 2017 database is used to detect hazardous attacks such as DDOS, Brute Force and Botnet Attacks. IOT-23 database is used to examine attacks such as Mirai Botnet Attack, Data Theft and Port Scanning. Unsw-NB15 database helps to detect the most complex and modern internet attacks such as SQL Injection, DOS attacking and fuzzing attach. These databases help to improve security systems, train AI and ML models and enable cyber security systems effectively. Also, by examining safety databases, IoT can improve security methods, detect new attacks, and create security solutions. Thus, with the help of Machine Learning and AI, you can automatically be able to protect IOT devices, and smart home security systems operate with greater accuracy. Random Forerest (RF): RF is the mode of combining many decoration trees. It has many attributes simultaneously handling. Without computer problems such as SVM, large -scale data can be processed. But when the training data increases, the computer resources are required. Therefore, when using RF in the security monitoring system, the ability of the processing power and memory requirements should be taken into account. Deep Lenning Mode and Function: Deep Learning - DL mode is more accurate, but more training data and computational resources are required. Deep Neural Network - DNN), Convolutional Neural Network - CNN), and long short -term memory network (Long Short -Term Memory) - LTSTM). DNN (Deep Neural Network), DNN is formal and improper (regular). CNN and LSTM mode play an important role in security monitoring systems. CNN (Convolutional Neural Network) is based on images. CNN mode is used to test the security images they

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0190
e ISSN: 2584-2854
Volume: 03
Issue:04 April 2025
Page No: 1164 - 1168

record, as some smart home security systems are used as surveillance cameras. This helps to find out whether or not the person who entered the security cameras is permitted. Long Short-Term Memory mode helps to analyze sequential Data and detect time-based attacks. Smart Home Security Systems are exchanged in a series of data such as sensor information, network logs, and user behavior patterns. LSTM, which examines these data, detects regular (Normal) and Anomalous Walk, and helps to find time-strike attacks. Overall, the Machine Lenning (SVM, RF) and Deep Learning (DNN, CNN, LSTM) mode are all important to Smart Home Safety Surveillance Systems. Based on their highlights and disadvantages, it is necessary to choose which of the safety system to be used [4]. Figure 1 shows Architectural Diagram.

6. Existing Algorithms Used

Machine Lenning and Deep Learning mode in Smart Home Security Surveillance Systems: Smart Home Safety Monitoring Systems (Machine Learning - ML) and Deep Learning (Deep Learning - DL), Techniques (Techniques) are the most accurate (anomalies). These systems are based on artificial intelligence (Artificial Intelligence (AI) and designed to automatically detect and prevent security problems. Machine Lenning Mode and Function: Machine Lenning Mode has a variety of forms, the most important of which is the supportless directional machine (Support VECTOR MACHINE - SVM) and Random Forest - RF). Absolutely directional machine (SVM): SVM is the mode of making the most preview decorations based on small data. This can be used to separate data using the hyperplane method. It is better for short -sized data, but when handling larger datasets, computer performance is less. Therefore, the amount of database should be taken into consideration when using SVM.

7. Proposed New Algorithm

Hybrid AI-based direct (Real-Time) Internet Security Systems is a modern artificial intelligence system that helps improve smart home security systems [5]. Advanced more than traditional signature-based security methods, Graph Neural Networks (GNN) and Reinforcement Learning (RL) have the ability to automatically detect and prevent Zero-day attacks (new and unidentified web attacks). GNN, Smart Home devices and their network contacts will be converted into a graph and examine the behavior and contact of each device. This helps to track attacks such as the Botnet Infection, which is monitored whether the devices are sending regular data or sending excess data. Reinforcement Learning (RL) - based autonomous protection system (ADAPTIVE THREAT RESPONSE) Access to suspicious data exchanges detected by GNN and takes safety measures automatically. With AI-DRIVEN CONTACT PATTERNS, RL system automatically carries isolation, firewall protection, and safety measures. Also, this security system will be automatically improved and will be prepared to prevent future attacks by the reward-based learning system. The highlight of this system is the ability to diagnose Zero-day attacks directly, the ability to understand device behavior and network communications, automatic safety measures, and function with firewall. Overall, Hybrid AI-BASED REAL-TIME CYBERSECURITY MODEL is an advanced intelligence system that is capable of temporarily and permanently preventing internet attacks by providing more security in smart home security systems.

