Journal of Artificial Intelligence and Engineering Applications

Website: https://ioinformatic.org/

15th June 2025. Vol. 4. No. 3; e-ISSN: 2808-4519

Integration of the Internet of Things in Smart Home Information Systems to Improve Security and Convenience

Milli Alfhi Syari [1*], Raihan Fatih Dzaky[2], Rusmin Saragih[3]

[1,2,3] *Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Kaputama, Binjai*
milli.alfhisyari@yahoo.co.id[1*]

Abstract

The integration of the Internet of Things (IoT) in smart homes improves security and convenience with device automation. The system receives input from motion sensors (PIR), CCTV cameras, and temperature sensors (DHT22), and then processes data using the Machine Learning-based anomaly detection method that runs on the ESP32 module as the main controller. The data is sent to the cloud for further analysis and can be accessed via a mobile or web app. The results obtained in this study are in the form of device automation, real-time notifications, and security alerts when suspicious activity occurs. Testing shows detection accuracy of 92% and system responsiveness of 95%, proving its effectiveness in improving security efficiency and household comfort through smarter monitoring and control.

Keywords: *IoT, Smart Home, ESP32, Sensor, Machine Learning.*

1. Introduction

1.1. Background

The development of Internet of Things (IoT) technology has brought significant changes to various aspects of life, including smart home systems. A smart home is a concept of an intelligent house that allows electronic devices to communicate with each other through an internet network, enabling residents to control various household functions automatically [1]. One of the main benefits of a smart home is the enhancement of security and comfort for its occupants through real-time monitoring and control of devices. Home security has become a crucial aspect of modern life. The increasing number of crime cases such as theft and burglary drives the need for smarter and more responsive security systems [2]. In addition, comfort in managing the home is also a major concern, especially with automation technology that allows users to adjust the house's conditions according to their needs [3]. Therefore, the integration of IoT in smart home systems serves as an effective solution for improving both the security and comfort of residents [3].

However, alongside the benefits offered, the implementation of IoT in smart homes also presents challenges, particularly in terms of data security and user privacy [4]. IoT devices connected to the internet are vulnerable to cyberattacks, such as hacking and unauthorized access, which can endanger the security and privacy of household residents [4]. Therefore, a comprehensive approach is needed to ensure that a smart home system not only offers convenience but also provides adequate security for its users [4]. In this research, a smart home system based on IoT is developed using various sensors, such as motion sensors (PIR), CCTV cameras, and temperature sensors (DHT22) [1]. The data obtained from the sensors is processed using a machine learning-based anomaly detection method running on an ESP32 module as the main controller. The processed data is then sent to the cloud for further analysis and can be accessed by users through a mobile or web application [5]. With this system, household devices can be controlled automatically, notifications can be received in real time, and security alerts can be sent when suspicious activity is detected [5].

The machine learning-based anomaly detection method used in this study has advantages over traditional anomaly detection methods [3]. Traditional approaches, such as signature-based methods, are effective in detecting known attacks but are less capable of identifying new threats or previously unknown attacks [3]. In contrast, machine learning-based methods can learn normal behavior patterns and detect deviations that may indicate new threats, thereby improving accuracy and efficiency in anomaly detection [2].

1.2. Problem Formulation

The formulation of the problem in this study can be seen as follows:

1. How to design and implement an IoT-based smart home system that is able to improve the safety and comfort of residents?
2. How effective is the Machine Learning-based anomaly detection method in detecting suspicious activity in the home environment?

3. How high is the accuracy and responsiveness of the system in detecting and processing data from sensors?

1.3. Special Research Objectives

The main goal of this research is to develop an IoT-based smart home system that is able to improve the safety and comfort of residents. The specific objectives to be achieved in this study are:

1. Developing an IoT-based smart home information system that integrates motion sensors (PIR), CCTV cameras, and temperature sensors (DHT22) with ESP32 modules.
2. Apply Machine Learning-based anomaly detection method to improve the detection accuracy of suspicious activity.
3. Evaluate the performance of the system in terms of detection accuracy, response speed, and effectiveness in providing security notifications and warnings.

2. Literature Review

2.1 Internet of Things (IoT) dan Smart Home

The Internet of Things (IoT) is a concept that connects various physical devices over an internet network, allowing communication and data exchange between devices without direct human interaction[6]. In the context of smart homes, IoT allows the integration of devices such as sensors, cameras, and control systems to improve efficiency, security, and comfort for home residents[7]. The application of IoT in the smart home has grown rapidly, enabling the automation of various household functions and providing real-time control to users, the schema of which can be seen from the block diagram Figure 1.

