User authenticated smart home automation system with healthcare

Nagajayanthi B1,*, Vikneshrajan M1, Kuppala Navya1

1 School of Electronics Engineering, Vellore Institute of Technology, Chennai, Tamil Nadu, India

* nagajayanthi.b@vit.ac.in

Abstract. Traditional home automation is inconvenient for aging people. Biometric based personalized smart phone secures smart home automation. Internet of Things (IoT) is envisioned as a promising solution in the thrusting arenas of healthcare, industries, home automation and other domains due to its significant contribution towards connectivity, security, sleek design, low power, low cost and low workforce. This has come a long way industrially and is making an impact in the domestic market after Covid-19 pandemic. Social distancing and contact less solution is the need of the hour. Life style of people has changed from home to workplace such as remote monitoring, collaborative online work-place and online classes. This has increased the economic status of the home automation products manufacturing industry. User Authenticated Smart Home Automation with Healthcare Architecture considers security along with healthcare. This takes into account IoT reusable design concept that uses in-built user specific biometrics in smart phone for secured authentication. IoT based electronics and electrical devices are remotely monitored. The user activity is monitored and archived for future retrieval. An ambient temperature is maintained to make sure that the devices are operated in near ideal circumstances to avoid thermal throttling and this extends the lifetime of the devices. Thermal throttling causes serious threats to the devices and to the human being. In the proposed User Authenticated Smart Home Automation System with Healthcare, smart home is secured using user specific biometric authentication; sanitizer is provided and temperature is measured on entry; thermal throttling due to devices is prevented by maintaining the room temperature thereby providing healthcare.

Keywords – Biometric; Authentication; Flutter; Thermal Throttling; Healthcare.

1. Introduction

Covid-19 pandemic has immensely affected life routine. But amidst negatives, this has caused most of the people to spend quality time at home. So home automation and customization is a positive solution. With increased digitization, online meetings and online classes, people have purchased more laptops and mobiles [11] extending applications from school, college, industry, healthcare and so on. Pandemic has given a boom to this market after adoption to social distancing solutions [1]. IoT has reshaped and revolutionised the world by staying connected. In August 2020, the United States Government ordered Google to stop offering it’s Android services to the Chinese smartphone giant Huawei due to the pandemic crisis. This affected smart phone manufacturing business in Huawei. Google further stopped offering its services like GMail, Google Maps, YouTube etc., Pandemic affected the routine life and has slashed the economy of the country.
Majority of the Internet users are familiar with the usage of mobile and laptop devices. IoT home automation is expected to raise by 47% in 2025. Different strategies are used to minimize power, size etc., [7] qToggle is used to optimize IoT design. Biometrics is a unique trait of the person which could be fingerprint, face or voice [3]. Automation based approach has become stringent from the consumer point of view [4]. It enhances the approach of the problem statement by reducing manual effort. Biometric authentication [10] provides minimalist authenticated solutions to day-to-day activities like unlocking the door with minimum physical contact, and to control the connected devices of the ecosystem, remotely. Given the current scenario with the novel coronavirus breakout, there is a state of paranoia in people to avoid touching any public surfaces, to avoid transfer of the stain. The proposed research consists of four features that contributes to the automation of the household with minimal physical contact as well as providing a framework to handle security and thermal throttling solutions. A secured design has been adopted by engaging in data minimization to avoid security breaches. This application also provides transparency to the user by providing a copy of the data collected.

The four main features adopted include:

1.1. **User Authentication for Access Control** – Smartphone’s are using built-in biometrics for door unlocking. This facilitates reusing of the existing features thereby reducing the cost and simplifying the design. Biometrics [8] helps in verifying the user and allows the user to access the smart home ecosystem only when their biometrics is authenticated. Additionally, an OTP verification mechanism is also implemented for authentication. User can choose either biometrics or OTP mode for authentication.

1.2. **Sanitizer Dispenser and Temperature for Healthcare** – In pandemic, sanitizer contact is a major threat for virus spread. Sanitizing is automated [6]. Once the user enters his home, a generous amount of the sanitizer is dispensed into the user's hands. Temperature of the user is measured using a temperature sensor.

1.3. **Remote Access** - This feature enables the user to remotely access and control all the IoT based devices at home. As long as the devices are connected to the Wi-Fi Module [2], the user can access it from anywhere. An open source UI toolkit, Flutter is used to control the devices remotely.

1.4. **Ambience Temperature Monitoring for Healthcare**– The CPU or a GPU limits its peak performance when the surface temperature of the device is not reduced. This is called Thermal Throttling. Ideally an IoT device works with its full potential but practically the devices generate heat [9]. This heat needs to be dissipated for optimum performance. If this heat is not removed properly, the device gets heated up causing health hazards and also affects the performance of the device. This is a bigger concern in terms of passively cooled devices like smart phones. Since most of the devices are in contact with the user or are in near proximity to the user, heat generated by the devices needs to be monitored. The proposed system sets the device at an ideal temperature based on the environmental temperature, in order to ensure maximum performance of the system with extended lifetime. This avoids thermal throttling thereby preventing health hazards. This feature is useful when people spend most of the time with their devices at home during this pandemic.
All of the aforementioned features are developed into a User Authenticated Smart Home Automation System using flutter. Mobile development is developing at a faster pace in IoT [5]. Dart programming language brings UI to life. This is used to code flutter apps. The major advantage of Flutter is that, a single source code could be written for multiple platforms thereby supporting heterogeneity. In this application, a set of Dart files is used as the source code, and then the compiler would compile for different environments, say iOS and Android. Augmenting to these salient features, the novelty of this research is to provide User authentication for security, thermal throttling solution and social distancing solution for healthcare as the need of the hour.

