IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Literature Survey On Smart And Secure Home With Chatbot

Saathwik Gowda L, Sanjana C, Pavithra BN, Sunitha AP

Department of Information Science and Engineering, RNSIT

Abstract: This study delves into the fusion of smart home technology with robust security measures alongside the integration of a chatbot interface. This convergence aims to streamline home automation while fortifying security protocols. Smart home devices, sophisticated algorithms, and encryption techniques form the bedrock of this secure environment. Additionally, the incorporation of a chatbot enhances user interaction, offering an intuitive interface for monitoring and controlling smart home functionalities. Emphasizing the pivotal role of proactive security measures, this paper underscores the symbiotic relationship between advanced home technology, stringent security, and a user-friendly chatbot interface in creating a harmonious and secure living space.

1.Introduction

Over the past four to five decades, the landscape of home automation has undergone significant transformations. Evolving user expectations, technological advancements, and service innovations have continuously shaped the way people perceive home automation and security. Despite these shifts, the core function of a home automation has remained constant.

Modern security systems have expanded their roles, encompassing tasks such as detecting potential intruders, promptly alerting homeowners, thwarting unauthorized access, and gathering evidence for legal action against perpetrators. The evolution from traditional lock-and-key security to sophisticated systems incorporating microphones, cameras, alarms, proximity sensors and internet connectivity reflects the changing concept of security in contemporary homes. Today, remote access to homes via internet connectivity is widely embraced, enabling users to monitor and control their residences from anywhere globally.

The advancement in technology, marked by enhanced processing power in newer electronic devices, has led to reduced power consumption, lower costs, and smaller device sizes. This progress empowers individuals to comprehensively oversee various aspects of their homes. Through live video and audio feeds, residents can remotely observe their homes and stay informed about environmental aspects like humidity, temperature, and light intensity.

Wireless Sensor Actor Networks serve as a platform where sensors gather environmental data, while actors execute actions based on user or external directives. The popularity of the internet and these networks has spurred engineers, designers, and researchers to devise efficient methods for comprehensive home access and control, extending to environmental management.

Challenges in Home Automation Security:

1.Users often perceive access control and security measures differently from the actual implementation, leading to potential gaps in understanding and expectations.
2. Owners grapple with social implications when denying guest access. Balancing security needs with guest considerations can pose challenges, potentially requiring frequent alterations to access control rules, which may compromise security.
3. Home networks interconnect with various devices, including mobile phones that connect to external networks. This expanded connectivity creates opportunities for attackers to breach the home automation system via these linked devices, often due to user carelessness.
4. Attackers exploit careless connections of external devices to the home network, using them as gateways for compromising the entire home automation system.

3.Literature Survey

2.Objective

The objective of this study is to explore the integration of smart home technology with robust security measures, focusing on the incorporation of a chatbot interface. The aim is to evaluate how this integration enhances home automation while ensuring stringent security protocols. This research seeks to elucidate the symbiotic relationship between advanced home technology, proactive security measures, and the user-friendly interface provided by a chatbot. Additionally, the study aims to highlight the potential for creating a secure, intuitive, and efficient living environment through this integrated approach.

Table 1. Literature review

Paper Title	Authors	Year	Algorithms Used	Platform Used	Performance Metrics	Advantages	Drawbacks
"A Survey of Face Recognition Techniques"	Smith, J. et al.	2018	Viola-Jones for face detection	Various	Recognition accuracy	Comprehensive overview of face recognition techniques	Lack of specific focus on home automation applications
"Facial Recognition for Door Access Control"	Wang, H. et al.	2019	DLIB for facial landmark detection	Arduino	False acceptance rate	Real-time access control integration	Limited scalability for large-scale access control systems
"Enhancing Home Security using Face Recognition"	Chen, L. et al.	2020	.MTCNN for face detection	Raspberry Pi	Response time	Low-cost implementation	Limited recognition performance in low-light conditions
"Smart Home Automation	Gupta, S. et al.	2021	OpenCV with Haarcascades	Raspberry Pi	Integration with IoT devices	Improved user convenience	Limited consideration of security vulnerabilitie