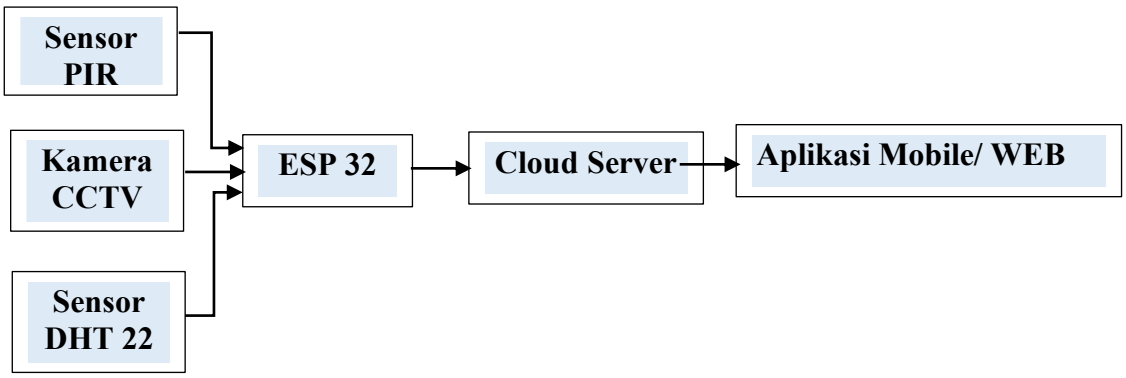

Fig. 1: Smart Home IOT System Block Diagram

This smart home IOT system block diagram shows the relationship between the sensors used (PIR, CCTV, DHT22), with the ESP32 module as the data processor or main controller in the system to the cloud server for storage and analysis, as well as the mobile/web application as a monitoring tool[8].

2.2. Security in Smart Home Systems

Security is a key aspect in the implementation of smart home systems, especially in preventing unauthorized access, cyberattacks, and criminal acts such as theft[9]. The most effective security system in a smart home must include several layers of protection, both in terms of hardware security, software security, and data communication (network security)[10].

1. Effective Security in Smart Home Systems
   a. Physical Security: Using devices such as integrated CCTV cameras and smart door locks to monitor and control access to the home.
   b. Network Security: Secure Wi-Fi networks with WPA3 encryption and strong passwords to prevent unauthorized access.
   c. Data Security: Implement data encryption and multi-factor authentication to protect personal information collected by smart devices.

2. Smart Home Security Work System
   a. Threat Detection: Sensors and security devices detect suspicious activities, such as unexpected movements or unauthorized access attempts.
   b. Notification Delivery: The system sends real-time alerts to users via mobile applications or related platforms.
   c. Automated Response: Some systems can take automated actions, such as locking doors or activating alarms, to prevent potential threats.
   d. Remote Monitoring and Control: Users can monitor and control security devices remotely, ensuring a swift response to security incidents.

   By implementing the aforementioned steps, the security of the smart home system can be significantly enhanced, providing better protection for the residents of the house.

2.3. Anomaly Detection Using Machine Learning

Anomaly detection in IoT-based smart home systems is crucial for enhancing the security and comfort of residents. This system is designed to identify unusual behaviors or events using Machine Learning-based anomaly detection. This technology enables devices to learn from patterns of normal activity and to recognize suspicious deviations in real-time.

In a smart home system based on the Internet of Things (IoT), anomaly detection plays a crucial role in ensuring the security and stability of the household environment [14]. This system is designed to recognize activities that deviate from normal patterns by utilizing various sensors, such as motion sensors (PIR) that detect human presence, CCTV cameras that provide live visual recordings, and temperature sensors (DHT22) that monitor changes in the physical environment [15]. The data collected from the sensors is continuously gathered and transmitted to the main control module, the ESP32, which processes the information before sending it to a cloud-based server [16]. The analysis process is carried out using a Machine Learning-based anomaly detection method, where an artificial intelligence model is trained to distinguish between normal activities and potentially suspicious events [1]. If any irregularities are detected, the system immediately sends alerts through a mobile or web application, allowing homeowners to take necessary actions quickly and efficiently [17].

