Published by The College of Science & Information Technology (COSIT), TASUED, Vol. 18, No. 1, pp. 8-21.

COSIT, TASUED
Journal of Science and Information Technology (JOSIT)

A Secure Smart Home Automation System with Mobile Platform

[1]✉Giwa T.A.; [2]Ajibola A.A.; [3]Oludare I.A.; [4]Abiodun E.O.; [5]Benedict A.D.; [6]Usman M.A.; and [7]Olawale-Shosanya S.O.

[1,3,4]Department of Computer Science, University of Abuja, Nigeria.
[2]Department of Accounting, Crescent University, Abeokuta, Ogun State, Nigeria.
[5]Department of Electrical and Electronics Engineering, Federal University of Technology, Akure, Nigeria.
[6,7]Department of Computer Science, Tai Solarin University of Education, Ogun State, Nigeria.
Corresponding Author: tawakalitu.giwa@uniabuja.edu.ng
Other Authors: ajibola.azeez14@gmail.com, oludare.abiodun@uniabuja.edu.ng, benedict.adeyi@gmail.com, morenikejiadebola@gmail.com, ssideeqoh@gmail.com

Abstract

The concept of a "smart home" has gained attention recently, facing challenges like decision-making, secure IoT device identification, continuous connectivity, and privacy. Existing systems address some of the issues, but a truly effective smart home needs built-in security and analytical capabilities. This work proposes a novel smart home using Z-wave and Wi-Fi, with the Dynamic Analysis and Preplanning Tool (DART) for maximum security. The system employs a support vector machine (SVM) classifier to determine device status ("OFF" or "ON"). The setup includes Raspberry Pi, a 5 V relay circuit, and sensors. An Android app communicates with the Raspberry Pi server via HTTP and Apache. Laboratory and field testing with common devices like TVs, air conditioners, and microwaves validate system effectiveness. TV reaction time increases with distance, but air-conditioner responses remain consistent, enhancing security through Z-wave, Wi-Fi, and DART integration. Our safety module safeguards smart home assets and blocks intruders, improving security and dependability in home automation. The performance of the model was assessed and validated using quantitative analysis techniques and statistical metrics in comparison with other state-of-the-art (SOTA) studies. Experimental findings analyzed using metrics like Mean Absolute Percentage Error (MAPE), Mean Absolute Error (MAE), Root Mean Square Error (RMSE), and VAPE, show that Z-wave, Wi-Fi, and DART offer superior dependability, low radio rebirth, simple operation, and straightforward interoperability compared to ZigBee, home plug, and INSTEON. This approach is cost-effective for replication, emphasizing potential security enhancements within a manageable budget.

Keywords: Internet of Things, Mobile application, Smart home devices, Wireless communications, Artificial intelligent language and Security.

1. INTRODUCTION

The pervasive presence of computers and the Internet in modern life renders their use unavoidable (Cretu et al., 2024; Yu et al., 2020; Kashaf et al., 2022; Phung et al., 2022). The concept of a smart home has gained significant interest in recent years.

The primary challenges in implementing smart homes include intelligent decision-making, secure identification and authentication of Internet of Things (IoT) devices, uninterrupted connectivity, data security, and privacy concerns. This paper introduces an innovative smart home concept utilizing a novel technology that incorporates three methodologies. to ensure optimal security in smart home automation for intelligent decision-making.

Cite as:
Giwa T.A., Ajibola A.A., Oludare I.A., Abiodun E.O., Benedict A.D. Usman M.A. and Olawale-Shosanya S.O. (2024). Mobile Application of Intelligent, Secure and Smart Home Automation System. *Journal of Science and Information Technology (JOSIT)*, Vol. 18 No. 1, pp. 8-21.

The protocols Z-Wave and Wi-Fi have been implemented alongside the Dynamic Analysis and Preplanning Tool (DART), an artificial intelligence language, to enhance security measures. This integration facilitates intelligent decision-making processes while leveraging Machine Learning (ML) to ensure the identification and authentication of IoT devices. Current systems often address only one or two of these concerns. However, there is a pressing need for a smart home automation system that encompasses robust security measures along with advanced decision-making and analytical capabilities.

Home automation, which includes the remote control and automation of electronic and electrical devices, is one of the most significant and widespread technological applications today. The multiple devices in a home can be wirelessly linked to one another and to the internet via wireless home automation networks (WHANs). Increasingly, people are recognizing the potential of data sharing and communication between multiple computers (Chen et al., 2014; Baykara & Çolak, 2018). Over the past decade, various smart home communication technologies have emerged to facilitate data sharing and connection among in-house appliances. Additionally, modern communication methods enable the remote management of various household appliances, significantly reducing the need for physical presence to perform tasks. There is a growing desire among individuals to manage household gadgets remotely.

Home automation systems as a technical method allow for control, feedback, appliance action, and smart monitoring based on the occupants' needs. Most switching processes today are still performed manually, without utilizing IoT principles. The convenience of controlling and operating all connected devices from a single interface is a major advantage. Fans, lights, and switches are among the household gadgets that can be managed remotely using a centralized control board.

Currently, many popular protocols, such as ZigBee, INSTEON, and HomePlug, are utilized to control home devices remotely (Talos, 2024). In this study, we analyze the Z-Wave protocol, a newer technology, and discuss its implementation in smart homes with remarkable performance. This wireless protocol offers superior reliability, low radio interference, high interoperability, and simple operation compared to the standard and widely adopted ZigBee protocol (Ahmad, Morelli, Ranise, & Zannone, 2022).

Recent work has addressed security issues in smart home automation systems, including Amazon Web Services (AWS) IoT, Samsung SmartThings, and Apple HomeKit. This study fills the security gaps identified in those systems. For instance, AWS IoT security gaps include (1) unrestricted and long-lived access to S3 buckets, (2) undetected request events to S3 buckets, (3) malicious AWS Application Programming Interface (API) requests, (4) unfiltered traffic from untrusted sources, (5) incorrect permissions and privileges, (6) login and credential theft, and (7) vulnerable multi-tenant cloud infrastructure (Ghayvat et al., 2015; Calderoni, 2019; Javeed, Gao, & Khan, 2021). An illustration of a smart home automation system using several IoT-connected appliances is provided in Fig. 1.