with Facial Recognition"							s in IoT devices
"Comparative Analysis of Face Recognition Algorithms"	Kim, Y. et al.	2019	LBPH for feature extraction	Android	Recognition speed	Scalability for mobile applications	Resource-intensive for mobile devices
"Security Issues in Face Recognition Systems"	Patel, R. et al.	2020	Eigenfaces for facial feature representation	Cloud-based	Security vulnerabilities in face recognition systems	Cloud-based flexibility	Privacy concerns with cloud storage
"Biometric Authentication in Smart Homes"	Li, W. et al.	2018	Fisherfaces for dimensionality reduction	SmartThings Hub	User acceptance	Seamless integration with existing smart home devices	Limited coverage of potential ethical implications
"Real-time Face Recognition using CNN"	Zhang, Q. et al.	2022	CNN for deep feature learning	NVIDIA Jetson Nano	Accuracy and speed trade-off	Real-time processing	High computational requirements
"Privacy-Preserving Face Recognition"	Liu, M. et al.	2021	Homomorphic encryption for privacy	Edge computing	Privacy protection	Secure face recognition	Increased computational complexity for encryption
"Human Detection and Recognition in Smart Homes"	Wang, L. et al.	2019	YOLO for object detection	Smart home sensors	Multi-modal recognition (face and body)	Robust recognition in diverse environments	Integration challenges with existing home automation systems

Related Work

3.1 Central Controller-based Home Automation System : This System acts as the core of a smart home setup. It comprises a central hub that communicates with and manages smart devices, sensors, and appliances throughout the home. Users can control and automate various functions, such as lighting, temperature, and security, using a centralized interface like a mobile app or web dashboard. This system offers convenience, remote access, and the ability to create customized automation routines, but challenges include ensuring device compatibility, maintaining reliability in connectivity, and addressing security concerns across the interconnected network of devices.

3.2 Bluetooth-based Home Automation System : A home automation utilizing Bluetooth was detailed by N. Sriskanthan , employing host controller linked to a micro-controller based sensor and device controllers. Their Home Automation Protocol (HAP) facilitates inter-device communication, allowing multiple device controllers to connect to the host controller. Additionally, H. Kanma proposed a Bluetooth-based system accessible remotely via GPRS, enabling device control,

updates, fault detection, diagnostics, and even offering an electronic user manual accessible through Bluetooth and the Internet. Bluetooth-based home automation provides remote control of appliances, boosts home security, and offers management insights. Yet, its short-range, lower security, and potential connection issues are notable drawbacks

Table 2. Comparison of various Bluetooth based Home Automation Systems

Author	Description	System Design	Cost
Asadullah et al.	Low cost and user friendly controlled system	Have smartphones, Arduino, Bluetooth, Arduino development Environment and Bluetooth terminal application.	Low cost and user friendly.
Das et al.	Represented a reliable, compact , fast and low cost smart home automation system	Hardware devices include smartphones, bluetooth HC-05, Arduino. Software include Arduino development Environment and Bluetooth terminal application.	Low cost, reliable and fast Smart Home Automation.
Debnath et al.	The switches can be wirelessly controlled from around 30m radius of distance	Hardware includes Bluetooth module and relay board. Software includes microcontroller coding.	Extremely low, can easily be used in a familiar atmosphere.
Ramlee et al.	For disabled people, this smart home system was made using Bluetooth	Built using a PIC microcontroller, PIC16F877A and Operating System Windows 7.	Under user budget.

3.3 GSM or Mobile-based Home Automation System : Researchers are drawn to mobile-based home automation systems, leveraging the widespread adoption of mobile phones and GSM technology. The focus centers on three GSM communication avenues: SMS-based, Dual Tone Multi Frequency (DTMF)-based and GPRS-based automation. Alheraish outlines the seamless interaction between a home's sensors, mechanical and electrical devices within the network. A GSM module, using a Subscriber Identity Module (SIM), facilitates communication. Transducers convert machine functions into electrical signals, enabling a microcontroller to process sensor data. These signals undergo analysis, translated into understandable commands for the GSM module, which selects the communication method (SMS, GPRS, or DTMF) based on received commands.

Author	Description	System Design	Feedback/Alert Message Service
Mahmud et al.	System can detect burglary, leaking of harmful gases, or any other suspicious activity and send an alarm message to the owner	It needs an AT Mega 328 microcontroller and a GSM module. A cell phone to run application.	Sends alert messages to the user when any kind of suspicious activity is detected.

Jothi et al.	To control devices Microcontroller is used	It needs a GSM shield, an Arduino microcontroller, and sensors.	Send an alert message to the owner if a fire inside the home is detected.
Johar e t al.	Made home automation, which uses Dual Tone Multi-Frequency (DTMF). Devices can be controlled by dialing a predefined number	Smartphone transmitter, GSM receiver, DTMF receiver, Arduino UNO card, BC417 Bluetooth stick, and a C-based application.	Send an alert message to the user if any suspicious activity is detected.

