Global Journals LaTeX JournalKaleidoscope™

Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

A Secure Framework for IoT Smart Home by Resolving Session Hijacking

Fozilatoon Humaira[1], Md Sanju Islam[2], Sanjida Akter Luva[3], Md Bayazid Rahman[4] and Md Bayazid Rahman[5]

[1] Notre Dame University Bangladesh

Received: 16 December 2019 Accepted: 31 December 2019 Published: 15 January 2020

Abstract

IoT is a blessing in the field of information and technology. It is developing and deploying day by day. It is working for our betterment in the section of home, environment, retail, security, factory, industry, agriculture, education, energy, healthcare, and so on. In the Smart Home section, there are a numerous inventions. Vast analysis and working can be possible if needed. We have worked with session hijacking and implement it in our Smart Home Prototype. This paper represents the basic concept of IoT in Smart Home with Security like Session Hijacking.

Index terms— IoT, internet of things, smart home, session regeneration, security, session hijacking

1 I. Introduction

nternet of Things is a system of systems that means all the electronic devices are connected in a local area forming a system. Further, this system will connect with each other to build up a bigger system. Basically, IoT is a concept or technology which aims to connect all the devices to the internet and help them communicate with each other using the internet as a medium. This technology is developed for better efficiency and accuracy apart from minimizing human interaction with the device. Some application areas of the Internet of Things are: Home Automation, Healthcare, Agriculture, Transportation, Manufacturing, and Environment. We have worked in the Smart Home part and develop its security.

The organization of the paper is as follows: section 2 discusses the related work and motivation. Required tools described in section 3. Proposed Web app and Improved Security schemes are discussed in section 4. Our Experimental results are in section 5. And we have put our Future work in section 6 and in the study we have faced some problems that have limited some scopes and these limitations are also in this chapter. Section 7 concludes our work with the conclusion part.

2 II. Related work and Motivation

There are a lot of IoT applications that we can see. A famous website Product Hunt lets users share and discover new products which have made a ranking that is displayed below:

Author ? ? ? ?: Department of Computer Science and Engineering Notre Dame University Bangladesh, Motijheel, Dhaka, Bangladesh. e-mails: h.fafpa21@gmail.com, sanjuislam30@gmail.com, sanjida.luva@gmail.com, bayazid@ndub.edu.bd Analyzing these we have decided to work in the session hijacking and smart home. We have also gone through some related papers.

In paper [b9], a lightweight handshake mechanism is used between the client and server for authentication that produces encrypted payloads. Although they claim the scheme is efficient for replay attack but they cannot determine whether it can prevent other security attacks or not.

By reading the [b10], we have got to know this paper proposes an IoT-Based Dual-Mode Smart Home Automation System. The system uses a touch screen interface mode. A mobile app is developed to enable home users to monitor and control their home appliances using mobile.

In paper [b8], we have found that A smart home-based on the internet of thing to enable the control and the remote monitoring of home's devices and to allow the user to adapt the system to his desires and needs. This paper presents an approach to implementing a smart home system using the Internet of thing IoT, Web services, and an Android App.

By going through [b11], Session-id is encrypted and de-crypted between the server and the client. Here the attacker cannot know the session id as it is already a signed value that needs not to be encrypted.

3 III. Tools

A detailed study has been done to find the appropriate hardware and software resources to fulfill the requirements of the smart home.

Hardware For our work purpose, we have used Arduino Uno as Micro-controller, ESP8266 as WIFI Module, DHT11 as Temperature and Humidity sensor, LED and Fan.

4 Software

Arduino IDE, Xampp.

5 Language

6 PHP, JavaScript

Database MySQL

7 IV. Proposed Approach

Within the IoT Functional Block, we have worked with devices, application, the security of the smart home, and smart home application.

8 a) Proposed Web app

Our proposed scheme includes an IoT based Smart Home, where different sensors and devices will act as clients, which will be controlled with the help of an application. The application is mainly web-based that will help to monitor and control the smart home. The proposed web-based app will be built with the help of HTML, PHP, and JavaScript. The user interface will be designed with HTML and PHP, and JavaScript will be used for the development of the web application. A database will also be comprised in the proposed scheme to store the data related to smart home and smart home app. The database will consist of two tables -user and weather. The user table will hold the information of the registered users such as User name, email, and password. The password will be stored in the database in an encrypted form with the help of Hashing. The weather table will hold the information about the weather of the smart home. It will store the data about temperature and humidity. The web application at first will have a registration page. A user must be registered to the app by providing the information such as username, email, and password which will be then stored in the database. After completing the registration, the user will automatically be logged into the application.

A user must log in to the app to control the appliances of the smart home for which the app will have a login page. When the username and password provided by the user will match with the stored information in the database, then the user can log in to the application.

9 Fig. 3: Login sequence

After logging into the app, the user can monitor the temperature and humidity of the smart home and can control appliances of the smart home. The temperature and humidity will be captured by the DHT sensor and stored in the weather table of the database. Then readall.php file will read the weather information from the database. The user can read all the weatherrelated data by accessing the readall.php file. After that, the index.php file of the proposed web app will get data from readall.php file and display the last current value of temperature, humidity on the app.

