International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

IOT based Intelligent Home Safety Control Centre

R.Kennady1 , Shiva2
1Department of Artificial Intelligence and Data Science, Rajalakshmi Institute of Technology, Chennai, Tamilnadu
2Department of Computer Science and Engineering, Rajalakshmi Institute of Technology, Chennai, Tamilnadu
1kennady.r@ritchennai.edu.in, 2 shiva.s@ritchennai.edu.in

Abstract
This research focuses on the development of an IOT (IoT) intelligent home safety control centre. System consists of a user side, a safety control centre, and a terminal node, with each component having specific functionalities to enhance the safety and safety of the intelligent home environment. Key modules include data encrypting/decrypting, safety communication, control centre of user access and verification of node identity, reliable platform for credibility verification, and log inspect and alarm. The system ensures data safety, authentication, credibility analysis, and system monitoring, thereby improving the safety performance and running efficiency of the intelligent home system.

Keywords: IOT, intelligent home, safety control centre, data encryption, safety communication, control centre, user access, verification, node identity, reliable platform, credibility verification, log inspect, alarm system.

Introduction

The rapid advancement of technology has led to the emergence of intelligent homes, where various devices and appliances are interconnected to provide convenience, comfort, and efficiency to homeowners. However, the increased connectivity and automation in intelligent homes also raise concerns about the safety and privacy of personal data. As the IOT (IoT) continues to revolutionize the way we interact with our homes, it is crucial to develop robust safety systems that can safeguard against potential threats and vulnerabilities. This research focuses on the development of an IOT intelligent home safety control centre, aiming to enhance the safety performance and running efficiency of intelligent homes. The system comprises three main components: the user side, the safety control centre, and the terminal node. Each component plays a vital role in ensuring a secure and protected intelligent home environment.[1]

The user side and the terminal node are equipped with data encrypting/decrypting modules responsible for encrypting and decrypting control orders and received data. This encryption process adds an extra layer of safety, ensuring that sensitive information remains confidential and protected. The modules utilize preset encryption programs on a remote client side or the terminal node, allowing for secure communication between devices within the intelligent home network. The safety control centre, a crucial component of the system, incorporates several modules to provide comprehensive safety measures. The safety communication module filters, reconstructs, and forwards data, guaranteeing the safety of bi-directional transmission. By implementing safety filters, potential threats and malicious data are detected and prevented from infiltrating the intelligent home network.[2]

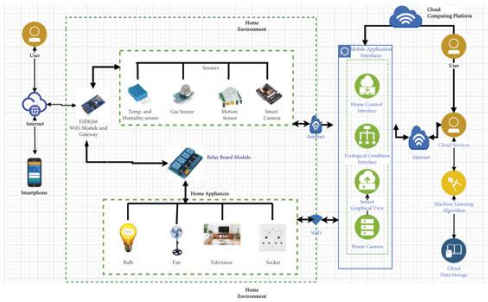
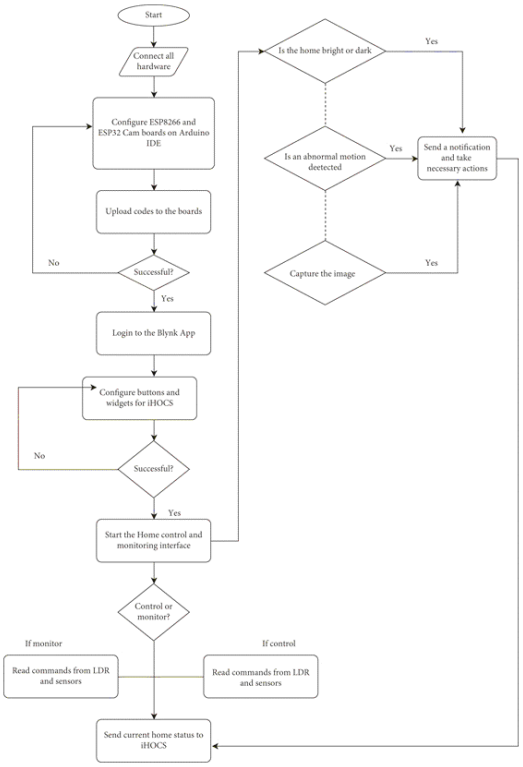


Figure 1 The iHOCS architecture.