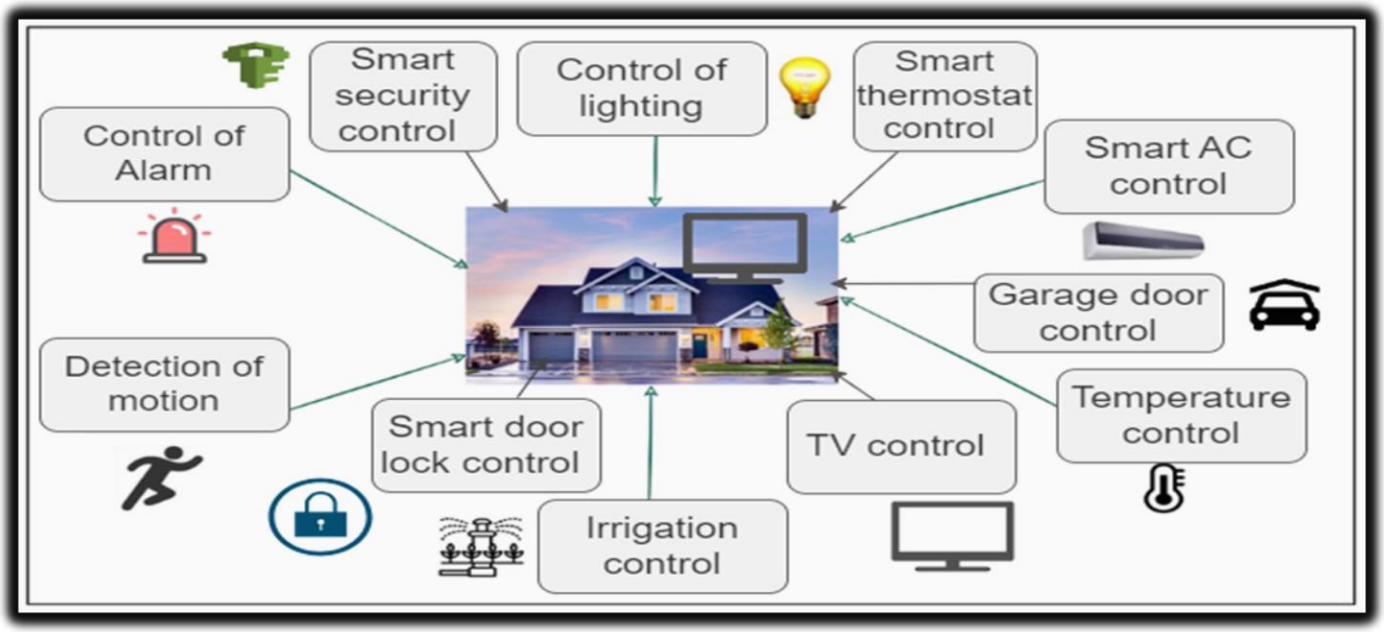

Fig. 1. Smart IoT-based home automation system with different sensing devices

The security gaps in Samsung SmartThings include multiple buffer overflow issues in the Samsung WifiScan handler of the 'video-core' Hypertext Transfer Protocol (HTTP) server used by the SmartThings Hub. An attacker could exploit this flaw by sending specially crafted HTTP POST requests to impacted devices. This vulnerability arises from the SmartThings hub processing user-controlled JavaScript Object Notation (JSON) incorrectly when it receives an HTTP POST request to the /Samsung WifiScan Uniform Resource Locator (URL).

These flaws can be activated by the values of the 'user', 'password', 'cameraIp', and 'callbackUrl' keys. This data is transferred to a destination buffer in memory using 'strcpy' without first validating the destination buffer's size, leading to an overflow condition (Mathew & Varia, 2014; Al-Boghdady, Wassif, & El-Ramly, 2021; Bosamia, 2013). Additionally, a significant security flaw in Apple's HomeKit has recently made headlines. For example, a typo can render iPhones and iPads useless. A vulnerability in iOS 11.2 enables unauthorized control of devices such as smart locks and

garage door openers (Yassein, Mardini, & Khalil, 2016; Abiodun et al., 2021; Taiwo, Ezugwu, Rana, & Abdulhamid, 2020).

This paper addresses all these security flaws in smart home automation systems, providing a comprehensive solution to enhance the security and functionality of IoT-connected devices in smart homes.

2. RELATED WORK

The IoT has many practical applications (Ho et al. 2016). and smart home automation is one of them since it enables convenient remote control and improved indoor air quality. It also reduced energy consumption. increased security, and other social and environmental benefits of connected living. With the help of IoT technologies, homeowners can manage their houses, appliances, environmental conditions, and activities in/out around their homes from anywhere in the world. Large number of commercial products have been created, tested, installed, and used for the intelligent control of smart house devices. These commercial products include Amazon Echo, Google Nest Hub, Apple HomeKit, Wink Hub2, and Samsung SmartThings which are just a few of them.

2.1. IoT

The IoT is a new generation of Internet technologies that promise to significantly improve life in several domains, including intelligent health, intelligent cities, intelligent

homes, and intelligent transportation, among others (Oliveira et al. 2018). Connecting and monitoring devices remotely through the Internet is what the IoT is all about (Stolojescu-Crisan, Crisan and Butunoi, 2021). The concept has advanced greatly in recent years and is used in many contexts, including smart homes, telemedicine, industrial settings, and many more. The IoT's wireless sensor network technologies allow for the worldwide interconnection of smart devices with expanded capabilities (Ho, Leung, Mishra, Hosseini, Song and Wagner, 2016). The Internet of Objects (IoOs) is an intelligent network that links all things to the Internet so they can exchange data and have two-way conversations via information shown in Table 1.

sensing devices using standard protocols. The IoT is a paradigm that relies on a system of embedded sensors and services. These sensors like Television, Air conditioners, fans, radios, light bulbs, and microwaves are built in to collect data and monitor environmental factors.