10 b) Improved Security of the web app

The concept of session id will be used with our app. Session id will keep the login status on record so the user can browse as many passwords-protected pages as he wants without having to login again until he logs out. After a user signs in, a session will be securely created by the server. Then, that session ID will be stored in a session cookie on the user's browser. While the user will remain logged in, the cookie will be sent with every subsequent request. At each appeal, the server will take a look at the session cookie to read the session ID. If it matches the data stored in its memory, it will send a response back to the browser, letting it know everything is okay and ready to go. But Session initiation is a prerequisite to access the app and the other document. If the user is not logged into the app, the server will not provide any session-id, and without the session id the user cannot browse any password protected page and will return to the login page with the request for doing log in.

A security attack can take place regarding log in process. If a person who will be not registered to the app, somehow can manage to get the session id, can log in to the app. With this session-id the attacker can send access requests to the server and will get access permission from the server.

11 Fig. 4: Sequence Diagram of Session Hijacking

To prevent this attack, session regeneration will be used. With the help of this, the current session will be invalid after logging out from the app and will generate a new session-id with the next login. Once the session becomes invalid, the attacker cannot access any of the information.

If the attacker logs into the app with the session id, then he can access the readall.php file to get all the weather data of that smart home. Here the proposed scheme will use an encryption method. All the weather data of the database will be encrypted with AES using only one secret key. As a result, the readall.php file will show the encrypted weather data. Hence the attacker can access the readall.php file, will only get the encrypted data.

12 V. Experimental Result

As discussed in our proposed scheme, we have developed a web-based app through which we can monitor the temperature and humidity of our smart home and control other appliances of the home.

Without any authentication process, anyone can use the app, which will be vulnerable for the security of the smart home. To enhance the surveillance of the smart home, we have developed an authentication scheme for our web app. In this scheme, a person must register himself to the database user table. For this, there will appear a registration page on the web app where the user must provide a username, email address, and password to sign up.

The database is created in MySQL, and a user table in the database has all the information that a user provides to register into the app. For the security purpose the passwords are encrypted with hashing function. The MD5 message-digest algorithm, is used for the hash function. It converts the password to 128-bit hash value and saves it in the database. Once a user completes the registration process, he can log in to the app with a proper username and id. If the username and password match with the information located in the user table of the database, he can log in to the app successfully.

13 Fig. 13: Session Start

If the username and password mismatch with the information saved in the database, then it will show a message saying wrong username/password combination. So to gain access to the app, the user must provide with proper username and password. Otherwise, no one can access the web app.

When a user logs into the app successfully with proper username and password, the server will provide with a sessionid. With this session id, the user can access any password-protected page. He does not need to submit the password again and again to browse any file. He can send the request with the session id to browse the file. If the session id is valid, the server will redirect him to the requested page.

The session will be valid until the application is logged in. When the user logs out from the application, the session will be invalid. Once the session becomes invalid, the user cannot access any file. To read any document, the user must login the application again. If the user requests to check over any file, it will redirect him to the login page. With the successful login process, the session will start again and permit to access files. If the attacker somehow gets the session id, he can log into the app with that session id. He does not need any proper username and password to log in to the application. With the valid session id, the attacker can successfully login into the application and browse any files, monitor, and control the smart home.

We copy the session id after successfully login to the app and use that session id to log in to app from chrome incognito and it successfully logs in to the app without the username and password. We can browse the files after logging into the application.

Here to update the security of the web app, we have to prevent this session hijacking. We have used a function called session regenerate. With this function, the different sessions will regenerate with every login process. Without this function, the same session id is provided for every login process. So if the attacker once gets the session id, he can easily log into the app with the id as many times as he wants. But this function provides different session-id with each login request. So the attacker cannot use the same session id to log into the application. Now, if the real user logs out from the application, then the session will be invalid. As a result, the attacker can no longer use the application with that old session id. So whenever the attacker sends a request to browse any file with that old session id, the server will redirect him to the login page.

We logged in to the application using session-id from chrome incognito. Then we logged out from the application from our browser and tried to browse the file from incognito. But it redirected us to the login page as the session became invalid.

We have used the DHT11 sensor to read the temperature and humidity amount. We have used led to turn on and off the light. The DHT11 sensor and LEDs are connected with the Arduino Uno. The DHT11 sensor reads the temperature and humidity with 3000 ms delay and inserts the values to the database weather table.

The readall.php file reads the temperature and humidity values from the database. We can see all the weather values in this file. The index.php file reads only the last value and shows it on the web application. So the temperature and humidity that are shown on the homepage of the application are the ending value of the database that is stored by the DHT11 sensor. Now when the attacker logs in to the app with the session id, he can browse the files till the session is valid. To protect the weather data from the attacker, we have encrypted the weather value in the readall.php file using the AES algorithm. As a result, the attacker can only see the encrypted values.

Finally, on the home page of our web application, there are temperature and humidity values, date, and log out option on the front side. Then we can choose different rooms of our smart home to control and monitor the devices.

We prefer session-id for improving the security of our web application than JWT (Java Web Token). JWT consists of three parts where session-id consists of the only session key. So if we store session id in a cookie the total size is Six bytes. If we store the id in JWT the aggregate content is 304 byte. As a result, the size of the token would become problematic because along with each request to the server we must include the JWT [1] A session is also more reliable because the only thing stored on the client is a session key. The actual data remains on the server, whereas in the term of JWT, the user information is stored in the payload.