The architectural design of the iHOCS system is presented in **Figure 1** above. The design showcases the components of the system, including the user, home appliances, sensors, a Wi-Fi module, and the cloud platform. The ESP8266 Wi-Fi module serves a dual purpose, functioning as both a communication device and a microcontroller. Through wireless communication, the ESP8266 collects data from the sensors and relay board and transmits it to the user over the Internet. The user interacts with the system using an Android mobile application, which communicates with the microcontroller (ESP8266) to send and receive commands and information. The key functionalities of the system include home monitoring, control, and security. A flowchart in **Figure 2** illustrates the sequence of processes and actions within the iHOCS environment.[3]

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*



Furthermore, the control centre of user access and verification of node identity ensure that only authorized users and devices can access the intelligent home system. This adds an additional layer of protection against unauthorized access and potential intrusions. Additionally, a platform for credibility verification is implemented to achieve system security verification, user behavior credibility analysis, data sealing storage, and free decoupling. This independent module can be maintained and upgraded separately, enhancing the system's scalability and adaptability to future safety requirements.[4]

To monitor and track the safety status of the intelligent home system, a log inspect and alarm module is incorporated. This module records user access and verification of node behaviors, performs safety inspects on log viewing operations, and promptly alerts users in the event of any abnormal activities or safety breaches. Timely detection and response to safety threats are vital in maintaining a secure and protected intelligent home environment. By implementing the IOT intelligent home safety control centre, the research aims to improve the safety performance and running efficiency of intelligent homes. This comprehensive and integrated solution addresses the challenges related to data safety, authentication, and system monitoring. The research aims to provide users with a reliable and secure intelligent home environment, ensuring their peace of mind and confidence in utilizing IoT technology for home automation.[6]

In the following sections of this research, we will delve into the specific functionalities, design considerations, and implementation details of the IOT intelligent home safety control centre. By exploring its capabilities and evaluating its performance, we aim to contribute to the advancement of secure and efficient intelligent home technologies.[5]

In summary, as the adoption of intelligent homes continues to grow, the need for robust safety measures becomes paramount. The IOT intelligent home safety control centre presented in this research offers a comprehensive and reliable solution to enhance the safety and safety of intelligent home environments. By integrating various modules and functionalities, the system aims to mitigate potential risks and vulnerabilities, providing users with a secure and protected intelligent home experience.[7]

Related Work

The existing intelligent domestic systems primarily focus on long-range or local control of devices within the home, utilizing IOT (IoT) technology and addressing indoor air chemical pollution. However, these systems often neglect crucial aspects such as information transmission safety, control safety, and user privacy, leaving them vulnerable to potential safety hazards and attacks.[3]

As the central control axis of an intelligent domestic system, the gateway plays a vital role in exchanging information between the internal and external networks. It is exposed to numerous safety threats from the external environment, while also being responsible for implementing access control and ensuring the overall safety of the intelligent domestic system.[5]

Unfortunately, due to limitations in hardware and software resources, gateways struggle to perform complex data safety processes. Moreover, the rapid development of networks poses significant challenges in terms of maintaining and upgrading the safety of intelligent domestic systems.

Therefore, it becomes essential to prioritize the safe design of intelligent domestic gateways, ensuring the safety of both users and terminals. This encompasses various aspects, including information safety, secure processing and transmission of data, and enhancing the system's ability to withstand attacks. By implementing robust safety measures for intelligent domestic gateways, the research aims to address these critical concerns. Enhancing user and terminal safety is of utmost importance, as it ensures the protection of personal information and sensitive data. Additionally, focusing on information processing and transmission safety safeguards against potential breaches or unauthorized access.[6]

Furthermore, with the ever-evolving threat landscape, it is crucial to enhance the system's ability to resist attacks. This

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

involves implementing advanced safety mechanisms and regularly updating the gateway's defenses to counter emerging threats effectively. In conclusion, given the limitations and vulnerabilities present in existing intelligent domestic systems, the safe design and implementation of intelligent domestic gateways are of utmost importance. By prioritizing user and terminal safety, ensuring information safety, and strengthening the system's resistance to attacks, the research aims to overcome these challenges and enhance the overall safety and reliability of intelligent domestic systems.[2]

Research Objective

The main objective of this research is to create a intelligent home safety control centre using IOT (IoT) technology that is both efficient and secure. The research aims to improve the overall safety and operational efficiency of intelligent home systems by integrating various advanced modules.

One of the key focuses of this research is on data encryption, which ensures that the information exchanged within the intelligent home system is protected from unauthorized access. By implementing strong encryption algorithms, the research aims to safeguard the privacy and safety of user data.

Another important aspect is the development of a safety communication module. This module plays a crucial role in securely transmitting data between different components of the intelligent home system. By establishing secure channels and implementing protocols for data filtering and forwarding, the research aims to ensure the integrity and confidentiality of the transmitted information.

The research also addresses the need for user access control and node identity authentication. These modules are designed to regulate and authenticate user interactions with the intelligent home system. By implementing robust access control mechanisms and identity verification protocols, the research aims to prevent unauthorized access and protect the system from malicious activities. Additionally, the research focuses on the development of a platform for credibility verification. This module is responsible for system-wide safety authentication, user behavior analysis, data storage, and decoupling. By providing a reliable and independently maintainable platform, the research aims to enhance the overall safety and stability of the intelligent home system.

Lastly, the research incorporates a log inspect and alarm module. This module records user access and authentication activities and performs regular safety inspects on the system. It detects any anomalies or abnormal behavior within the control centre and promptly raises alarms to alert the users and administrators. By achieving these research objectives, the aim is to create a comprehensive and reliable intelligent home safety control centre that ensures the safety and safety of IoT-enabled homes. The research contributes to the advancement of intelligent home technologies by providing an efficient and secure solution that protects user privacy, authenticates system components, and detects potential safety threats.