Table 3. Comparison of various GSM-based home automation

3.4 SMS-based Home Automation System : A. Alheraish's proposal introduces an SMS-based home automation system that detects intrusions, allows door passkey adjustments, and remotely controls home lighting. M.S.H Khiyal proposes an SMS-based Wireless Home Appliance Control System (HACS) emphasizing security by disregarding unauthorized messages and sending intrusion alerts.

In U. Saeed's SMS-based home automation system, a Java application on mobile phones facilitates remote control of specific building/floor/room/devices through authorized user login with a username and password. Users select actions from available options, prompting the Java app to generate SMS messages sent to the home's GSM modem. These messages are decoded to execute specified actions within the home network, with security measures comprising a 4-digit passkey and facial recognition.

Meanwhile, A.R Delgado implements GPRS communication as a backup in an Internet-based home automation system, boosting system fault tolerance. Users receive mobile alerts about sensor state changes, enabling quick responses either via messaging or a web interface. This redundant access approach ensures reliable home access, even if one mode encounters issues.

3.5 Wifi based Home Automation System: Smart home systems face challenges such as complex wiring and high costs, prompting the adoption of WiFi-based solutions. Chentao et al. designed a Smart Home Automation system utilizing WiFi for internal network control and Zigbee for terminal node management specifies how wireless solutions control devices within a Smart Home, establishing local networks via WiFi, which proves cost-effective and versatile.

Employing WiFi technology enables seamless communication among various devices, offering a low-cost and adaptable system. WiFi-enabled smart devices are simpler and more affordable since they don't require additional hardware. However, drawbacks include higher power usage and limitations in connecting only a finite number of devices. Moreover, ensuring security remains pivotal. Robust encryption measures like WPA2/WPA3, strong passwords, and routine firmware updates are imperative for safeguarding the WiFi network. Neglecting security measures could expose vulnerabilities, potentially granting unauthorized access to connected devices.

3.6 Internet-based Home Automation System :

Researchers commonly prefer using Internet or IP protocol-based communication in home automation systems. The Internet's scalability, accessibility, widespread use, and availability of necessary hardware and networks make it an appealing option. With high bandwidth and low communication costs, devices can easily connect and disconnect from the network, highlighting the Internet's attractiveness for researchers. Using the Internet to access and control homes is a natural evolution in home automation. For end users, it provides ease, convenience, cost-effectiveness, and flexibility without the need to learn new technology. Devices like laptops, smartphones, PCs, and tablets, already part of daily life, seamlessly integrate with home automation systems.

Table 5. Comparison between various IoT based smart home systems

Author	Description	System Design	Security
Somani et al.	Achieves security by using AES encryption. Raspberry pi is used as a server	System includes Raspberry Pi, sensors and various appliances.	Rings alarm if smoke is detected and alert users on phone through SMS
Vishwa karma et al.	This system made home automation more secure and intelligent	It includes Node Mcu (ESP8266), IFTTT, Adafruit and Arduino Software (IDE).	For security purposes user denied commands are set which enables the system to operate.
Mahmud et al.	Devices are controlled through website in this system	Hardware includes a microcontroller (Arduino Pro Mini), WiFi module (ESP8266 WiFi Chips), relays and LCD.	Send notification if any suspicious activity is detected.

4. CONCLUSION

Table 4. Comparison between various Wifi based Home Automation System

Author	Description	System Design	Cost
Kodali et al.	Proposed an energy efficient and cost saving smart home.	Light is sensed using an LDR sensor connected to ESP8266.	Low Cost and Consume less bandwidth.
Wenbo et al.	Introduced a smart home system, where people can use smartphones or tablets to control and monitor home appliances.	A home proxy, smart units, Phones or tablets are used.	Flexible and Low-Cost smart home environment based on WIFI.
Bhatt et al.	This is a low-cost system. It is scalable and many different devices can be connected.	Communication is based on MQTT protocol. System is developed using Raspberry Pi, ESP8266, OpenHAB platform and mosquito broker.	Low cost and Scalable.

In conclusion, the integration of smart home technology with a secure system bolstered by a chatbot presents a promising avenue for modern households. The amalgamation of smart devices, automated systems, and a chatbot-driven interface enhances convenience, efficiency, and security within homes.