2.2. IoT Security

There has been an increase in recent research into IoT security and, more broadly, safety. IOTGUARD is compared to several previous approaches that differ in scope, focus, precision, and runtime. The approaches examined here are the most applicable to IoT app source code, as

Table 1. Comparison of IoT attacks and their Applicability to the Smart-Things platform

References	**Area of problem**	**Description of attack**	**Platform**	**SmartThings applicability**
Kashaf et al., (2022)	Situational use problem	Safeguarding smart homes against undesired application actions	SmartThings	X
Djenna et al., (2021)		Critical cyber infrastructure cyber security issues	IoT based infrastructure	X
Ho et al., (2016)		unintentional unlocking	Bluetooth Smart locks	X
Ho et al., (2016); Francillon, et al., (2011)		Relay unlocking through Bluetooth	Bluetooth Smart locks	X
Xiao et al., (2020)	Authentication vulnerability	A framework for smart home authentication that does not require credentials	SmartThings	X
Fernandes et al., (2016)		Insertion of backdoor pin codes	SmartThings	X
Pa et al., (2015) Yu et al., (2015)		Obtain the device's remote shell.	Telnet-capable Internet of Things devices	N/A
Ronen et al., (2016)		Utilizing flashing lights to reveal information or cause seizures	Smart connected LEDs	X
Bai et al., (2016)		To steal data, impersonate a device.	IoT device that support Bonjour	N/A
Wang et al., (2022)	Malicious software/app/firmware	IoT device behavioral security detection using firmware virtualization and deep learning	IoT-DeepSense	X
Jerkins and Stupiansky, (2018); Fedler et al., (2013)		Malware	Scanner for barcodes	X

Sood and Enbody, (2012)		Surveillance in the dark	Sony security camera	X

The IoT security study focuses on three topics which are Devices, Protocols, and Platforms (Jerkins and Stupiansky, 2018). Several Telnet-capable IoT devices are reportedly insecure in the context of IoT devices because their debugging interfaces are not protected or have weak or default passwords Javaid and Sikdar, 2021). The Kwikset door lock and the Philips Hue lighting system both have access control issues that prevent them from supporting critical use cases, according to (Celik, Tan and McDaniel, 2019). By employing strobe light, Ronen et al. showed extended functionality attacks on smart lighting that can reveal information and trigger seizures (Bai et al. 2016). Researchers have shown that the implementations of the ZigBee and ZWave protocols used by IoT devices have weaknesses (Jia et al. 2017). More recently, it has been noted that the improper usage of some protocols, in particular IoT contexts has led to security and safety issues (Fernandes, Rahmati, Jung and Prakash, 2017). For instance, in the context of auto-unlock usage, using the BLE (Bluetooth Low Energy) range as evidence to confirm physical proximity is deemed insecure. Our work involves a comprehensive analysis of various IoT threats and examines the feasibility of porting them to the applied IoT platform.

Recent research on IoT platforms has uncovered several security-critical design problems, such as the SmartThings platform's coarse-grained authorization definition. Fernandes et al. (2016) suggested the FlowFence framework, which provides flow policy constraints for IoT apps, to restrict the use of sensitive data. The security issues with the amplified IoT platforms serve as another driving force behind our work. However, unlike FlowFence, this method is backward compatible and does not call for additional developer work. Moreover, Contex IoT provides user control in situations when a specific data flow may be permitted in one scenario but needs to be restricted in another. A comparison of IoT guards with other IoT systems is presented in Table 2.

Table 3 provides an exploration of the distinctions among several smart home protocols in relation to their power efficiency, advantages, drawbacks, security measures, and applications.

TABLE 2. A comparison of IoT guard with other IoT systems

		Limitations		
System	**Analysis of multiple apps**	**Analyze the trigger-action applet**	**Identification of policy**	**Policy enforcement at runtime**
IoTguard (Celik et al., 2019)	✓	✓	✓	✓
Soteria (Celik et al., 2018)	✓	x	✓	x
ProvThings (Wang et al., 2018)	✓	x	x	x
SmartAuth (Tian et al., 2017)	x	x	x	x
ContexIoT (Jia et al., 2017)	x	x	x	x

Table 3. Comparison between smart home communication protocols

Communication protocol	Security	Use cases	Benefits	Limitations
Z-Wave	AES-128 security	Smart lighting, security, thermostats	Self-repairing network	Limited third-party device support
Wi-Fi	WPA2/WPA encryption	Audio and video streaming, printers	Wide support, extensive coverage, ideal for data-intensive devices	May interact with other frequencies, Wi-Fi devices use more power.
DART	It is a tool that can find unknown threats, also called "zero-day threats."	It is a machine intelligence-based program that is mostly used by the U.S. military to plan and optimise the movement of goods or people and to solve other logistical issues.	By automating evaluation of these processes DART decreases the cost and time required to implement decisions	May miss dangerous code by viewing a certain execution path.
Ethernet	The implementation of a protocol via Ethernet facilitates the establishment of security measures.	Gaming consoles, smart TVs, media streaming devices	The provision of a high bandwidth, rapid, and dependable connection, together with the elimination of the potential for network interference.	A cable connection is required.
Zigbee	The AES-128 standard refers to the Advanced Encryption Standard with a key length of 128 bits.	Smart lights, thermostats, sensors	Compatible with mesh networking, dependable communication	The range is limited.
Bluetooth/BLE	The AES-CCM encryption algorithm is a widely used cryptographic technique that combines the Advanced Encryption Standard (AES) with the Counter with	Intelligent locking mechanisms, sensory devices, luminous bulbs, and intelligent audio devices	Ideal for smart home devices that run on batteries, fast data transfer, and direct contact between devices	Data transfer speeds and coverage regions are limited.
Matter	AES-128 encryption	Smart lights, sensors, and heaters	Makes sure that smart home standards can work with each other.	Needs Certification
Thread	Built-in security	Sensors and smart plugs	Scalable, suited for battery-powered devices	Low device availability