Session id does not need to be encrypted as It is already a signed value. But JWT needs to be encrypted as it carries user information [2].

In [3] paper, the session-id is encrypted. But as session-id already a signed value so encrypted session id cannot play a meaningful role where session regeneration can be a goof reliable. Insecure session.

14 Our Proposed Scheme

Attacker cannot access the user creden-tials and session hi-jacking is prevented.

Maintenance cost and the unnecessary ports can not be blocked

15 VI. Future Work and Limitations

In doing this thesis study, we have found some limitations. We also have bounded time, so we have to pause our work for some time and will have to do in the near future with more research and study. a) Future Work

16 Use Encrypted Communication

We will try to use a TSL certificate to make our communi-cation encrypted and more secure.

17 Two-factor authentication

We will try to use email and SMS service in Twofactor authentication regard.

18 Android Application

Discussed earlier, we have developed a webbased app for our smart home. We will try our best to add more features in this work, such as to develop a mobile application to control the smart home.

Till now, we have developed the control of appliances only for the living room of our smart home. In the future, we will complete the whole smart home.

19 b) Limitations

20 Maintenance Cost of Server

We have used the server as an ordinary user. But some days later, we were unable to work on that as there needed a premium account for further work. That's why we were unable to provide more security features for our smart home.

21 Database encryption

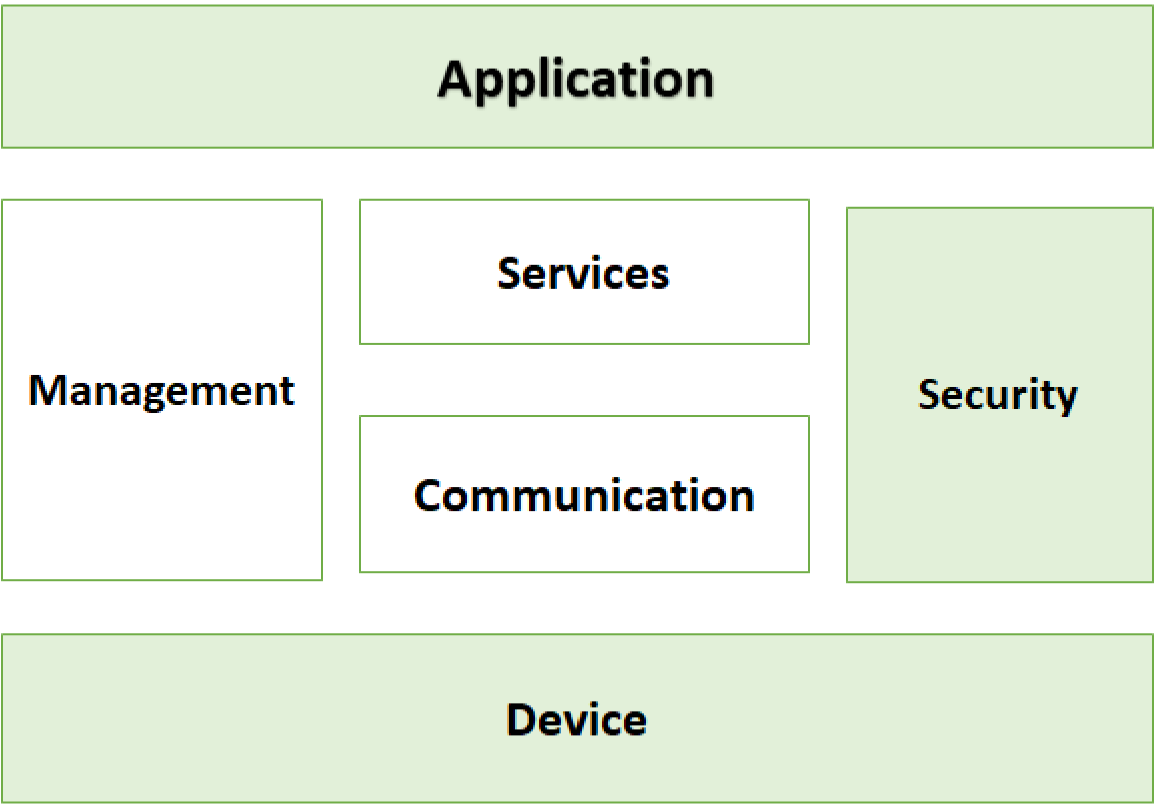
As at last, we have to use the server an usual user, we cannot use the encryption function in the database.

22 Block unnecessary ports

As we were unable to use the proper database so we cannot block unnecessary ports.