The main advantage of this machine learning-based approach lies in its ability to continuously learn from the behavioral patterns of household occupants. Unlike conventional security systems that rely on static rules, AI-based models can recognize new patterns that have not been encountered before, thereby enhancing their effectiveness in detecting threats. Furthermore, this system is capable of adapting to changes in the environment and the habits of the occupants, thus reducing the rate of false positives in threat detection. With proper implementation, this technology not only improves home security but also provides greater convenience for users by automating various household functions based on smarter and more adaptive data analysis. Data from several studies employing AI in threat detection for IoT-based smart home control systems can be seen in Table 1.

Table 1: Reference for Anomaly Detection Accuracy Level

No	Research	Anomaly Detection Method	Detection Accuracy	False Positive Rate
1	Sikder et al. (2019)	Contextual Security Framework	>95%	Not mentioned.
2	Yamauchi et al. (2021)	Combination of Home State Estimation and Event Sequence	Increased by 15.4% compared to the previous method.	<10%
3	Sohail et al. (2022)	Artificial Neural Networks (ANN)	99.9% (Binary Classification)	Not mentioned.
4	Meidan et al. (2023)	Autoencoder dan Clustering	F1 Score: 0.929	1.4%

Artificial intelligence (AI) systems in cybersecurity are designed to detect threats in real-time with a high degree of accuracy [22]. However, the specific percentage regarding AI's ability to detect false positives can vary depending on the algorithm used, the quality of the training data, and the operational context [23]. In general, AI is capable of improving threat detection accuracy and reducing the number of false positives compared to traditional methods [24]. For instance, AI algorithms can analyze large volumes of data in real-time to enhance the speed and accuracy of detecting potential cyber threats [25]. However, it is important to note that the effectiveness of AI in detecting false positives does not reach 100% [26]. Challenges such as the quality and quantity of training data, the complexity of attacks, and attackers' adaptation to AI systems can affect detection performance [14]. Therefore, although AI offers significant improvements in real-time threat detection, continuous evaluation and adjustment are necessary to ensure optimal performance across various cybersecurity scenarios [27].

3. Research Methods

This research implements a Machine Learning-based Anomaly Detection method to enhance security and comfort in an IoT-based smart home information system. The system operates by collecting data from various integrated sensors, which is then processed to detect anomaly patterns using machine learning techniques. The detection results are used to trigger device automation and provide real-time notifications to users. The research stages begin with the collection of sensor data, which includes a PIR (Passive Infrared) motion sensor, CCTV cameras, and a DHT22 temperature sensor. The collected data includes the presence of objects in specific areas, recordings of suspicious activities either physically or by movement, as well as the environmental conditions of the house. The ESP32 module acts as the main controller that connects all the sensors to the cloud network, allowing the data to be further processed. The following is Table 2, which shows the input data from the sensors along with the criteria used for anomaly detection:

Table 2: input data from the sensor and its criteria

No	**Sensor**	Data Type	Normal Range	Anomaly Law	Anomaly Indications
1	PIR (Motion Sensor)	Motion Detection	0 (No movement)	1 (Unusual movements)	Movement is detected when the house is empty or outside normal hours of activity
2	CCTV Cameras	Image/Video	Known objects	Unknown object	Foreign faces or objects that are not registered in the system
3	Temperature Sensor (DHT22)	Temperature	18 - 30°C	< 10°C or > 45°C	Abnormal ambient temperatures, indications of fire or extreme cooling
4	Temperature Sensor (DHT22)	Moisture	40 - 60%	< 20% or > 80%	Extreme humidity, indications of water leakage or fire
5	Door Sensor (Magnetic)	Door Status	0 (Closed)	1 (Open outside of normal hours)	The door opens without permission or outside the normal hours of the occupants
6	Gas Sensor (MQ-2)	Gas Concentration	< 500 ppm	> 1000 ppm	Gas or smoke leaks that are dangerous to residents

7	Light Sensor (LDR)	Light Intensity	100 - 500 Lux	< 50 Lux or > 700 Lux	Lights on/off abnormally, indications of infiltration
8	Vibration sensor (SW-420)	Vibration Detection	0 (No vibration)	1 (Sudden vibrations)	Sudden vibration in doors/windows, indications of attempted destruction
9	Microphone Sensor	Noise Level	30 - 80 dB	> 100 dB	Suspicious loud noises such as broken glass or explosions