3. METHODOLOGY

Investigation of this study was done through relevant literature, which includes papers, studies, journals, and books. The Alexa AI was employed extensively in the pioneering IoT-based smart home industry. The research conducted by Alexa focuses on developing the necessary framework for incorporating voice assistants into intelligent office environments. The framework aims to assist employees in the daily tasks, such as managing ambient conditions, maintaining attendance records, and generating reports. The utilization of an interactive speech interface enables Alexa to provide users with a hands-

free method of engaging ability. Individuals have the ability to utilize their vocal capabilities to carry out routine activities like accessing current events, engaging in auditory experiences, and participating in recreational activities. In addition to manual input methods, individuals have the capability to employ their vocal commands for the purpose of managing cloud-connected gadgets. Most of Alexa's skills include the utilisation of HTTP requests to facilitate communication between distinct microservices. In addition to being compatible with a wide range of smart home gadgets, Amazon's Alexa AI also function with a wide range of Amazon Echo devices. As a language for AI, the Dynamic Analysis and Preplanning Tool (DART) was chosen. Nevertheless, within the realm of Alexa's abilities, it is plausible for hackers to potentially acquire access to this data via security breaches, so exposing users to the peril of identity theft and various other manifestations of cybercrime. Another concern pertains to the perpetual listening functionality of Alexa, is the potential to surreptitiously record conversations and other auditory content without the explicit knowledge or agreement of the user. This study addresses the security breaches of Amazon Alexa Automation Assistant. The architecture of the proposed system is described as follow;

3.1. Architecture of the Proposed System

The architecture consists of the user/agent, devices, a shared network, and a common platform, which in this case is the Amazon Alexa Digital Assistant AI. For this project, we enforce a uniform protocol for all the associated devices to use when communicating.
The IoT is the network of interconnected computing devices that can exchange data and coordinate automated tasks without human intervention. Connectivity between these devices depends on electronics, software, a network, and sensors.

- **The user/agent**: software that acts on behalf of a user to retrieve and display web material and to enable the user to interact with that content.
- **Device**: hardware devices that include sensors, actuators, appliances, etc. that are programmed for certain applications and can transmit data over the internet.
- **Network**: a collection of interconnected devices that communicate with other devices, e.g. smart appliances.
- **Platform**: software (mobile application) with multiple layers that allows for the direct management and automation of linked objects in the IoT universe.

The structure of the Internet-of-Things communication network platform is shown in Fig. 3.

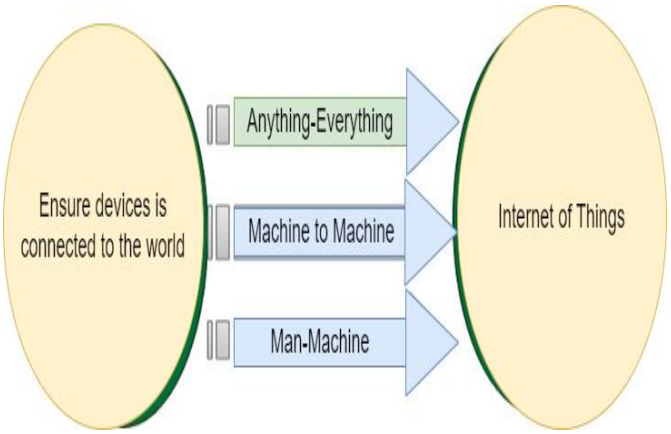

Fig. 3. Structure of the internet-of-things communications protocols

Communication protocols can be utilised in the development of smart home systems to design a smart home device that will be appreciated by end users such as Z-Wave, Wi-Fi, DART, Ethernet, Zigbee, Bluetooth/BLE, Matter, and Thread.

3.2. System Architecture

The architecture of the proposed system. It depicts the activities performed by the user, devices, and some other nodes on the system. It starts by setting a user preference. Commands are then sent. An indication on whether the command sent is switched ON or OFF the home appliances was done, and also if the command sent is from unauthorized access, the user or agent is then notified in order to take necessary action. Communication protocols must be chosen in order to construct a smart house. Today, the Zigbee and Z-Wave standards are widely utilized. The range of coverage differs between the two, with the Zigbee having a 10-meter range and the Z-Wave's30-meter range. The z-wave wireless communication protocol was adopted in this study. Z-wave and the Wireless Fidelity (Wi-Fi) communication standard are the communication protocols employed in this research; it was chosen because of the large range of devices it supports. System Process Architecture is presented in Fig. 4.