23 VII. Conclusion

The rising technology Internet of Things is changing lives by connecting limitless devices. In the near future, IoT has a remarkable effect. There will be a net of IoT connecting worldwide devices. It will bring the nations closer. It will help to connect people and get information anytime and anywhere in the world. Home is one of the most important things for human beings. It should be confirmed with security at all times. The development of IoT has penetrated various areas of life, one of the applications is the smart home system. A Smart home is built to provide convenience and comfort to residents in the management of their homes. Also, this system can also be a solution in an energy-saving effort at home. Some essential things that need to be designed in a smart home system are communication protocols, network security, as well as databases. In addition, the database in My SQL can also be managed perfectly and always in sync with every process that is being run. This paper puts the light on a smart home with security regarding IoT. b We are exploring Applications, and here we also are working for additional insights. [1] [2]



12

Figure 1: Fig. 1 :Fig. 2 :

[1] © 2020 Global Journals

[2] © 2020 Global JournalsA Secure Framework for IoT Smart Home by Resolving Session Hijacking

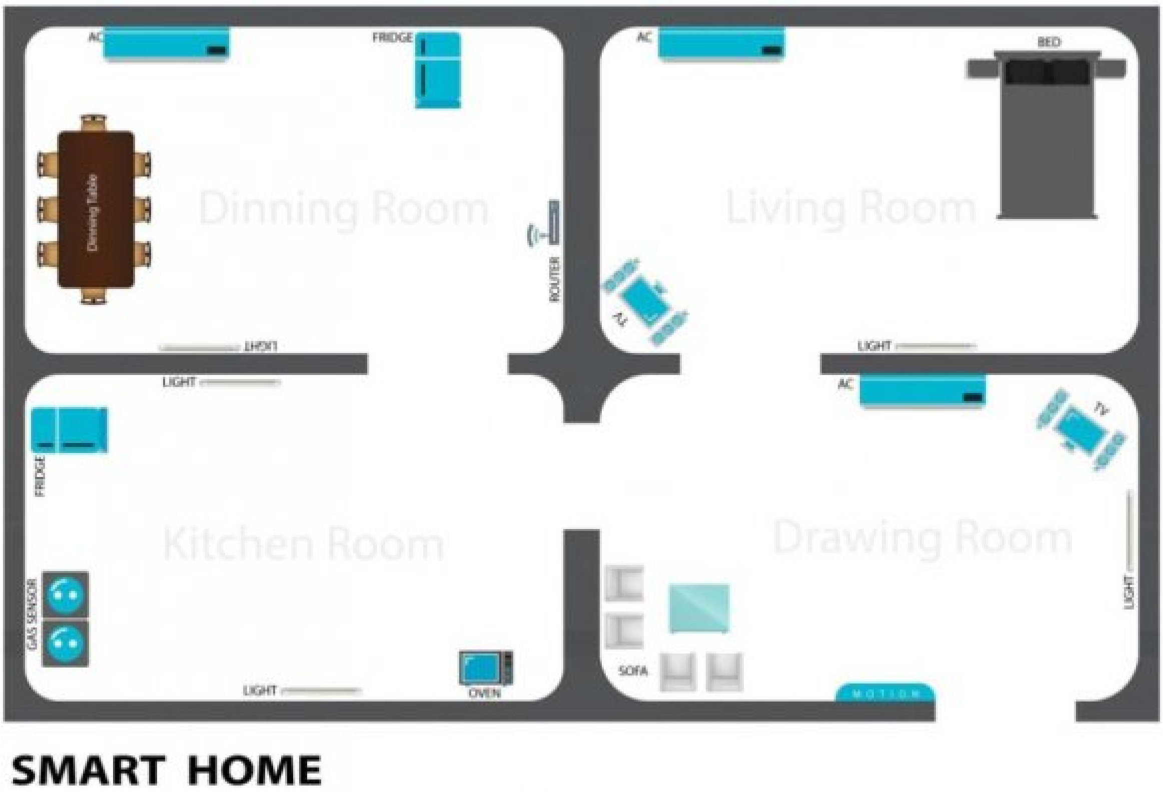
5 

Figure 2: Fig. 5 :