IOT Intelligent Home Safety Control centre

The IOT (IoT) intelligent household safety control centre described here has specific characteristics. It consists of three main components: the user side, the safety control centre, and the terminal node. The user side and the terminal node are equipped with a data enciphering/deciphering module, while the safety control centre includes several modules: a secure control centre of user access and verification of node identity, reliable platform for credibility verification, and a log inspect and alarm module.

The data enciphering/deciphering module in the user side and terminal node is responsible for encrypting and decrypting the control commands and received data using a predefined encryption method on the Terminal Server Client or the terminal node itself. The secure communication module ensures the safety of data transmission by working collaboratively with other modules. It guarantees the secure exchange of data in both directions, providing a secure channel for communication.

The user access control and node identities authentication module manage and controls user access to the system and verifies the identities of the connected nodes. It ensures that only authorized users and authenticated nodes can interact with the system. The log inspect and alarm module keeps a record of user access and authentication activities. It performs regular safety inspects on the system's operations and checks for any anomalies during the control centre's safety monitoring process. If any unusual activity or safety breach is detected, it promptly raises an alarm.

In simpler terms, this IoT intelligent household safety control centre has various components that work together to ensure the safety and safety of the system. The user side and terminal node have modules that encrypt and decrypt data, while the safety control centre includes modules for secure communication, user access control, node authentication, and log inspecting with alarm capabilities. These features help protect user privacy, authenticate system components, and detect any suspicious or abnormal behavior within the system.

By implementing such a system, households can enhance the safety of their IoT devices, safeguard personal data, and have better control over who can access their intelligent home system. This research contributes to the development of intelligent household safety and provides a reliable solution for IoT-enabled homes.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

Conclusion

In conclusion, the research has successfully developed an IOT (IoT) intelligent home safety control centre that significantly improves the safety performance and running efficiency of intelligent homes. By integrating several key modules, the system offers robust protection and safety measures.

One of the notable features of the system is the data encrypting/decrypting module, which ensures that all control commands and received data are securely encrypted and decrypted using preset encryption programs. This module safeguards the confidentiality and integrity of the transmitted information, protecting it from unauthorized access. The safety communication module plays a crucial role in the system by enabling secure and reliable data transmission. It filters and forwards data while guaranteeing the safety of bi-directional communication. This module ensures that the data exchange within the intelligent home system is protected from potential safety threats.

The control centre of user access and verification of node identity provides strict control over user access and authenticates the identities of the system's components. This helps prevent unauthorized access to the system and ensures that only trusted devices and users can interact with the intelligent home. The credible platform module enhances the system's safety by facilitating system-wide safety authentication, user behavior analysis, and data storage. It also allows for independent maintenance and upgrades, ensuring the system's stability and safety.

The log inspect and alarm module records user access and node authentication behaviors, conducts regular safety inspects, and promptly alerts users and administrators of any abnormal activities or potential safety risks. This module adds an extra layer of safety and ensures that any suspicious behavior is quickly detected and addressed.

Overall, the IoT intelligent home safety control centre presented in this research provides comprehensive and reliable safety measures for intelligent homes. It improves the safety of IoT-enabled households, giving users peace of mind and a secure environment. The system successfully achieves its research objective of developing an efficient and secure gateway solution for IoT intelligent homes, contributing to the advancement of intelligent home technologies.

Reference

1. The Role of Internet of Things in Smart Homes - S Padmanaban, MA Nasab, ME Shiri - based Smart Power - 2023 - Wiley Online Library
2. Enabling automation and edge intelligence over resource constraint IoT devices for smart home - M Nasir, K Muhammad, A Ullah, J Ahmad, SW Baik - Neurocomputing, 2022 – Elsevier
3. “It would probably turn into a social faux-pas”: Users' and Bystanders' Preferences of Privacy Awareness Mechanisms in Smart Homes - PK Thakkar, S He, S Xu, DY Huang, Y Yao - Human Factors - 2022 - dl.acm.org
4. An IoT-based smart home automation system - C Stolojescu-Crisan, C Crisan, BP Butunoi - Sensors, 2021 - mdpi.com
5. Anonymous authentication scheme for smart home environment with provable security - M Shuai, N Yu, H Wang, L Xiong - Computers & Security, 2019 - Elsevier
6. A review of intelligent home applications based on IOT - M Alaa, AA Zaidan, BB Zaidan, M Talal - Journal of Network - 2017 – Elsevier
7. IOT (IoT) for building intelligent home system - T Malche, P Maheshwary - Conference on I-SMAC IoT in 2017 - ieeexplore.ieee.org
8. Design and fabrication of intelligent home with IOT enabled automation system - WA Jabbar, TK Kian, RM Ramli, SN Zubir - IEEE - 2019 - ieeexplore.ieee.org