2. Implementation of User Authenticated Smart Home Automation with Healthcare System Architecture

The proposed User Authenticated Smart Home Automation System is designed to perform: (i) User Authentication using biometrics or OTP (ii) Tracking, Monitoring and actuating devices (iii) Analyse the thermal throttling effects on human and devices. An IoT based mobile app is designed to authenticate, track, monitor and analyse using flutter. Flutter enables cross-platform applications to run on multiple platforms. Dart provides flawless UI experience. Flutter apps are coded using Dart and are compiled using ReactNative. This provides secured access. IoT devices at home are paired with the Mobile using Wi-Fi or Bluetooth. User Interface (UI) integrates IoT devices with Wi-Fi. The corresponding Plug-Ins needs to be added. Finally these are connected with an Arduino for customization. UI is designed with the corresponding widgets for customization. HTTP protocol has been used to enable the App to communicate with ThinkSpeak Cloud. All the commands for monitoring and controlling are provided using HTTP protocol. For temperature monitoring, ideal temperature is set using OpenWeatherMapAPI for the devices to perform optimally.

Technologies augmented with IoT to design and develop User Authenticated Smart Home automation system is as shown in Figure 1.

![Figure 1](image_url)
OTP is entered in the text field provided, the user is authenticated. Once the User is verified, access will be granted to all the connected IoT devices.

![Diagram](image1)

**Figure 2.** Sequential Flow involved in User Authentication

Figure 2 depicts the sequential steps involved in User authenticated smart home automation system. Most of the intensive processing steps are done using Flutter application. The control and actuating commands are sent from the app to Arduino using ThingSpeak API. Arduino is programmed to carry out instructions as per the command it receives.

![Diagram](image2)

**Figure 3.** Access Control based on User Authentication

Figure 3 signifies access control based on biometrics or OTP. As soon as the App is started, the users need to authenticate their identity. Once Users are verified, the door is unlocked and commands are
sent as customised to the appropriate devices. A prototype of the user authenticated smart home automated system was implemented using Tinker Cad as shown in Figure 4.

![Figure 4](image_url)

**Figure 4.** User Authenticated Smart Home Automated System with Healthcare

Figure 4 signifies the proposed system. Once the user is authenticated by the flutter app, a customized quantity of sanitizing liquid is provided for sanitization. His temperature is checked at the entry point using a temperature sensor. If these values are as per the threshold ranges, the person is allowed entry into the home else an alert message of denial is displayed. An Arduino is used for customized control. As per the signal received from the App based on access control, IoT devices could be controlled.

![Figure 5](image_url)

**Figure 5.** Temperature Monitor Circuit

Figure 5 indicates temperature monitoring inside the room. Temperature is monitored and displayed in the LCD. If the temperature is more, the temperature of the devices are controlled by maintaining optimal temperature inside the room. Most of the people are exposed to hazardous radiations from gadgets while working from home or studying from home during pandemic. Data is sent to the Cloud using ThingSpeak and is accessible remotely. Figure 6 signifies ThingSpeak customized to receive the parameters from the IoT device remotely. Unique Channel ID and API key is set for the IoT device.
Once the ambient room temperature is adjusted, the device temperature is controlled. Inferences on IoT device performance is displayed in ThingSpeak with and without A/C as shown in Figure 7. This shows the effect of cooling. Thermal throttling is reduced with temperature control. The ambient room temperature is adjusted to assist with the CPU of the mobile device to control its core temperature. Observations are plotted for a smart phone under two circumstances with and without AC. This is signified for Samsung mobile as shown in Figure 8. This signifies fall in peak performance due to rise in CPU temperature.
Figure 7 depicts significant rise in temperature without cooling. Figure 8 signifies peak performance of the device in optimized temperature environment.

3. Performance Analysis

After deploying the Dart code in the Flutter app, simulation ends up in the home page of the mobile phone. This layout is shown in Figure 9. The second image in Figure 9 corresponds to the unlock page. Once the user clicks “Verify Your Identity” on the home page, User would be guided to the unlock page. The unlock page has options for the user to verify his/her identity. The users can either opt for biometric based unlock or OTP based authentication method.

![Figure 9. Home page and Unlock page of the App](image)

Once the user presses “Biometrics” button, the app will trigger the system commands of all the built-in biometrics authentication features in the specific smartphone. Biometrics could be user specific function relating to face, fingerprint, etc., This smart phone unlocking feature design is suitable for all smart phone models, irrespective of brand and model. This implementation can also make use of iPhone’s FaceID as well. Figure 10 shows the screen that the user will be seeing when the biometric authentication process is taking place.