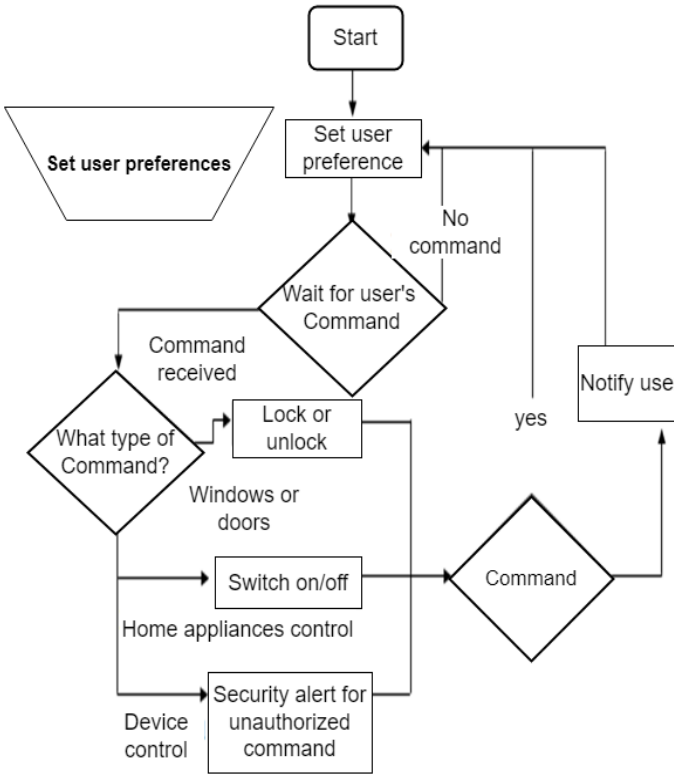

Fig. 4. System process architecture

The proposed system has two operating modes for mobile applications: In admin mode, the user will be able to draw his or her entire home prototype using a simple drag-and-drop interface. Each device is given a Raspberry Pi pin number, which controls how electronic devices work on the backend. Though the user may not be able to see the entire prototype of the home, the admin can control the operation of each appliance based on pin configuration. Figure 5 shows a nice and interactive GUI-based interface with attractive icons that lets the user easily understand how it works.

Icons changing are used to inform the user of an electronic device's current state, with a touch active button to change state. There is also an intensity bar that allows the user to customize the fan speed and light brightness. The status of devices is displayed with the active state of working and the passive state. The proposed system is also capable of making decisions on the functionality of each home device such as switch-off of a system when there is an unusual rise in temperature.

The state of each sensor, as well as current values, is displayed in the second tab of the main screen. Sensor values are updated using backend services that refresh themselves every 30 seconds. It can also prompt alert if there is a security breach. The next section is the presentation of result.

4. RESULT ANALYSIS

This study focuses on the design and development of a mobile application for an intelligent smart home system operating on the principles of the Internet of Things. The system was evaluated with various home appliances such as smart TVs, microwaves, and air conditioners, and their response times were recorded at different distance intervals. The sitting room contains several pieces of furniture and smart devices, including a television and an air conditioning unit, which can be operated through a mobile application installed on a smartphone. The smart home control panel serves as a centralized interface for managing various smart devices within the home. This panel encompasses features such as accessibility, functionality, and command execution. It allows users to control individual items within the smart home, such as lights, air conditioners, microwaves, smart TVs, and other similar devices. Activation of the control panel is achieved by pressing the control button on the mobile application. The project incorporates electronic components with precise specifics and specifications, as presented in Table 4.

Table 4. System Components and Specification

Devices	Specifications
Smartphone, wireless	Compatible with Android
Relay Pack Circuit	The 8-relay, 5V-capable, circuit board
Pi 2B Raspberry	Operational voltage 7-12 V, 40 GPIO pins, 1 GB RAM, 900 MHz quad-core ARM Cortex-A7 CPU
Motor L293D control panel	Output current: 600 mA/channel; supply-voltage range: 4.5-36 V
DS18B20 digital sensor temperature	Range of temperature from 55 to 125 degrees Celsius (67 to +257 degrees Fahrenheit).
The LM393 is a device that possesses the ability to quantify intensities of light.	Switching digital (0 and 1) outputs for the outside world 3.3 V-5 V

The MQ2 smoke detector	flammable gases and smoke

The temperature regulation command codes control the activity of temperature regulation in the mobile application. These codes are responsible for the overall control of the house's temperature. The variance and time taken for the smart TV to respond to commands from the mobile app at various distance intervals are presented in Table 5.

Table 5. TV variance/changes with time

S/N	TV Distance in meter	Response Time in second
1	2	1.17
2	4	2.12
3	6	2.68
4	8	3.86
5	10	4.11
6	20	6.48
7	40	8.26
8	50	8.31
9	100	8.51
10	200	8.51

Table 5 depicts the variations and changes in the time taken (in seconds) for the smart devices to respond to commands from the smartphone controlling the smart home at various distance intervals (in meters). The parameters in Table 4 support the research by determining the time taken for devices such as smart TVs to respond to commands from the mobile app at different distance intervals. These parameters also validate the research in terms of measuring the response time of the TV at various distances, helping to determine the effectiveness and efficiency of the proposed system. Additionally, they show how the distance of the mobile control affects the response time of the smart TV, providing further insight into this relationship.

The graphical representation of the variance and time taken for the smart TV to respond to commands from the smartphone controlling the smart home is shown in Fig. 5.

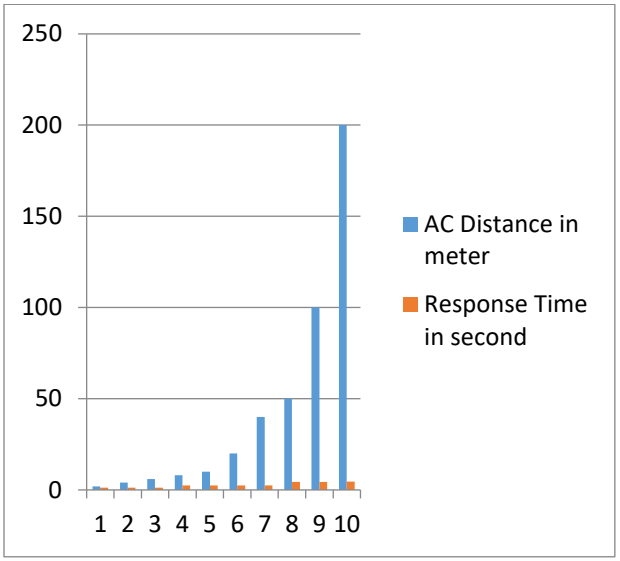

Fig. 5. Home TV distance against response time

As the distance (in meters) of the device increases, there is also an increase in the time taken for the TV to respond. This graph shows the time delay (in seconds) at different distances for the smart TV to respond when turned ON or OFF from the mobile application on the smartphone. Variations in the time taken for the smart AC to respond to commands from the mobile app at various distance intervals are presented in Table 6.