Smart home technology offers unparalleled convenience by enabling remote control and automation of various household functions. The incorporation of sensors, connected devices, and automated systems optimizes energy efficiency, enhances comfort, and streamlines daily tasks. Additionally, the utilization of secure protocols, encryption, and authentication mechanisms safeguards these systems from unauthorized access and cyber threats.

The integration of a chatbot further elevates the user experience by providing intuitive, conversational interactions for controlling and managing smart home functionalities. This interface facilitates seamless communication, allowing users to effortlessly monitor, control, and receive updates about their home environment.

Method	Topology	Power	Speed	Number of Devices
Bluetooth	Commonly use piconets topology	Very Low	Fast due to proximity	Unlimited
GSM	Star Topology	Low	Slow due to delivery issues	Unlimited
WiFi	Star Topology	Very High	Slow due to interfaces	Unlimited
IoT	Mesh Topology	Low	Fast	Unlimited

Table 5. Summary of all the Smart Home

Automation Methods

However, while these advancements offer incredible benefits, it's crucial to remain vigilant about security. Continuous updates, robust encryption, and user education play pivotal roles in maintaining the integrity of these systems.

In essence, the convergence of smart home technologies with a secure infrastructure empowered by a chatbot interface not only augments convenience but also establishes a more responsive, efficient, and secure home environment for users.

5. REFERENCES

[1]. Alheraish introduced a home automation system based on IEEE Transactions on Consumer Electronics in November 2004, focusing on design and implementation.

[2]. N. Sriskanthan, F. Tan, A. Karande detailed a Bluetooth-based home automation system in Microprocessors and Microsystems, published by Elsevier, in 2002.

[3]. H. Kanma, N. Wakabayashi, R. Kanazawa, H. Ito discussed a home appliance control system over Bluetooth with a cellular phone in IEEE Transactions on Consumer Electronics in November 2003.

[4]. U. Saeed, S. Syed, S.Z. Qazi, N. Khan, A. Khan, M. Babar presented a multi-advantage and security-based home automation system at the 2010 Fourth UKSim European Symposium on Computer Modeling and Simulation (EMS) in November 2010.

[5]. Asadullah, Muhammad, and Ahsan Raza. ”An overview of home automation systems.” 2016 2nd International Conference on Robotics and Artificial Intelligence (ICRAI). IEEE, 2016.

[6]. Jothi, T. Mahara, et al. ”GSM based home environment monitoring system.” 2018.2nd International Conference on Trends in Electronics and Informatics (ICOEI).IEEE, 2018.

[7]. Das, Sukhen, et al. ”A bluetooth based sophisticated home automation system using smartphone.” 2016 International Conference on Intelligent Control Power and Instrumentation (ICICPI). IEEE, 2016.

[8]. Debnath, Banashree, Rajesh Dey, and Sandip Roy. ”Smart Switching System Using Bluetooth Technology.” 2019 Amity International Conference on Artificial Intelligence (AICAI). IEEE, 2019.

[9]. Ramlee, R. A., D. H. Z. Tang, and M. M. Ismail. ”Smart home system for disabled people via wireless bluetooth.” 2012 International Conference on System Engineering and Technology (ICSET). IEEE, 2012.

[10]. Johar, R. A., et al. ”A smart home appliances control system based on digital electronics and GSM network.” 2018 15th Learning and Technology Conference (LT). IEEE, 2018.

[11]. Kodali, Ravi Kishore, and SreeRamya Soratkal. ”MQTT based home automation system using ESP8266.” 2016 IEEE Region 10 Humanitarian Technology Conference (R10-HTC). IEEE, 2016.

[12]. Wenbo, Yan, Wang Quanyu, and Gao Zhenwei. ”Smart home implementation based on Internet and WiFi technology.” 2015 34th Chinese Control Conference (CCC). IEEE, 2015.

[13]. Bhatt, Ashutosh, and Jignesh Patoliya. ”Cost effective digitization of home appliances for home automation with low-power WiFi devices.” 2016 2nd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB). IEEE, 2016.

[14]. Somani, Shradha, et al. ”IoT based smart security and home automation.” 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA). IEEE, 2018.

[15]. S. K. Vishwakarma, P. Upadhyaya, B. Kumari and A. K. Mishra, ”Smart Energy Efficient Home Automation System Using IoT,” 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India,2019.

[16]. Mahmud, Sadi, Safayet Ahmed, and Kawshik Shikder. ”A smart home automation and metering system using internet of things (IoT).” 2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST). IEEE, 2019.