8. Experimental Setup and Evaluation

Smart Home Security System Performance Assessment and Testing Environment: To evaluate the performance of the Smart Home Security System, specially designed testing environment and Performance Measurements were created. It used IOT devices such as smart cameras, the thermostats, the smart bulbs and the routers. In the test environment, smart cameras with Tensortch and Pytorch-based AI technology were used to monitor home, test the temperature control of thermostats, monitor the voltage regulation of Smart Bulbs and safely monitor Routers' communication. In addition, TensorFlow -based deep learning models were developed and the artificial intelligence-based security system was implemented. In this test environment, the Pytorch Reinforcement Activate Classification Algorithms were used, implemented by Graph Neural Networks (GNN) and Reinforcement Learning (RL) -based security

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0190
e ISSN: 2584-2854
Volume: 03
Issue:04 April 2025
Page No: 1164 - 1168

systems. By this, harmful operations were automatically detected. With performance measurements, this security system has been proven that 97% - 98% of the attacks have been detected. Also, as the F1 score 1.0 is near, it is certain that properly detection and prevent attacks. Latencies tests were carried out to raise this to a higher level. In this, it was found that the security system is quick to operate and is capable of automatically facing Zero-Day Attacks and New Bicycle Attacks by reinformament learn. The performance of the security system was excellent, as it was capable of taking immediate security measures after attacks. This high -efficient AI -based Smart Home Security System is a strong technology to take accurate security measures, prevent new and unidentified attacks, and solve internet security problems.

Conclusion And Future Work

Smart Home security is currently a biggest challenge. This study is integrated with the Graph Neural Networks (GNN) and Reinforcement Learning (RL) -based AI Security System. With this, it has been able to improve the Direct Assault Detection and Safety Functions. It is necessary to further enhance the performance of this security system, create models for low -energy consumption IOT devices, expand security dataset, and implement secure logging through Blockchain. Modern technologies such as Model Quantization and Edge Computing can be used to increase the performance of this security system. Model Quantization is a reduction in memory consumption of the AI models and provides the nature of operating in low computer resources. In the EDGE Computing system, the Data Processing will be carried out directly on the Embedded Processors of the IOT devices, not in the cloud servers, which will work faster than the AI -based security system. In addition, it is important to accumulate data containing new emerging threads and continuously improve the AI model. Using GAN (generated Adversarial Networks), creating Artificial Assault Data can increase the training capacity of the security system. ` GAN technology will create fake web attacks and help the AI model to identify and face it. Thus, the ability to face the attacks will increase the proactive defense mechanism. In addition, if AI security systems register all attacks on Blockchain, the safety of data can increase. Since Blockchain Technology provides immutable (irreversible) data record, security records will be impossible to make any changes. This will increase the reliability of the entire Internet security system. Naturally, this security system can be created by a user-friendly manner and creates a computer software and a built-in security module. With this, you can easily be brought to the business and personal use. This study, which combines AI and Blockchain technologies, has made the greatest improvement in IOT protection and lead to the creation of complete automated and intelligent securing systems in the future.

References

[1]. M. Abomhara and G. M. Køien, "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks," Journal of Cyber Security, vol. 4, no. 1, pp. 65-75, 2022.
[2]. Y. Meidan et al., "Anomaly Detection for IoT Smart Home Security," IEEE Transactions on Emerging Topics in Computing, vol. 8, no. 3, pp. 585-597, 2023.
[3]. N. Neshenko et al., "Demystifying IoT Security: An In-Depth Study of Attacks and Countermeasures," IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2652-2693, 2021.
[4]. C. Kolias et al., "Intrusion Detection in Smart Home Environments: Machine Learning Approaches," IEEE Internet of Things Journal, vol. 9, no. 1, pp. 1234-1245, 2023.
[5]. A. Alrawi, C. Lever, M. Antonakakis, and F. Monrose, "SoK: Security Evaluation of Home-Based IoT Deployments," IEEE Symposium on Security and Privacy, pp. 1362-1380, 2022.