IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 3, March 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

[| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203129 |

False Data Injection Attack Prevention

Samanvitha H S, Vidyashree A L, Saptami V, Sanjay D N, Dr. Ramesh B

Student, Department of Computer Science and Engineering, Malnad College of Engineering, Hassan, India

Student, Department of Computer Science and Engineering, Malnad College of Engineering, Hassan, India

Student, Department of Computer Science and Engineering, Malnad College of Engineering, Hassan, India

Student, Department of Computer Science and Engineering, Malnad College of Engineering, Hassan, India

Professor, Department of Computer Science and Engineering, Malnad College of Engineering, Hassan, India

ABSTRACT: The report contains design and implementation of security protocol for IOT system. The user will send a registration request to authority node. If the sent request is a valid one, the authority node will approve the request by generating a digital certificate and multiple keys. The certificate is stored in cloud database. The user will check the status and is allowed to download certificate and keys. After registration, the user will send a control request to authority node. The authority node checks the sent certificate with stored certificate, if both matches admin will grant permission to user for accessing IOT system.

KEYWORDS*:* FDI attack, admin console, user console, authentication.

I. INTRODUCTION

The Internet of Things is a system of interrelated computing device, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human to human or human to computer interaction. The Internet Of Things is the network of physical objects or "things" embedded with electronics, software, sensors and network connectivity, which enables these objects to collect and exchange data.

The IOT allows object to be sensed or controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based system and resulting in improved efficiency accuracy and economic benefit in addition to reduced human intervention. When IOT is augmented with sensors and actuators, the technology became an instance of the more general class of cyber-physical system, which also encompasses technologies such as smart grids, virtual power plant, smart home, intelligent transportation and smart cities.

IOT has evolved from the convergence of wireless technologies, micro-electromechanical system (MEMS), micro services and the internet. The convergence has helped tear down the silo walls between operational technologies (OT) and information technology (IT), allowing unstructured machine-generated data to be analysed for insight that will drive improvements. Practical application of IOT technology can be found in many industries today, including precision agriculture, building management, healthcare, energy and transportation.

The concept of the internet of things became popular through the auto-2D centre, radio frequency identification (RFID) as a prerequisite for internet of things at that point. If all objects and people in daily life were equipped with identifiers, computer could manage and store them.

II. APPLICATIONS OF IOT

The applications for internet connected devices are extensive. Multiple categorizations have been suggested, most of which agree on a separation between consumer, enterprise (business), and infrastructure applications.

The ability to network embedded devices with limited CPU, memory and power resources means that IOT finds applications in nearly every field. Such systems could be in charge of collecting information in settings ranging from natural ecosystems to buildings and factories, thereby finding applications in fields of environmental sensing and urban planning.

IOT has many applications such as consumer application, smart home, enterprise, media, infrastructure management, manufacturing, agriculture, energy management, environment monitoring, building and home automation, metropolitan scale deployments.

[| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203129 |

III. EXISTING SYSTEM

Although many protocols for the Internet have been put forward, it is still not enough to meet the increasingly complex requirements from applications. Many of them are not efficient enough to adapt the device diversity and timely communication environment. Nowadays, network connects people, data, processes and things; standardized ultra-low power devices with wireless technologies, including Wi-Fi, RFID.
As time passes, powerful embedded devices such as smart phones and tablets will occupy the great part of the IOT. The different devices not only bring various applications, but limitations in terms of reliability, information leakage, privacy and security issues. Another issue is limited hardware resources and energy. It makes difficult to implement complex security protocols in order protect the system and the information.

A. LIMITATIONS

- Less Reliable
- Lack of security
- Privacy issues
- Information are not safe guarded.

B. Aim and Objective

The major aim of the project is to provide an efficient security protocol for the embedded systems or platforms severing the Internet of Things. And also, to promote the development of the Internet Of Things.
The objective is to develop a system which will not only cover the integrity of messages, but also the authentication of each user by providing an efficient authentication mechanism.