Table 6. AC variance/changes with time

S/N	AC distance (in meters) from the control mobile application	Response time in the second
1	2	1.2
2	4	1.2
3	6	1.2
4	8	2.41
5	10	2.42
6	21	2.43
7	40	2.44
8	50	4.31
9	100	4.31
10	200	4.51

Table 6 shows the variations and changes in the time taken (in seconds) for smart devices to respond to commands from the smartphone controlling the smart home at various distance intervals (in meters). The parameters in Table 5 support the research by determining the time taken for devices such as smart ACs to respond to commands from the mobile app at

different distance intervals. These parameters also validate the research in terms of measuring the response time of the AC at various distances, helping to determine the effectiveness and efficiency of the proposed system. Additionally, they show how the distance of the mobile control affects the response time of the smart AC.

The parameters further explain how the distance of the mobile control affects the response time of the smart AC. Command distances within 2 to 6 meters have a significant impact on the response time, while distances beyond 6 meters have little effect. The graph shows the time delay (in seconds) at different distances for the smart AC to respond when turned ON or OFF from the mobile application on the smartphone. The graph of smart home AC distance in meters versus response time is shown in Fig.6

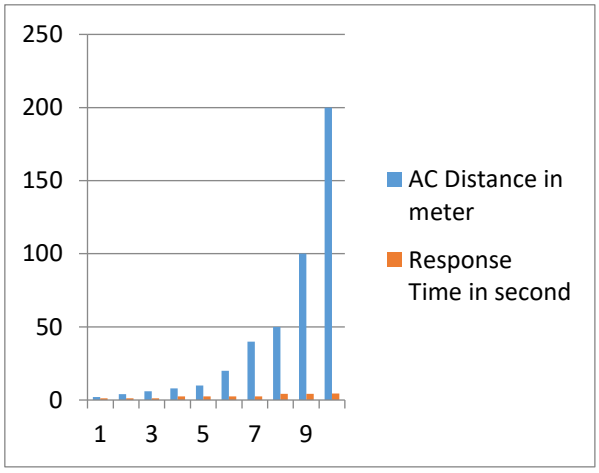

Fig. 6. Smart home AC distance against time

4.1 Comparison of the proposed model with SOTA baseline

Comparison of the proposed model with state-of-the-art (SOTA) baseline models using smart TV and AC distance and time parameters and machine learning models such as the SVM model. The result shows that the proposed new model performs better than SOTA baseline models as presented in Table 7.

Table 7. Comparison of the proposed model with sota baseline models using smart tv and ac distance and time parameters and machine learning (svm) methods

Approach	MSE	RMSE	MAE	MAPE
SVM	-	0.36	-	-
SVM	-	1.25	1.12	-
SVM	-	-	-	0.89
Deep learning	0.35	0.59	0.33	-
Deep learning	0.38	-	0.39	-
Deep learning	-	0.74	-	-
Deep learning	0.29	0.54	0.39	-
Proposed smart system	0.21	0.34	0.31	0.75

In Table 7, the authors indicated the error rate of the state-of-the-art (SOTA) baseline approaches by times, mostly owing to its remarkable ability to achieve exceptional performance across several domains. Therefore, within this field, deep learning has demonstrated better results, as evidenced in the Table 7.

zemploying commonly used assessment metrics. The presence of hyphens (-) in the table signifies missing values, indicating that the writers did not utilise that particular metric. Deep learning has emerged as a prominent and prevailing approach in contemporary

Recent advancements in deep learning techniques have demonstrated improved outcomes. However, these approaches exhibit a deficiency in adequately capturing crucial information pertaining to the modelling of SMART devices parameters. Consequently, the performance of these models is rather suboptimal. During the literature review, this study acknowledged this constraint and have developed a machine learning (ML) model such as Support Vector Machine (SVM) that comprehensively addresses many aspects of security breaches. This model facilitates the modelling of SMART devices parameters and the identification of spatial and spatiotemporal cues with ease. The motivation behind the design of the ML framework is the impressive performance of deep learning in forecasting time-series problems. Therefore, we present a new methodology, which yields superior results compared to existing baseline methods. The novel model has enhanced smart home automation systems in the domains of security, dependability, and intelligence by rigors experimentation. Hence, the present study successfully demonstrated a decrease in response time for devices situated at varying distance intervals, thereby suggesting an enhancement in operational effectiveness.

4.2 DISCUSSION

This paper employed Z-wave, WiFi and explore the software development process of DART in the IoT to promote security for remote control of automatic smart home system. The system was evaluated with different smart device and time taken for each device to respond to the command from the mobile app at distance interval was recorded. The distance of the smart devices from the mobile app that controls it was measured in meters (2m, 4m, 6m, 8m, and 10m, 20m, 40, 50, 100m, 200m). At 2m it takes smart TV 1.17sec to respond, at 4m it takes 2.12sec, at 6m it increasing by 0.01sec and continue till it reached 100m. The result shows that AC response time is independent of its distance from the mobile command application within 2 to 6 meters while TV response time increases as the distance of the command application increases. The result indicates that the best time effective response of TV is 1.17 seconds at 2-meter distance while that of AC is 1.2 seconds between 2 to 6 meters' distance intervals from the device.

Two levels security was also used to ensure the system is well secure through the authentication of authorized users from the mobile application using password, and security alert for every attempt to access or control the smarts devices. The study achieved the implementation of the smart home mobile control, and ensure the smart home is well protected from unauthorized access.

takes 2.68sec, at 10m it takes 4.11while it takes 8.50sec to respond at 200m distance intervals. The smart TV response time keeps increasing as it distances from the application that controls it increases.

Meanwhile, the air conditioner maintains a fixed response time at distance intervals, from 2m to 6m its response time is 1.2sec, it changes at 8m and increases by 1.4sec which makes the response time at 8m to 2.41, it also maintains the response time until 20m when the time increase by 0.01, it keeps

To justify the used of the proposed communication security protocols, experimental result revealed that the proposed Z-wave, Wi-Fi protocols and DART offers superior dependability, low radio rebirth, simple operation,
and straightforward interoperability compared to the standard and popularly adopted protocols such as ZigBee, home plug and INSTEON protocol. It is also made sure that the hardware and technology employed in the concept may be replicated for little cost.