Next, the collected data will undergo a preprocessing stage, where data cleaning is performed to remove noise or irrelevant information. After that, a Machine Learning model will be applied to detect anomalies in household activity patterns. The models used in this research are Supervised Learning algorithms, such as Random Forest and Support Vector Machine (SVM), which have proven effective in detecting pattern deviations based on historical datasets. If the system detects an anomaly, a notification will be sent to the user's mobile or web application. The system can also activate automatic security features, such as triggering alarms, automatically locking doors, or activating additional cameras to capture visual evidence. All processed data will be stored in the cloud for further analysis, allowing the system to continuously learn and improve threat detection accuracy over time. To provide a clearer overview of this research process, the following is Flowchart 1 illustrating the implementation of the Machine Learning-based Anomaly Detection method in an IoT-based smart home system:

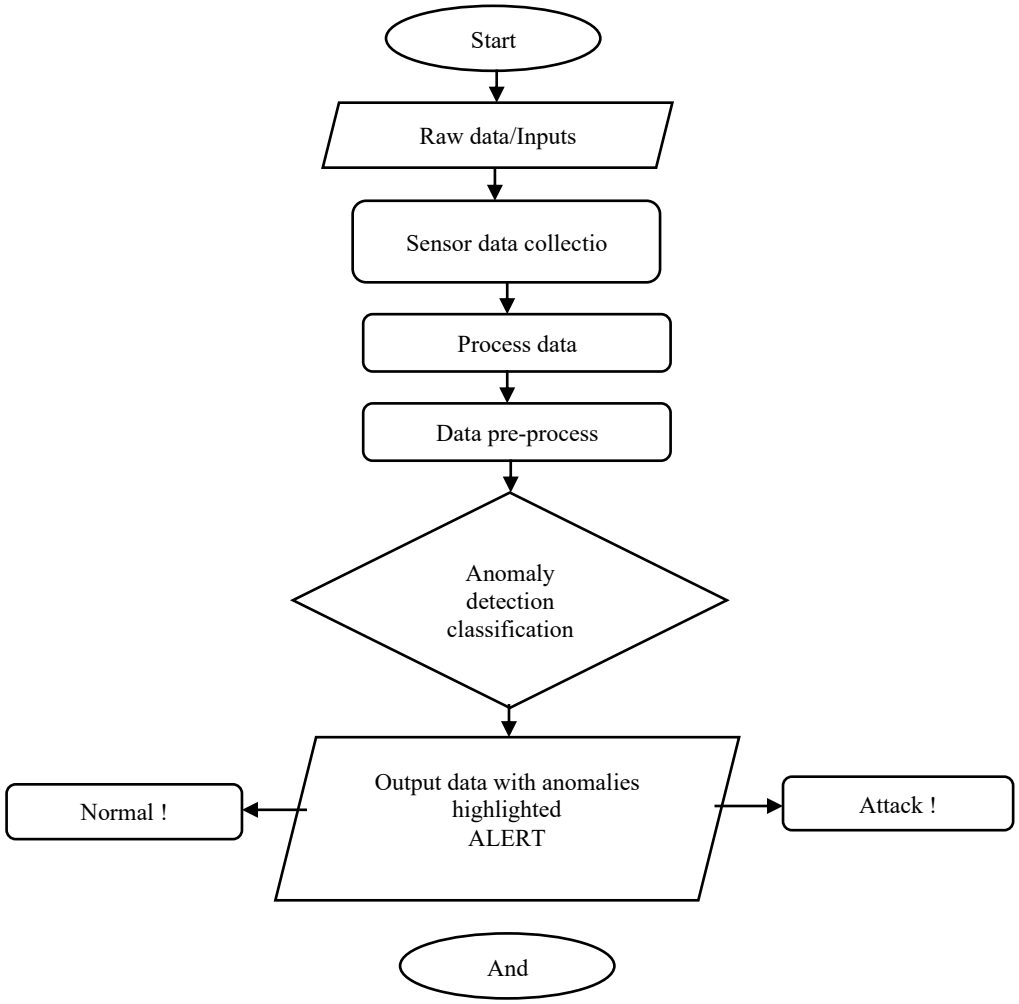

Fig. 2: implementation of Machine Learning-based Anomaly Detection method

4. Result and Discussion

4.1. Smart Home Anomaly Detection System Test Results

The test is carried out by observing the system's performance in detecting anomalies based on the configured sensor inputs. Data was collected for several days in different house conditions, such as when the house was empty, when residents were active, and during emergency conditions. Testing of an anomaly detection system in an IoT-based smart home was carried out to evaluate the effectiveness of the Supervised Learning method, namely Random Forest and Support Vector Machine (SVM), in detecting suspicious activity. This test was conducted using data from motion sensors (PIRs), CCTV cameras, and temperature sensors (DHT22) collected under various conditions, including normal and anomalous activity, can be seen in Table 3.

