Smart Home Security System Using AWS Services

Contents

Abstract

The purpose of this review is to scout the viability of smart home security systems with the help of AWS services that will be involved in completing the project. The hardware part includes the smart sensor and Arduino along with the services available in AWS. And exploring the possible hazards or difficulties that may encounter in this project by inspecting similar projects.

Introduction

Smart home security systems have become increasingly popular due to the rise of home automation technology. Smart home security systems allow homeowners to remotely monitor and control various aspects of their home, including security cameras, locks, and alarms, using their smartphones or other internet-connected devices. AWS (Amazon Web Services) is a cloud-based platform that offers a range of services that can be leveraged to build a smart home security system. In this literature review, we will explore the various AWS services that can be used to build a smart home security system.

Some current research areas and trends in smart home security system projects include:

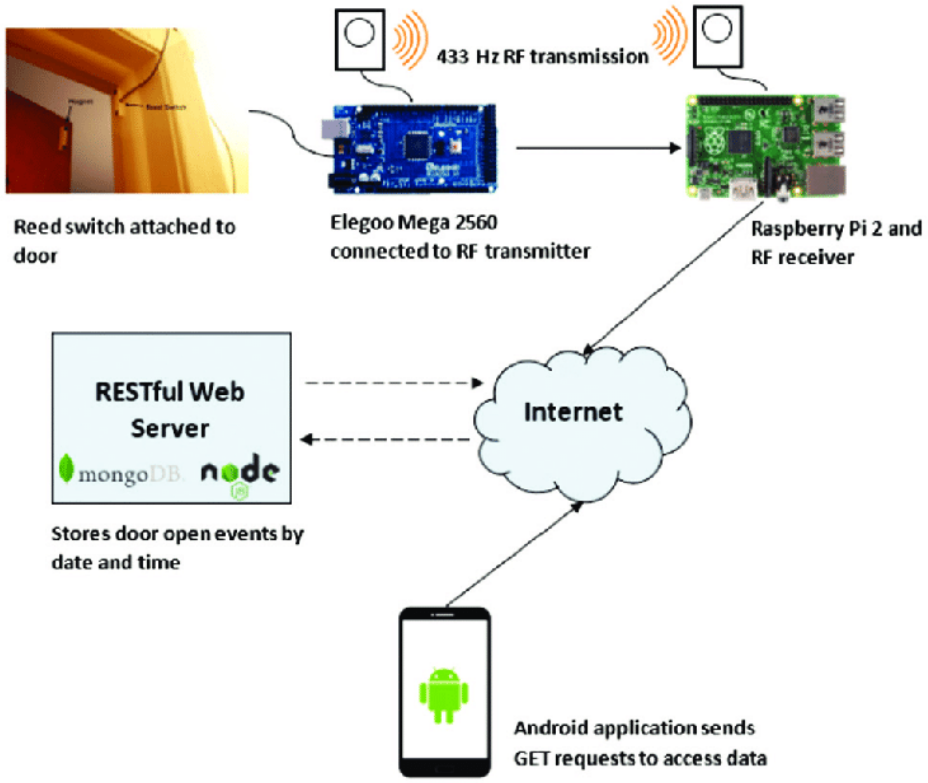
- Sensor fusion: Sensor fusion is the process of combining data from multiple sensors to improve accuracy and reduce false alarms. Many researchers are exploring ways to use sensor fusion to improve the accuracy of smart home security systems, such as combining data from motion sensors and door sensors to more accurately detect intruders.
- Machine learning and artificial intelligence (AI): Many researchers are exploring the use of machine learning and AI techniques to improve the effectiveness and accuracy of smart home security systems. For example, some studies have explored the use of deep learning algorithms to analyze sensor data and detect anomalies that may indicate a security breach (Rajalingam and Priya 2018).
- Integration with other smart home devices: Smart home security systems are increasingly being integrated with other smart home devices, such as smart locks and smart thermostats. Researchers are exploring ways to improve the interoperability of these devices and create more seamless and integrated smart home security systems.