Take for instance, Z-Wave is a wireless technology that offers dependable and secure communication between devices by operatsing in the sub-GHz frequency range, which is less than 1 GHz. By functioning as nodes in a mesh network, Z-Wave devices expand network coverage and keep connections intact in the event that a node fails. In order to guarantee that only authorised devices can join the network, its security analysis includes Z-Wave's capacity to function on AES-128 encryption

and provide two-way authentication between devices. Z-Wave uses over-the-air' (OTA) updates to guarantee continuous security.

5. CONCLUSIONS

This work implemented a mobile application of intelligent smart home automation based on IoT. Physical objects (things) such as Smart TV, Fan, Air conditioner, light-emitting diode (LED) bulbs, Smart Fridge, Microwave, Oven, etc., were embedded with sensors and actuators for the purpose of connecting and exchanging data with devices over the internet. These devices were connected through Z-wave and Wi-Fi communication protocols. While we explore the concept of developmental process of DART. The new model improved smart home automation systems in terms of security, reliability, and intelligence through testing. A mobile Android app was developed for smart home automation control, allowing users to manage sensor-equipped devices via a smartphone's control panel. The process involves pressing the "ON" button to activate and deactivate the chosen device. Response times at various distances were examined, with some devices responding consistently and others experiencing increased delays with greater distance. Smart homes, empowered by AI software, provide significant value but also raise security concerns. Performance evaluation employed metrics such as MAPE, MAE, RMSE, and VAPE, revealed that protocols like Z-wave, Wi-Fi, and DART offer reliability and compatibility advantages over ZigBee, home plug, and INSTEON. The study also emphasized cost-effective hardware and technology duplication.

Future research should prioritize exploring IoT security and privacy issues, as well as improvements in network and data security. Maintaining data security is crucial in designing future smart home systems and investigating the impact of factors like frequency and temperature on smart device response times remains a valuable area to examined.

Compliance with ethical standards

Competing interest: The authors declare that there is no competing interest required in this article.
Data Availability: This manuscript has no open data availability and has used open-source data obtained online.

ACKNOWLEDGEMENT
This work was performed in part using computing facilities at the University of Abuja, Nigeria which were provided by the Department of Computer Science, University of Abuja, and Tertiary Education Trust Fund (TETFund).

Authors Contributions

The authors confirm their contribution to the paper as follows:
Study conception and design: Tawakalitu Afoluwaso Giwa,
Data collection: Tawakalitu Afoluwaso Giwa, Oludare Isaac Abiodun, Benedict
Analysis and interpretation of results: Tawakalitu Afoluwaso Giwa, Omolara, Usman, and Olawale.
Draft manuscript preparation: Tawakalitu Afoluwaso Giwa.
All authors reviewed the results and approved the final version of the manuscript.

REFERENCES

Abiodun, O. I., Abiodun, E. O., Alawida, M., Alkhawaldeh, R. S., & Arshad, H. (2021). A review on the security of the internet of things: challenges and solutions. *Wireless Personal Communications*, *119*, 2603-2637.

Ahmad, T., Morelli, U., Ranise, S., & Zannone, N. (2022). Extending access control in AWS IoT through event-driven functions: an experimental evaluation using a smart lock system. *International Journal of Information Security*, *21*(2), 379-408.

Al-Boghdady, A., Wassif, K., & El-Ramly, M. (2021). The presence, trends, and causes of security vulnerabilities in operating systems of IoT's low-end devices. *Sensors*, *21*(7), 2329.

Bai, X., Xing, L., Zhang, N., Wang, X., Liao, X., Li, T., & Hu, S. M. (2016, May). Staying secure and unprepared: Understanding and mitigating the security risks of Apple ZeroConf. In *2016 IEEE Symposium on Security and Privacy (SP)* (pp. 655-674). IEEE.

Bardram, J. E., & Christensen, H. B. (2007). Pervasive computing support for hospitals: An overview of the activity-based computing project. *IEEE Pervasive Computing*, *6*(1), 44-51.

Baykara, M., & Çolak, E. (2018, March). A review of cloned mobile malware applications for android devices. In *2018 6th international symposium on digital forensic and security (ISDFS)* (pp. 1-5). IEEE.

Bosamia, M. (2013). Positive and negative impacts of information and communication technology in our everyday life. Dostupno na: https://www. Research gate. net/publication/325570282_Positive_and_Negative_Imp acts_of_Information_and_Communication_Technology_in_our_Everyday_Life [30. kolovoza 2021.].

Calderoni, L. (2019, August). Preserving context security in AWS IoT Core. In *Proceedings of the 14th International Conference on Availability, Reliability and Security* (pp. 1-5).

Celik, Z. B., McDaniel, P., & Tan, G. (2018). Soteria: Automated {IoT} safety and security analysis. In *2018 USENIX annual technical conference (USENIX ATC 18)* (pp. 147-158).

Celik, Z. B., Tan, G., & McDaniel, P. D. (2019, February). IoTGuard: Dynamic enforcement of security and safety policy in commodity IoT. In *NDSS*.

Chen, S., Xu, H., Liu, D., Hu, B., & Wang, H. (2014). A vision of IoT: Applications, challenges, and opportunities with China perspective. *IEEE Internet of Things Journal*, *1*(4), 349-359.

Cretu, A. M., Rusu, M., & de Montjoye, Y. A. (2024). Re-pseudonymization Strategies for Smart Meter Data Are Not Robust to Deep Learning Profiling Attacks. *arXiv preprint arXiv:2404.03948*.