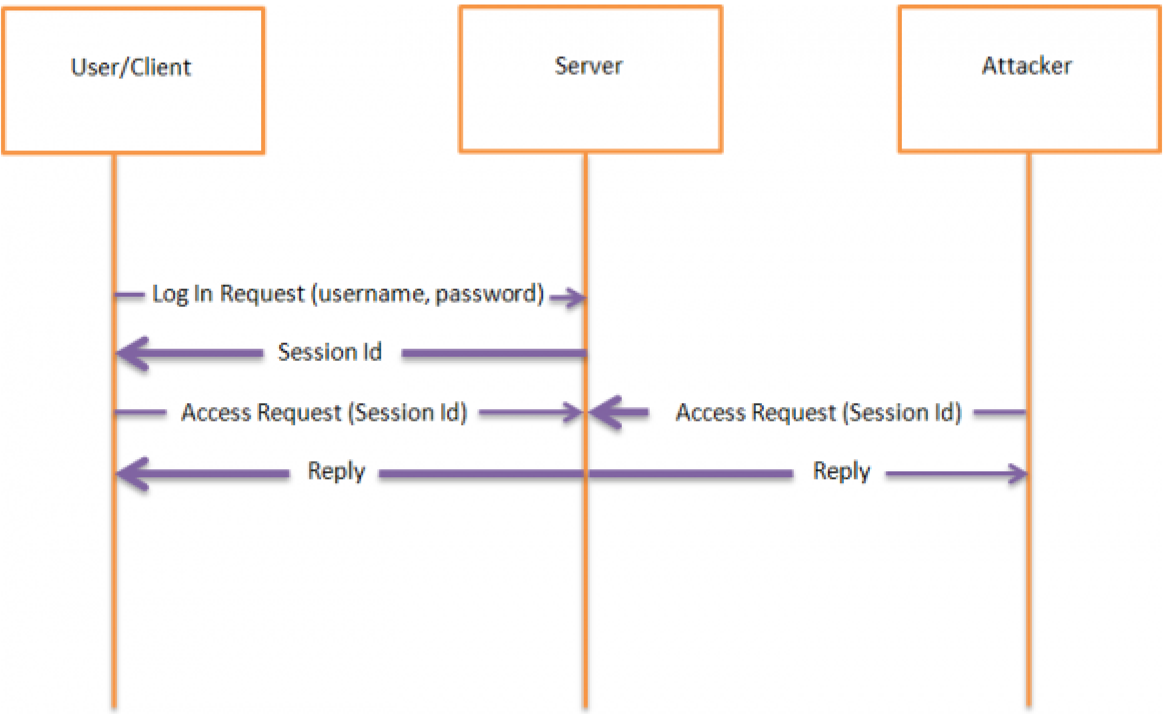
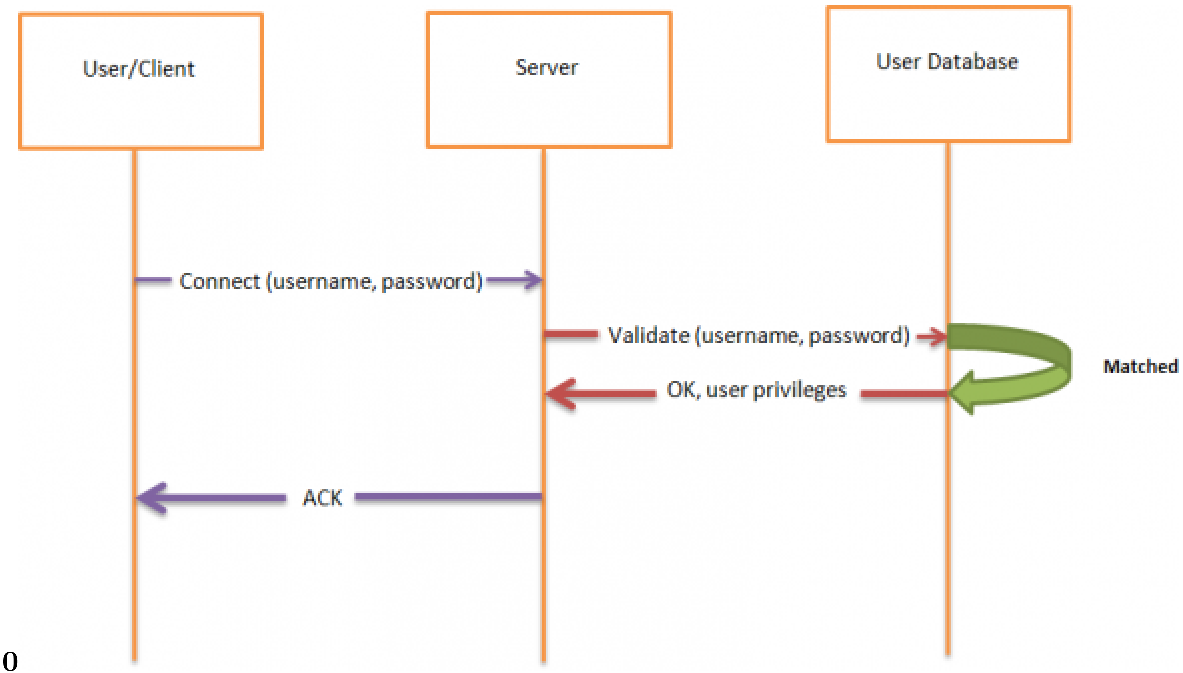
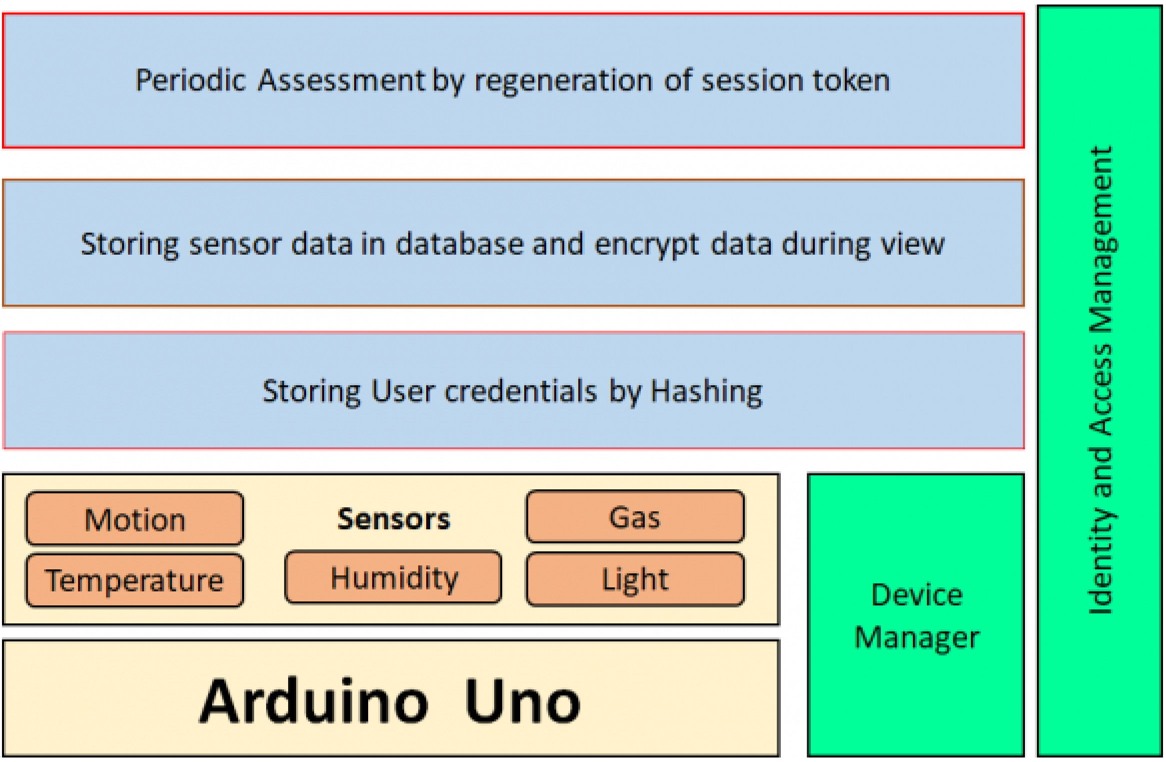
6 
User/Client
Server
Attacker
Log In Request (username, password)
Session Id
Access Request (Session Id)
Access Request (Session Id)
Reply
Reply