Smart Home Security System

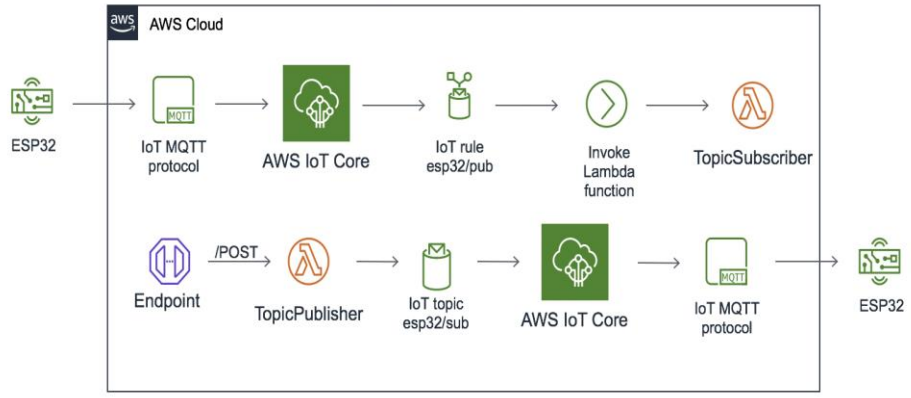
Smart home security system is a technological solution designed to increase the safety and security of residential properties. It is composed of advanced sensors, cameras, and other devices that can monitor and control the home environment. The system is capable of detecting and alerting homeowners of potential security threats such as break-ins, fires, gas leaks, and

water damage. Additionally, it can automate various aspects of home security, such as turning off lights and locking doors when the homeowners are away.

This paper focuses on various hone security system methods that provide perception and are available on how we can improve and increase the security system.



Source: (Mohammad & Chad, 2019)



Source: Amazon

Current Research

1. Threats to Smart Homes: Several studies have identified the different types of threats that smart homes face. These include physical attacks such as theft and vandalism, cyberattacks such as hacking, and privacy violations such as data breaches.

2. Machine Learning Algorithms: Machine learning algorithms are increasingly being used in smart home security systems to improve their ability to detect and respond to security threats. These algorithms can analyze data from sensors and cameras to identify patterns and anomalies that may indicate a security breach.

3. Integration with Other Systems: Smart home security systems can be integrated with other smart home devices such as thermostats and lighting systems to create a more comprehensive and efficient smart home ecosystem. Studies have shown that integrating these systems can improve the overall security of smart homes.

4. Components of Smart Home Security Systems: Smart home security systems consist of several components such as sensors, cameras, and control panels. These components work together to detect and respond to security threats. Studies have shown that the effectiveness of smart home security systems is directly related to the quality and reliability of these components.

5. User Experience: The usability and user experience of smart home security systems are also important factors that contribute to their effectiveness. Studies have shown that users are more likely to use and trust a security system that is easy to set up and use.

Technologies

It is necessary to examine the technologies carefully for every project that are used to accomplished it to ensure that the technologies used are suitable and properly fitted for the project.

Sensors

Sensors are an important component when it comes to smart home security projects as they can detect and alert homeowners of potential security threats or intrusions. These sensors can be installed in various locations throughout the home, such as doors, windows, and other entry points.

Motion sensors: These sensors are used to detect movement within a specific area. They can be placed in different parts of the house, such as the entryway, hallways, or rooms, and can trigger an alarm or a notification to the homeowner or security system if any motion is detected. Examples of motion sensors include the Philips Hue Motion Sensor and the Nest Detect. (Danny Jost, 2019)

Door and window sensors: These sensors are used to detect when a door or window is opened or closed. They can be installed on any door or window and can trigger an alarm or notification if they detect any unauthorized access. Examples of door and window sensors include the Samsung SmartThings Multipurpose Sensor and the Ring Contact Sensor. (Krista Brunton, 2020)

Security

As with any technology, smart home security systems are not immune to issues and potential vulnerabilities. Some of the current issues on smart home security systems include:

- Privacy concerns: Smart home security systems collect a lot of data about the home and its occupants, such as activity patterns, voice commands, and video footage. There is a risk that this data can be misused or stolen, compromising the privacy of the homeowners.
- Technical issues: Smart home security systems are complex and require regular updates and maintenance. Technical issues such as system failures, connectivity problems, and software glitches can impact the effectiveness of the system and cause inconvenience to homeowners.
- Compatibility issues: Smart home security systems often require different devices and components to work together seamlessly. If the components are not compatible, the system may not function properly or may require additional expenses to upgrade or replace the incompatible components.
- Cybersecurity risks: Smart home security systems are connected to the internet, which makes them vulnerable to hacking and cyberattacks. If a hacker gains access to the system, they can disable or manipulate the security features, putting the home and its occupants at risk.