Fernandes, E., Paupore, J., Rahmati, A., Simionato, D., Conti, M., & Prakash, A. (2016). FlowFence: Practical data protection for emerging IoT application frameworks. In *25th USENIX Security Symposium (USENIX Security 16)* (pp. 531-548).

Fernandes, E., Rahmati, A., Jung, J., & Prakash, A. (2017). Security implications of permission models in smart-home application frameworks. *IEEE Security & Privacy*, *15*(2), 24-30.

Francillon, A., Danev, B., & Capkun, S. (2011). Relay attacks on passive keyless entry and start systems in modern cars. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*. Eidgenössische Technische Hochschule Zürich, Department of Computer Science.

Ghayvat, H., Liu, J., Babu, A., Alahi, E. E., Gui, X., & Mukhopadhyay, S. C. (2015). Internet of Things for smart homes and buildings: Opportunities and Challenges. *Journal of Telecommunications and the Digital Economy*, *3*(4), 33-47.

Ho, G., Leung, D., Mishra, P., Hosseini, A., Song, D., & Wagner, D. (2016, May). Smart locks: Lessons for securing commodity internet of things devices. In *Proceedings of the 11th ACM on Asia conference on computer and communications security* (pp. 461-472).

Javaid, U., & Sikdar, B. (2021, January). A lightweight and secure energy trading framework for electric vehicles. In *2021 International Conference on Sustainable Energy and Future Electric Transportation (SEFET)* (pp. 1-6). IEEE.

Javeed, D., Gao, T., & Khan, M. T. (2021). SDN-enabled hybrid DL-driven framework for the detection of emerging cyber threats in IoT. *Electronics*, *10*(8), 918.

Jia, Y. J., Chen, Q. A., Wang, S., Rahmati, A., Fernandes, E., Mao, Z. M., & University, S. J. (2017, February). ContexIoT: Towards providing contextual integrity to appified IoT platforms. In *ndss* (Vol. 2, No. 2, pp. 2-2).

Jerkins, J. A., & Stupiansky, J. (2018, March). Mitigating IoT insecurity with inoculation epidemics. In *Proceedings of the ACMSE 2018 Conference* (pp. 1-6).

Kashaf, A., Sekar, V., & Agarwal, Y. (2022, May). Protecting smart homes from unintended application actions. In *2022 ACM/IEEE 13th International Conference on Cyber-Physical Systems (ICCPS)* (pp. 270-281). IEEE.

Mathew, S., & Varia, J. (2014). Overview of Amazon web services. *Amazon Whitepapers*, *105*(1), 22.

Mouha, R. A. (2021). Internet of things (IoT). *Journal of Data Analysis and Information Processing*, *9*(2), 77-101.

Oliveira, L. B., Pereira, F. M. Q., Misoczki, R., Aranha, D. F., Borges, F., Nogueira, M., ... & Liu, J. (2018). The computer for the 21st century: present security & privacy challenges. *Journal of Internet Services and Applications*, *9*, 1-25.

Omolara, A. E., Alabdulatif, A., Abiodun, O. I., Alawida, M., Alabdulatif, A., & Arshad, H. (2022). The internet of things security: A survey encompassing unexplored areas and new insights. *Computers & Security*, *112*, 102494.

Pa, Y. M. P., Suzuki, S., Yoshioka, K., Matsumoto, T., Kasama, T., & Rossow, C. (2015). IoTPOT: analyzing the rise of IoT compromises. In *9th USENIX Workshop on Offensive Technologies (WOOT 15)*.

Phung, K. A., Kirbas, C., Dereci, L., & Nguyen, T. V. (2022). Pervasive healthcare Internet of Things: a survey. *Information*, *13*(8), 360.

Ronen, E., & Shamir, A. (2016, March). Extended functionality attacks on IoT devices: The case of smart lights. In *2016 IEEE European Symposium on Security and Privacy (EuroS&P)* (pp. 3-12). IEEE.

Sood, A. K., & Enbody, R. J. (2012). Targeted cyberattacks: a superset of advanced persistent threats. *IEEE Security & Privacy*, *11*(1), 54-61.

Stolojescu-Crisan, C., Crisan, C., & Butunoi, B. P. (2021). An IoT-based smart home automation system. *Sensors*, *21*(11), 3784.

Talos, C. (2024). Vulnerability Spotlight: Multiple Vulnerabilities in Samsung SmartThings Hub These vulnerabilities were discovered by Claudio Bozzato of Cisco Talos–Global Security Mag Online.

Taiwo, O., Ezugwu, A. E., Rana, N., & Abdulhamid, S. I. M. (2020). Smart home automation system using ZigBee, Bluetooth and Arduino technologies. In *Computational Science and Its Applications–ICCSA 2020: 20th International Conference, Cagliari, Italy, July 1–4, 2020, Proceedings, Part VI 20* (pp. 587-597). Springer International Publishing.

Tian, Y., Zhang, N., Lin, Y. H., Wang, X., Ur, B., Guo, X., & Tague, P. (2017). SmartAuth: User-centered authorization for the Internet of Things. In *26th USENIX Security Symposium (USENIX Security 17)* (pp. 361-378).

Xiao, Y., Jia, Y., Liu, C., Alrawais, A., Rekik, M., & Shan, Z. (2020). HomeShield: A credential-less authentication framework for smart home systems. *IEEE Internet of Things Journal*, *7*(9), 7903-7918.

Yassein, M. B., Mardini, W., & Khalil, A. (2016, September). Smart homes automation using Z-wave protocol. In *2016 International Conference on Engineering & MIS (ICEMIS)* (pp. 1-6). IEEE.

Yu, M., Zhuge, J., Cao, M., Shi, Z., & Jiang, L. (2020). A survey of security vulnerability analysis, discovery, detection, and mitigation on IoT devices. *Future Internet*, *12*(2), 27.

Yu, T., Sekar, V., Seshan, S., Agarwal, Y., & Xu, C. (2015, November). Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the internet-of-things. In *Proceedings of the 14th ACM workshop on hot topics in networks* (pp. 1-7).