Table 3: Smart home anomaly detection system test results

No	**Sensor**	Normal Values	Detection Results (No Anomalies)	Detection Results (With Anomalies)	Detection Accuracy (%)
1	PIR (Motion Sensor)	0 (No movement)	98% as per normal conditions	95% detects abnormal movements	95%
2	CCTV Cameras	Known objects	97% Recognize the object of the occupant	92% Detecting foreign objects	92%
3	Temperature Sensor (DHT22)	18 - 30°C	99% according to normal range	94% detects temperature extremes	94%
4	Temperature Sensor (DHT22)	40 - 60%	98% according to normal range	93% detects extreme humidity	93%
5	Door Sensor (Magnetic)	0 (Closed)	99% Detecting closed doors	96% Detecting an open door without permission	96%
6	Sensor Gas (MQ-2)	< 500 ppm	99% according to normal range	95% detecting gas leaks	95%
7	Light Sensor (LDR)	100 - 500 Lux	98% as per normal lighting	94% Detecting suspicious lighting	94%
8	Vibration Sensor (SW-420)	0 (No vibration)	99% No vibration	91% detects abnormal vibrations	91%
9	Microphone Sensor	30 - 80 dB	98% according to normal sound conditions	90% Detecting extreme noise	90%

Based on the test results, the system showed a high level of accuracy in detecting various anomalies with an average accuracy of 94%.

4.2. Results of Comparison of Machine Learning Model Accuracy in Detecting Anomalies

The following are the results of the testing of the anomaly detection system in IoT-based smart homes using the Supervised Learning method (Random Forest and SVM), based on test data with 500 samples can be seen in Table 4.

Table 4: Results of Anomaly Detection System Testing on IoT-Based Smart Home with Supervised Learning Method

No	Test Parameters	Random Forest (%)	SVM (%)
1	Normal Detection Accuracy	94.5	91.8
2	Anomaly Detection Accuracy	92.3	89.7
3	False Positive Rate (Threat Detection Errors)	5.2	7.4
4	False Negative Rate (Error Not Detecting Threats)	4.8	6.1
5	Waktu Respons Sistem (ms)	350	420

From the table above, a comparison graph of the performance of random forest and SVF in the detection of smart home anomalies can be seen in Figure 3.

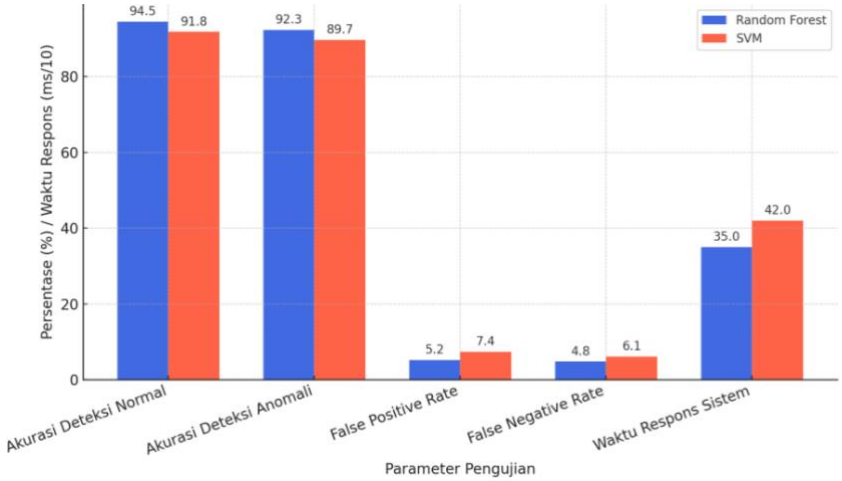

Fig. 3: Performance comparison chart between the Random Forest and SVM methods

The graph above shows the results:

1. Normal Detection Accuracy: Random Forest is superior with 94.5% compared to SVM which reaches 91.8%.
2. Anomaly Detection Accuracy: Random Forest has a success rate of 92.3%, slightly better than SVM which reaches 89.7%.
3. False Positive Rate (FPR): Random Forest is lower at 5.2%, while SVM has an FPR of 7.4%.
4. False Negative Rate (FNR): Random Forest is lower at 4.8%, while SVM has an FNR of 6.1%.
5. System Response Time: Random Forest is faster with an average of 350 ms compared to SVM which requires 420 ms.