Figure 3: Fig. 6 :



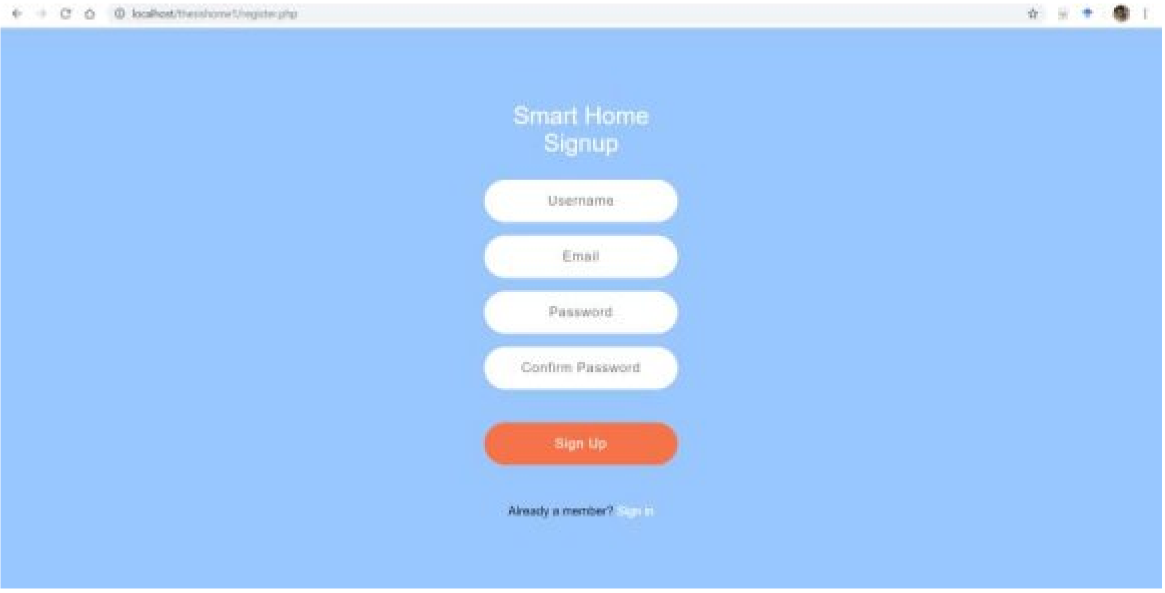
7910

Figure 4: Fig. 7 :Fig. 9 :Fig. 10 :


Periodic Assessment by regeneration of session token
Storing sensor data in database and encrypt data during view
Storing User credentials by Hashing
Motion
Sensors
Gas
Temperature
Humidity
Light
Arduino Uno
Device Manager
Identity and Access Management