AWS IOT core

AWS IoT Core is a managed cloud service that allows us to connect IoT devices to the cloud and process data generated by devices. In terms of smart home security systems, AWS IoT Core can be used to connect sensors and other devices to the cloud and process the data

generated by those devices. One way to use AWS IoT Core for a smart home security system is to set up rules that trigger push notifications when specific events occur. For example, we can set up a rule that triggers a push notification to our smartphone when a motion detector is triggered or when a door or window sensor is opened. You can use Amazon SNS (Simple Notification Service) to send push notifications when a rule is triggered. We also need to set up the appropriate permissions and security settings to ensure that only authorized users are able to receive push notifications.

Similar Projects

IoT Based Home Automation Using Raspberry Pi by K. Venkatesh S. Hemaswathi3, B.Rajalingam

In 2018, Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, four authors of Department of Computer Science and Engineering developed the process of smart home automation using raspberry Pi, they established the internet connection for IoT by using IP addresses. They connected Raspberry Pi and mobile phones through Wi-Fi and used cloud services for monitoring and controlling the house appliances.

In 2019, a smart Home Security System Using IoT and Blockchain Technologies was introduced that utilizes IoT and blockchain technologies to enhance security and privacy. The authors discuss the various components of the system, such as motion sensors, cameras, and a blockchain-based authentication mechanism. They also highlight the advantages of using blockchain for data storage and authentication in smart home security systems. (H. Taha, A. Al-Fuqaha, M. Khattab, & M. Ayyash, 2019)

A Machine Learning-based Smart Home Security System

This paper proposes a smart home security system that uses machine learning algorithms to detect anomalies in the sensor data. The authors discuss the different types of sensors used in the system, such as motion sensors and door sensors. They also present the results of their experiments, which show that the proposed system can accurately detect anomalies in the sensor data. (S. Kim, J. Kang, & Y. Kim, 2019)

Conclusions

Smart home security systems are becoming increasingly important as more people adopt smart home technologies. This literature review paper has identified the key features that make a secure smart home, including reliable hardware and software components, machine learning algorithms, a good user experience, and integration with

other smart home systems. These features should be considered when designing and implementing smart home security systems to ensure their effectiveness and usability.

References

Hsu, Y.-L., Chou, P.-H., Chang, H.-C., Lin, S.-L., Yang, S.-C., Su, H.-Y., Chang, C.-C., Cheng, Y.-S. and Kuo, Y.-C. (2017). Design and Implementation of a Smart Home System Using Multisensory Data Fusion Technology. *Sensors (Basel, Switzerland)*, [online] 17(7). doi:https://doi.org/10.3390/s17071631.

W. M. Kang, S. Y. Moon, and J. H. Park, “An enhanced security framework for home appliances in smart home,” *Human-centric Computing and Information Sciences*, vol. 7, no. 1, p. 6, 2017.

A. Singh, D. Gupta, and N. Mittal, “Enhancing home security systems using IOT,”, pp. 133–137, Coimbatore, India, October 2019.

Hackster.io. (n.d.). *Smart Security Camera*. [online] Available at: https://www.hackster.io/hackershack/smart-security-camera-90d7bd.

R. Liu and Y. Ge, “Smart home system design based on Internet of Tings, pp. 444–448, july 2017

Khattar, S., Sachdeva, A., Kumar, R. and Gupta, R. (2019). *Smart Home With Virtual Assistant Using Raspberry Pi*. [online] IEEE Xplore. doi:https://doi.org/10.1109/CONFLUENCE.2019.8776918.

Kang, W.M., Moon, S.Y. and Park, J.H. (2017). An enhanced security framework for home appliances in smart home. *Human-centric Computing and Information Sciences*, 7(1). doi:https://doi.org/10.1186/s13673-017-0087-4.

Sehgal, K. and Singh, R. (2019). *Iot Based Smart Wireless Home Security Systems*. [online] IEEE Xplore. doi:https://doi.org/10.1109/ICECA.2019.8821885.

Kim, J.T. (Steve) (2022). *Analyses of Open Security Issues for Smart Home and Sensor Network Based on Internet of Things*. [online] *www.intechopen.com*. IntechOpen. Available at: https://www.intechopen.com/chapters/78119 [Accessed 29 Mar. 2023].

Lee, Y., Rathore, S., Park, J.H. and Park, J.H. (2020). A blockchain-based smart home gateway architecture for preventing data forgery. *Human-centric Computing and Information Sciences*, 10(1). doi:https://doi.org/10.1186/s13673-020-0214-5.