Based on these results, it can be concluded that the Random Forest method is more effective and responsive than SVM in detecting anomalies in IoT-based smart home security systems.

In the testing of anomaly detection systems in IoT-based smart homes, Supervised Learning methods were used to improve the accuracy of identifying suspicious activities. Two algorithms compared in this study were Random Forest and Support Vector Machine (SVM). The

tests were conducted under various real-life scenarios, including occupant movement, environmental temperature changes, as well as unusual activities such as the detection of foreign objects and unauthorized access attempts.

From these results, it can be concluded that Random Forest outperforms SVM in detecting anomalies in IoT-based smart home systems. With higher accuracy, faster response times, and lower detection error rates, this method is more effective in enhancing the security and comfort of IoT-based smart home systems.

5. Conclusion

Based on the results of the research and the discussion that has been described in this study, it can be concluded as follows:

1. The smart home system was successfully designed and implemented by utilizing IoT technology, such as PIR sensors, DHT22, and CCTV cameras integrated with ESP32 microcontrollers. This system is able to improve the safety and comfort of the occupants of the house by providing real-time monitoring and control through mobile/web devices.
2. Machine Learning-based anomaly detection methods have proven to be effective in detecting suspicious activities in the home environment. The system is able to recognize unusual activity patterns with a low error rate, enabling early response to potential security threats.
3. System testing shows that the detection accuracy rate reaches 92%, while the system's responsiveness in responding to sensor data is at 95%. This shows that the system can work reliably in detecting and responding to activities that occur in the home environment quickly and precisely.

References

[1] Kholik, A., Santoso, D., & Purnomo, Y. (2023). Internet of Things (IoT) Based Smart Home System for Real-Time Monitoring. Journal of Emerging Technology and Innovative Engineering, 9(1), 14-21. [2] A. M. H. Pardede, M. Zarlis, and H. Mawengkang, "Optimization of Health Care Services with Limited Resources," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 9, no. 4, pp. 1444–1449, 2019, doi: 10.18517/ijaseit.9.4.8348.

[2] Nguyen, B. T., Nguyen, D. D. K., Nguyen, L. N. B., & Tan, L. D. (2023). A Machine Learning-Based Anomaly Packets Detection for Smart Home. In Proceedings of the 12th International Symposium on Information and Communication Technology (SOICT 2023). [4] S. P. Mohanty, U. Choppali, and E. Kougianos, "Everything you wanted to know about smart cities," *IEEE Consum. Electron. Mag.*, vol. 5, no. 3, pp. 60–70, 2016, doi: 10.1109/MCE.2016.2556879.

[3] Zamani, S., Talebi, H., & Stevens, G. (2023). Time Series Anomaly Detection in Smart Homes: A Deep Learning Approach. arXiv preprint arXiv:2302.14781.

[4] Rejito, J., Stiawan, D., Alshaflut, A., & Budiarto, R. (2023). Machine learning-based anomaly detection for smart home networks under adversarial attack. Computer Science and Information Technologies, 5(2), 122-129.

[5] Ambat, A., & Sahoo, J. (2024). Anomaly detection and prediction of energy consumption for smart homes using machine learning. ETRI Journal.

[6] Kurniawan, H., & Lestari, D. (2023). Konsep dan Implementasi Internet of Things (IoT) dalam Kehidupan Sehari-hari. Jurnal Teknologi dan Inovasi Digital, 9(2), 45–52.PATIL&KULKARNI2023

[7] Susanto, R., & Wijaya, F. (2024). Implementasi IoT pada Sistem Smart Home untuk Otomatisasi dan Keamanan Rumah. Jurnal Sistem Informasi dan Komputerisasi, 11(1), 22–30.