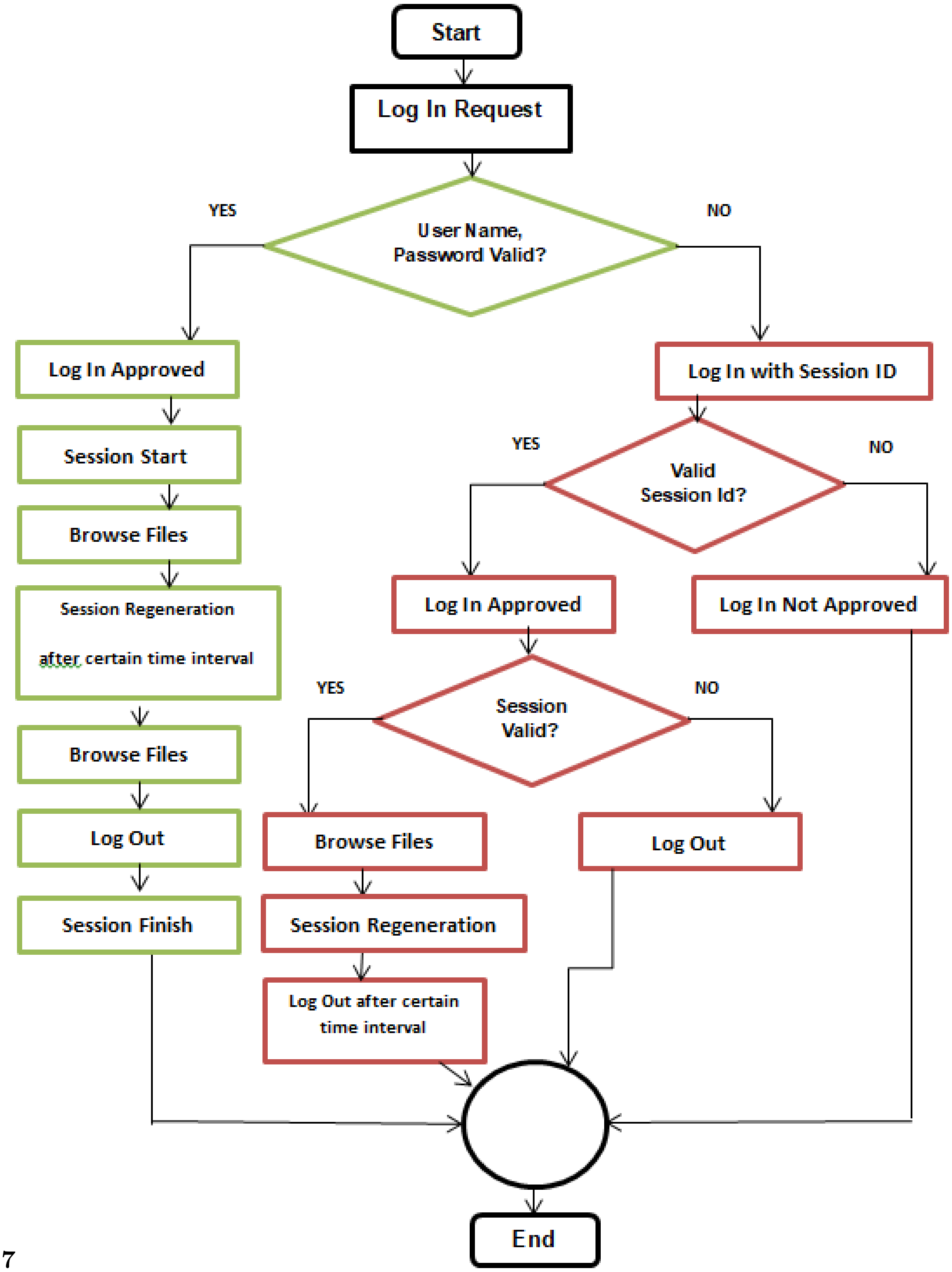
11

Figure 5: Fig. 11 :



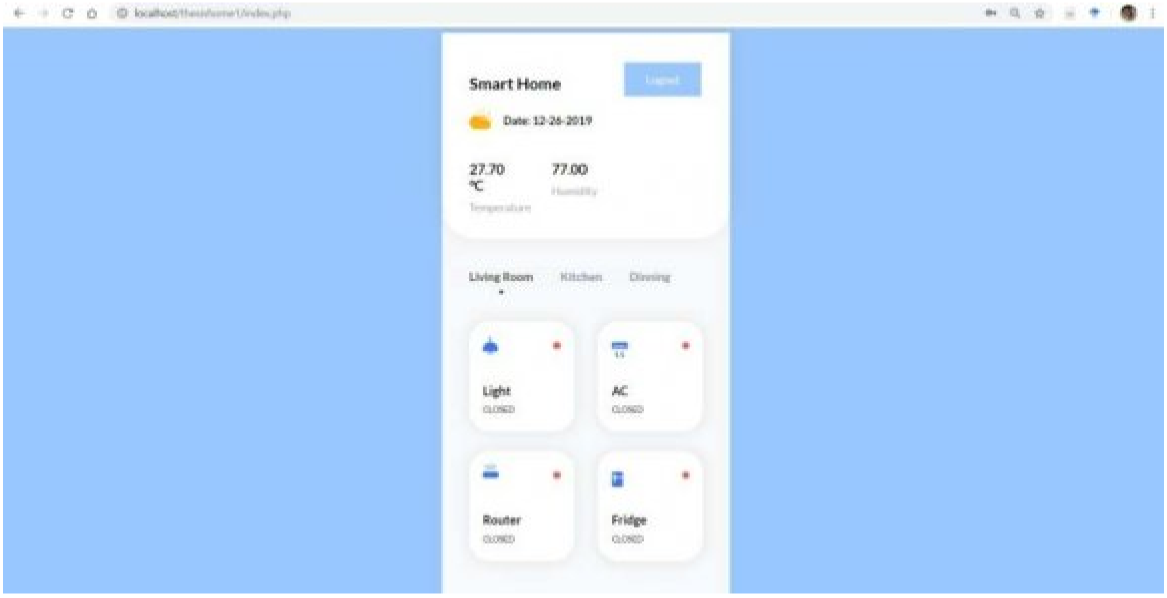
14

Figure 6: Fig. 14 :



17

Figure 7: Fig. 17 :



Smart Home

Date: 12-26-2019

27.70 °C Temperature

77.00 Humidity

Light CLOSED

AC CLOSED

Router CLOSED

Fridge CLOSED

Figure 8:

1

Applications	Popularity	Twitter search	Google search
Smart Home	100	3.3k	61k
Wearables	63	2k	33k
Smart City	34	0.5k	41k
Smart Grid	28	01.k	41k
Industrial Intranet	25	1.7k	10k
Connected Car	19	1.2k	5k
Connected Health	6	0.5k	2k
Small Retail	2	0.2k	1k
Smart Supply Chain	2	0.2k	0k
Smart Farming	1	0.0K	1k

Figure 9: Table 1 :

2

	of Web Application Vulnerabilities [3]	
S.No.	Vulnerability	Percentage
1	SQL Injection	30
2	Session Hijacking	28
3	Cross-site scripting	18
4	Distributed DoS attack	8
5	Phishing attack	8
6	Cloning attack	4
7	Others	4

Figure 10: Table 2 :

III

Approach	Description	Tools
A Prevention Model for Session Hijack At-tacks in Wireless Net-works Using Strong and Encrypted Ses-sion ID [3]	Session-id is Encrypted and decrypted between the server and the client	AES, RSA, SKS algorithm
JSON Web Token (JWT) based client authentication in Message Queuing Telemetry Transport (MQTT) [4]	JSON Web Token is Exchanged between broker and client	TLS, MQTT protocol
Design of Database And Secure Communication Protocols for Internet of Things based Smart Home System Trio Adorno [5]	The communication is encrypted with both AES and RSA. The database is used to store the data.	AES,RSA algorithm, MYSQL.
Our Proposed Scheme	Session fixation and encrypted data.	AES algorithm, PHP, MD5 hash function, MYSQL

Figure 11: Table III :

IV

	A Secure Framework for IoT Smart Home by Resolving Session Hijacking		
Year 2 020 16 Volume XX Issue II Version I ( ) G			
Global Journal of Computer Science and Technology	Approach A Prevention Model for Session Hijack At-tacks in Wireless Net-works Using Strong and Encrypted Ses-sion ID [3] JSON Web Token (JWT) based client authentication in Message Queuing Telemetry Transport (MQTT) [4] Design of Database based Smart Home and Secure Communication Protocols for Internet of Things	Advantage The attacker cannot know the session id Encrypted communication Encrypted Communication.	Disadvantage Session Id is already a signed value which needs not to be encrypted User information is stored in JWT
	System Trio Adiono [5]		
© 2020 Global Journals			

Figure 12: Table IV :

.1 Acknowledgment

The fulfillment of this undertaking could not have been possible without the participation and assistance of so many people whose names may not all be enumerated. Their contri-butions are sincerely appreciated and gratefully acknowledged. We are thankful to our supervisor Md Bayazid Rahman. We are also grateful to A.H.M Saiful Islam (Chairman, Department of Computer Science and Engineering), Dr. Fernaz Narin Nur and the respected faculty of Computer Science and Engineering, Notre Dame University Bangladesh for their guidance in our work.

To all relatives, friends, and others who in one way or another shared their support, either morally, financially and physically, thank you.

Above all, to the Great Almighty, the author of knowledge and wisdom for giving countess blessings.

[Jan and Ahmad ()] ‘A payload-based mutual authentication scheme for Internet of Things’. Mian Jan , Ahmad . *Future Generation Computer Systems* 2019. 92 p. .

[Manivannan and Sathiyamoorthy ()] ‘A prevention model for session hijack attacks in wireless networks using strong and encrypted session ID’. S S Manivannan , E Sathiyamoorthy . *cybernetics and information technologies* 2014. 14 p. .

[Manivannan and Sathiyamoorthy ()] ‘A prevention model for session hijack attacks in wireless networks using strong and encrypted session ID’. S S Manivannan , E Sathiyamoorthy . *cybernetics and information technologies* 2014. 14 p. .

[Shingala ()] *An alternative to the Public Key Infrastructure for the Internet of Things*, Krishna Shingala . 2019. NTNU. (MS thesis)

[Solapurkar ()] ‘Building secure healthcare services using OAuth and JSON web token in IOT cloud scenario’. Prajakta Solapurkar . *2nd International Conference on Contemporary Computing and Informatics (IC3I)*, 2016. 2016. IEEE.

[Adiono ()] *Design of database and secure communication protocols for internet-of-thingsbased smart home system*, Trio Adiono . 2017.

[Karimi and Krit ()] *Internet of Thing for Smart Home System Using Web Services and Android Application*, Khaoula Karimi , Salahddine Krit . 2019. Singapore: Springer. p. . (Smart Network Inspired Paradigm and Approaches in IoT Applications)

[Hamdan ()] ‘IoT-based interactive dual mode smart home automation’. Omar Hamdan . *IEEE International Conference on Consumer Elec-tronics (ICCE)*, 2019. 2019. IEEE.

[Shingala ()] *JSON Web Token (JWT) based client authentication in Message Queuing Telemetry Transport (MQTT)*, Krishna Shingala . arXiv:1903.02895. 2019. (arXiv preprint)

[Woods ()] *School of Computing Information Engineering*, Derek Woods . 2018.

[Kumar et al. ()] *SECURITY ISSUES AND APPLI-CATIONS OF INTERNET OF THINGS*, Kumar , Farooq , Sunar . 2019. 6 p. .