C. Literature Survey

1. Proposing Secure and Lightweight Authentication scheme for IoT Based E-Health Applications: Instead of individual nodes registering with the IoT gateway head node is assigned through which the registration and Authentication process is done. If the head node is compromised than it will lead to security breaches.[1]

2. Secure-Anonymous User Authentication Scheme for e-Healthcare Application Using Wireless Medical Sensor Networks: The patient an medical expert registrations should be done in prior, then using a Smart card followed by set of predefined protocols
the medical expert will be able to access the patient data. ECC algorithm is used for Encryption. Needs smart cards and smart card readers increases the production cost and if smart card is misplaced than may lead to intruder attacks.[2]

3. A secure and lightweight authentication scheme for next generation IoT Infrastructure: A smart card-based authentication is used for pre-registered users and server. Also, time stamps are used to validate authentic or non-authentic users. Needs smart cards and smart card readers increases the production cost and if smart card is misplaced than may lead to intruder attacks.[3]

4. A lightweight remote user authentication scheme for IoT communication using elliptic curve cryptography: A payload-based encryption mechanism is used along with 4-way handshaking mechanism for authentication. Additionally, system uses offline provisioning phase which generates look-up table required for handshaking. If the look-up table at the server is modified by the intruder it will lead to security failure.[4]

5. Secure and Efficient Authentication Scheme in IoT Environments: A novel lightweight and secure architecture are proposed that uses crypto-modules, which optimize the usage of one-way hash functions, elliptic-curve cryptography, and an exclusive-or operation using informal security analysis. The performance and the implementation time is quite high compared to other lightweight models.[5]

6. A Robust, Low-Cost and Secure Authentication Scheme for IoT Application: A low-cost authentication protocol for IoT edge devices that exploits power-up states of built-in SRAM for device fingerprint generations. Unclonable ID generated from the on-chip SRAM could be unreliable, and to circumvent this issue, a novel ID matching scheme is proposed that alleviates the need for enhancing the reliability of the IDs generated from on-chip SRAMs. The bits generated from an SRAM may be unstable and create different IDs for the same device. Error correction codes needed to be used to increase the reliability of the SRAM-PUF response.[6]

D. DESIGN

The project concentrates on the design of a Security Protocol for the IOT and the implementation of the corresponding Security Protocol on the Sensible Things Platform. The Security Protocols will not only cover the integrity of the message, but also the authentication of each user by providing an efficient authentication mechanism. The

[| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203129 |

functioning laboratory Prototype of the Secured Communication implemented on Sensible Things Platform is introduced. The Sensible Things platform is a open source platform for creating efficient and fast internet things applications. It is a common Platform for communications between sensors and actuators on global Scale and enables a widespread Proliferation of IOT Services. This secure communication provides more efficient information for transmission mechanism.

Security Protocol

The Security Protocol involves:

- Registration process
- Approval process
- Certificate Generation
- Certificate Sharing
- Request to control
- Control to access

Registration Request Process

The Registration Request Process carried out between the recently joined User and Authority Node (AN). The Registration Request Process is carried out between User and Admin. The user will send a request to admin, in which all user information such as, Username, Mac ID, IP address, Machine name, Date and Time will be auto fetched and filled into registration form and the request is sent to admin. The registration form is in read-only method, no intruder can edit the user information.

Approval Process

During approval process, the registration request details are stored in cloud database and this request will be waiting for Admin approval. The admin will take-up the request from the cloud database, if it is valid request the admin will approve the request otherwise the request is deleted.

Certificate Generation and Sharing

The admin will take up the combination of user information that is username, Mac ID, IP address, machine name and is given to SHA. This algorithm generates a cipher text and is used to generate a digital certificate. The private and public keys are generated by RSA.

The user will have an option of checking his approval status. If the request is approved by admin, he can download a certificate and a private key from cloud data base.

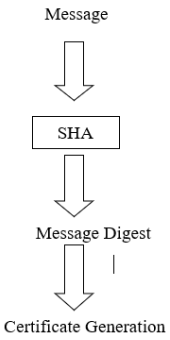

Figure 1. Generation of Certificate using SHA

Request to control

The user will send a request to admin along with certificate. The cloud server will compare the send certificate with stored certificate to verify whether the request is from the same user or not. If both certificate matches it will generate OTP, encrypted by public key and is send to user. User will decrypt this token by private key and he will send the OTP. If both OTP are same, admin will generate a session key and is given to user.

Control to Access

The user will send a request and session key to IOT system. As long as the session key exists, the user can control the IOT. Once the session key expires, he has to send a request again.

[| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203129 |

High Level Design

High Level Design (HLD) is over all system design covering the System architecture and database design. It describes relation between various modules and functions of the system. Data flow, flow chart and data structures are covered under HLD.

Data Flow Diagram (DFD)

Data flow diagrams show how data is processed at different stages in the system. Data flow models are used to show how data flows through a sequence of processing steps. The data is transformed at each step before moving on to the next stage. These processing steps of transformations are program functions when data flow diagrams are used to document a software design.