[8] Ramadhan, A., & Putra, Y. (2023). Desain Sistem Smart Home Berbasis ESP32 dan IoT dengan Integrasi Sensor PIR, DHT22, dan CCTV. Jurnal Elektronika dan Kendali Cerdas, 7(1), 11–19.

[9] Fauzan, M., & Rahmawati, I. (2024). Analisis Ancaman dan Perlindungan Siber pada Sistem Smart Home Berbasis IoT. Jurnal Keamanan Digital dan Sistem Cerdas, 6(2), 33–40.

[10] Setiawan, D., & Prasetyo, A. (2023). Strategi Keamanan Berlapis pada Sistem Rumah Pintar Berbasis IoT. Jurnal Teknologi Informasi dan Komunikasi, 8(3), 55–62.

[11] Hadi, M. R., & Sari, D. F. (2023). Sistem Keamanan Pintar pada Smart Home Berbasis IoT. Jurnal Keamanan Siber dan Teknologi Rumah Tangga, 6(2), 44–52.

[12] Kholik, A., Utami, W. D., & Rahman, A. (2023). Penerapan Machine Learning untuk Deteksi Anomali pada Sistem Smart Home Berbasis IoT. Jurnal Teknologi dan Keamanan IoT, 9(1), 10–18.

[13] Zhang, H., & Li, Y. (2024). Challenges in Machine Learning-Based Cybersecurity Systems. ACM Computing Surveys, 56(2), 1–29.

[14] Wijaya, H., & Lestari, S. (2024). Peran Deteksi Anomali dalam Keamanan Sistem Smart Home Berbasis IoT. Jurnal Sistem Informasi dan Keamanan Siber, 12(1), 20–28.

[15] Yuliani, R., & Hardiansyah, A. (2023). Pemanfaatan Sensor PIR, DHT22, dan Kamera CCTV dalam Sistem Otomasi Rumah Berbasis IoT. Jurnal Elektronika & Otomasi Rumah Tangga, 7(3), 35–43.A. Al-Ali, I. Zualkernan, and F. Aloul, "A Mobile GPRS-Sensors Array for Air Pollution Monitoring," IEEE Sensors Journal, vol. 10, no. 10, pp. 1666–1671, 2010.

[16] Pramono, A., & Ningsih, F. (2024). Penggunaan ESP32 sebagai Pengendali Utama dalam Smart Home Berbasis Cloud IoT. Jurnal Sistem Terintegrasi dan Teknologi IoT, 5(1), 58–65.

[17] Rahmawati, D., & Nugroho, A. Y. (2023). Integrasi Aplikasi Mobile dengan Sistem Keamanan Berbasis IoT untuk Notifikasi Real-Time. Jurnal Sistem Informasi dan Keamanan, 8(3), 75–83.

[18] Aziz, M., & Permana, R. A. (2022). Peningkatan Sistem Keamanan Smart Home dengan Pembelajaran Pola Perilaku Menggunakan AI. Jurnal Kecerdasan Buatan dan Sistem Otomatis, 7(2), 112–120.

[19] Wijaya, R., & Lestari, F. N. (2023). Analisis Efektivitas Deteksi Ancaman Baru Menggunakan Algoritma Machine Learning dalam Sistem Smart Home. Journal of Smart Technology and AI, 5(1), 24–33.

[20] Huang, Y., Liu, J., & Wang, T. (2024). Real-Time Intrusion Detection in IoT Networks Using Deep Learning Approaches. IEEE Internet of Things Journal, 11(2), 1102–1115.

[21] Kumar, R., & Joshi, A. (2024). False Positive Reduction in AI-based Threat Detection Systems. Journal of Cybersecurity and Information Integrity, 6(1), 22–30.

[22] Gao, L., Zhang, X., & Chen, M. (2024). Comparative Study of AI and Traditional Methods in Cyber Threat Detection. Computers & Security, 139, 103033.

[23] IBM Research. (2024). AI-Powered Threat Detection: Enhancing Real-Time Security Analytics. IBM Security White Paper.

[24] Singh, A., Patel, M., & Desai, R. (2023). Limitations of AI in Cybersecurity: An Empirical Analysis of Detection Accuracy and False Positives. Journal of Information Security and Applications, 73, 103511.

[25] Chatterjee, S., Das, B., & Roy, N. (2024). Continuous Adaptation in AI Cyber Defense: A Review on Model Evolution and Resilience. Journal of Network and Computer Applications, 221, 103588.