![Figure 10. User authentication using built in biometrics](image)

The other method for authentication in the App is through OTP. When the user presses the “OTP Authentication” button, an OTP is sent to the registered mobile number as shown in Figure 11. This OTP is to be typed in the text field for verification.
After authentication, the users are re-directed to the control panel as shown in Figure 12. Here the user has full control to all the connected devices in the smart home environment. Users can unlock the door, send commands to the IoT enabled appliances such as fan, light, etc., Multiple devices could be controlled based on availability.

From here the user navigates to control specific devices such as light and fan as shown in Figure 13.

The status of the controlled devices is updated to the Cloud using ThingSpeak as shown in Figure 14 and 15 simultaneously, where it is stored for future reference.
For temperature monitoring, the temperature is taken from the OpenWeatherMapAPI for reference as displayed in Figure 16. Based upon this temperature, an ideal room temperature is set as shown in Figure 17.
The Wi-Fi module (ESP8266) connects the User Authenticated Smart Home Automation System to the Cloud using ThingSpeak. Cloud is vulnerable to attacks. Protective measures are to be taken [12] for bug-free environment.

4. Summary

A prototype of the User Authenticated Smart Home Automation System was successfully implemented and tested. Security is a pressing issue in smart home devices. Even though the end points are secured, IoT connects the devices through gateways and Cloud, which are open to malicious threats and hackers. If hackers get hold of the devices in a smart home, the end results would be devastating. Devices need to be connected to the network always. The main objective of this research is to develop an economical and secured smart home automation system along with healthcare benefits to counteract the effects of pandemic. The user can have secured access to his devices at minimal cost and optimal design. As the App is being built and developed in flutter, the scope of cross platform compatibility is very high. This ensures strong support for the App in future with constant bug fixing and addition of more features. Implementation of real time video feed, night vision cameras with live feed to mobile phones would be the next milestone. Some of the salient standout features of this work is that, as the app is built on flutter, it can work efficiently on both Android and iOS platform. With future updates, even a windows app could be implemented using the same source code. IoT Reusability concept has been integrated by using the Built-in biometrics in smartphone .This implementation does not require any additional hardware for functioning. This reduces the cost involved in the design of additional hardware for authentication.

References

[1] Arjun Sharma, B. Nagajayanthi, A. Chaitanya Kumar, Shirish Dinakaran, [2021].” IoT-Based COVID-19 Patient Monitor with Alert System”, Futuristic Communication and Network Technologies, Springer Professional.

[2] N. A. Ali, A.R. Syafeezza, A. S. Ja'afar, Norihan Abdul Hamid and Ts Saleha binti Mohamad Saleh,[2019].” Home automation monitoring system based on Internet-of-Things application”, Journal of Physics , Conference Series.

[3] Bhawna Narwal, Amar Kumar Mohapatra, [2021],”A survey on security and authentication in wireless body area networks”, Journal of System Architecture, Vol. 113.

[4] Cristina Stolojescu-Crisan , Calin Crisan and Bogdan-Petru Butunoi ,[2021],” An IoT Based Smart Home Automation System”, Sensors, Vol.27,pp.3784.

[5] Frank Zammetti, [2019],” Practical Flutter”, Apress, Berkeley, CA.
[6] Juhui Lee, Jin-Young Lee, Sung-Min Cho, Ki-Cheol Yoon, Young Jae Kim, Kwang Gi Kim,[2020],” Design of Automatic Hand Sanitizer System Compatible with Various Containers”, Health Information Res, Vol.26(3), pp.243-247, PMC.

[7] B. Nagajayanthi, [2019], “Energy Efficient Light Weight Security Algorithm for Low Power IoT Devices “, International Journal of Engineering and Advanced Technology (IJEAT), Vol. 9 (1S3), pp. 2249 – 8958.

[8] Nor Syazwani Md Noh, Haryati Jaafar , Wan Azani Mustafa, Syed Zulkarnain Syed Idrus, A. H. Mazelan,[2020],” Smart Home with Biometric System Recognition”, Journal of Physics: Conference Series, Vol.1529, IOP Publishing.

[9] Théo Benoit-Cattin, Delia Velasco-Montero and Jorge Fernández-Berni,[2020],” Impact of Thermal Throttling on Long-Term Visual Inference in a CPU-Based Edge Device”, Electronics, Vol.9, pp. 1-16.

[10] Teena Joseph, S.A. Kalaiselvan, S.U. Aswathy, R. Radhakrishnan, A.R. Shamna,[2020],” A multimodal biometric authentication scheme based on feature fusion for improving security in cloud environment” , Journal of Ambient Intelligence and Humanized Computing, Vol.12, pp.6141-6149.

[11] Urvi Singh, M.A. Ansari,[2019],” Smart Home Automation using Internet of Things”, Second International Conference on Power Energy, Environment and Intelligent Control, IEEE Explore.

[12] I. Vaccari, M. Aiello, F. Pastorino and E. Cambiaso, "Protecting the ESP8266 Module from Replay Attacks," 2020 International Conference on Communications Computing, Cybersecurity, and Informatics (CCCI), 2020, pp. 1-6.