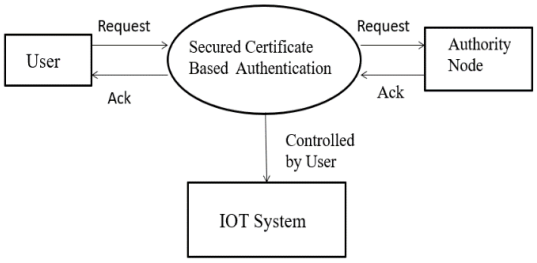

Figure 2. DFD for Secured Authentication

The communication is between User and Authority Node. User sends a request to the admin using the secured certificate based authentication. Admin checks the requested user is a valid or not. If the requested user is valid, admin sends acknowledge to the user. If user wants to control the IOT system and user will send the request to admin, the admin will check and grant the permission to the user to access the IOT system.

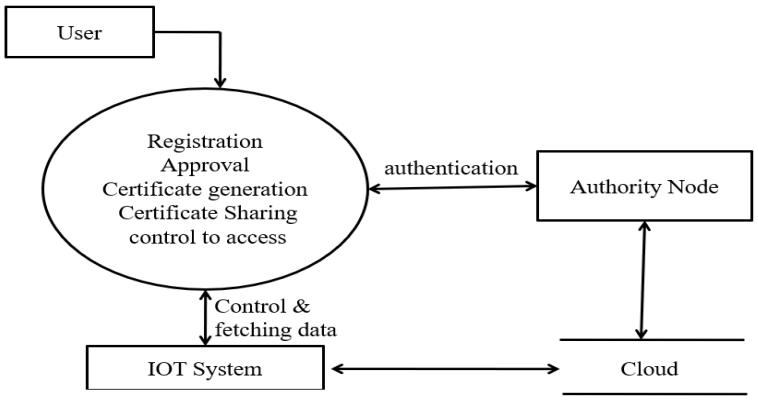

Figure 3. DFD for Secured Authentication

Flow Chart

A flowchart is a common type of chart, which represents an algorithm or process, showing the steps as boxes of various kinds, and their order by connecting these with arrows. Flowcharts are used in analysing, designing, documenting or managing a process or program in various fields.

There are many different types of flow charts on the one hand there are different types for different users, Such as Analysts, Designers, Engineers, Manager or Programmer on the other hand those flowcharts can be represent different types of objects.

Four general types of flowcharts

- Document flow chat, showing a document flow through system.
- Data flow chat, showing a data flow in a system.
- System flow chat, showing control at a physical or resource level.
- Program flow chat, showing the control in a program within a system.

[| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203129 |

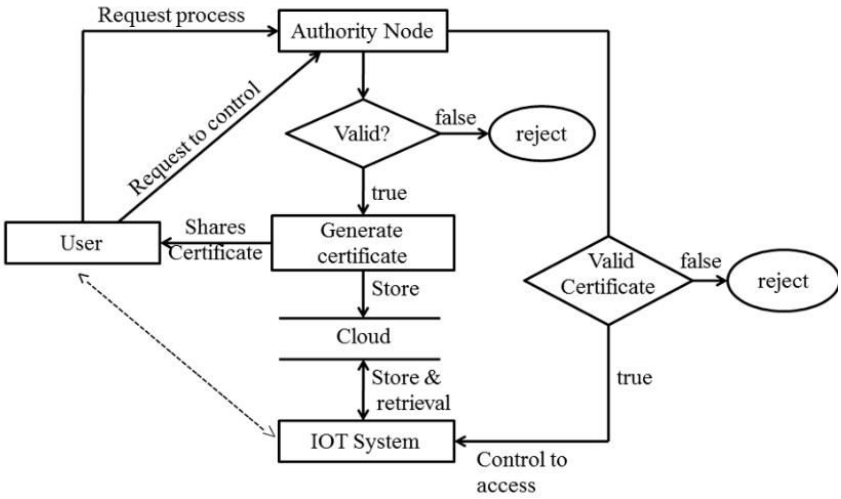

Figure 4. Flow Diagram for Secured Authentication.

Low Level Design (LLD)

Low Level Design is a component level design process that flows a step-by-step refinement process. This process can used for design data structure, required software architecture, Source code and performance.

Sequence Diagram

A sequence diagram shows object interactions arranged in time sequence. It depicts the objects and classes involved in the scenario and the sequence of messages exchanged between the objects needed to carry out the functionality of the scenario.

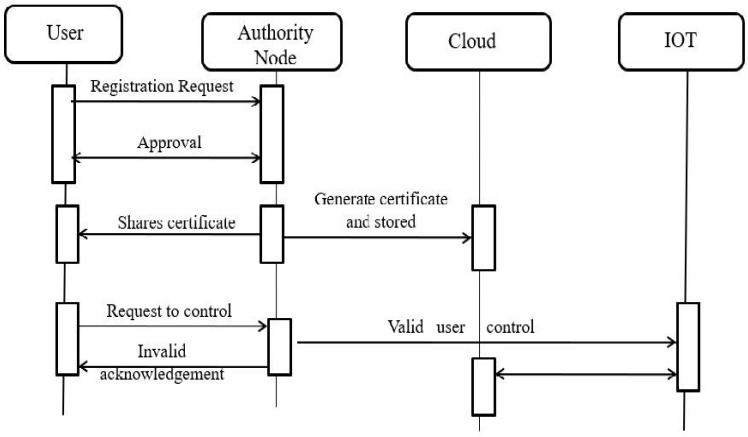

Figure 5. Sequence diagram of Secured Authentication.

Use Case Diagram

A use case diagram at its simplest is a representation of a user's interaction with the system that shows the relationship between the user and the different use cases in which the user is involved.

[| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203129 |

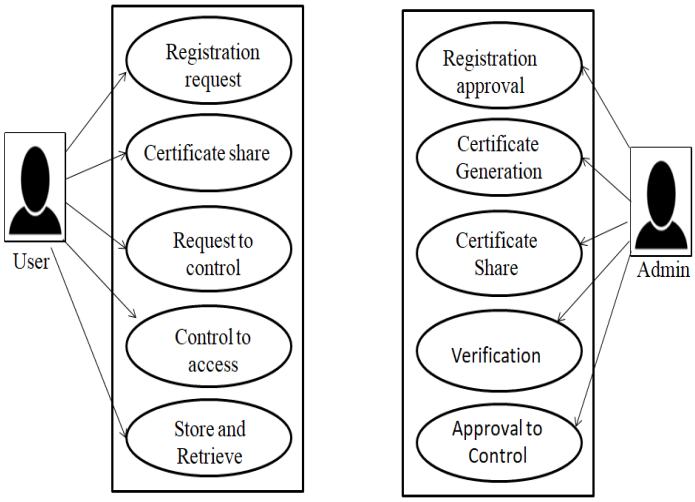

Figure 6. Use Case Diagram of User and Admin.

Software testing is performed to verify that the completed software package functions according to the expectations defined by the requirements/specifications. The overall objective is not to find every software bug that exists, but to uncover situations that could negatively impact the customer, usability and/or maintainability.
Verification and validation is a generic name given to checking processes, which ensures that the software confirms to its specification and meets the demand of its users.

IV. RESULTS

Figure 7. Main Menu

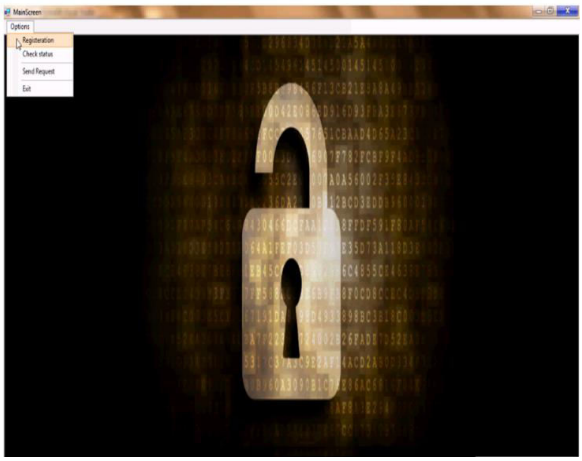

Figure 8. Main Menu of Client

The above snapshot 7 describes the Introduction Screen for the Main Menu of the Internet Of Things. The Internet of Things (IOT) is the network of physical objects or "things" embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data.

The above snapshot 8 describes Client Main Menu form which contains options like registration, check status, send request and exit. These options can be used to process the operations. Initially Registration is the first process used in user screen. Sequentially remaining operations will be processed.

[| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203129 |

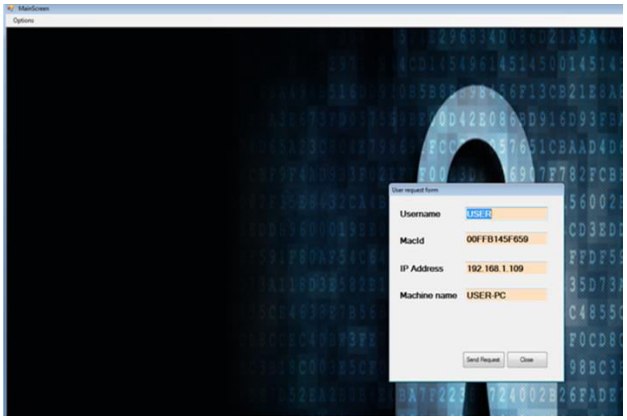

Figure 9. User Request Form

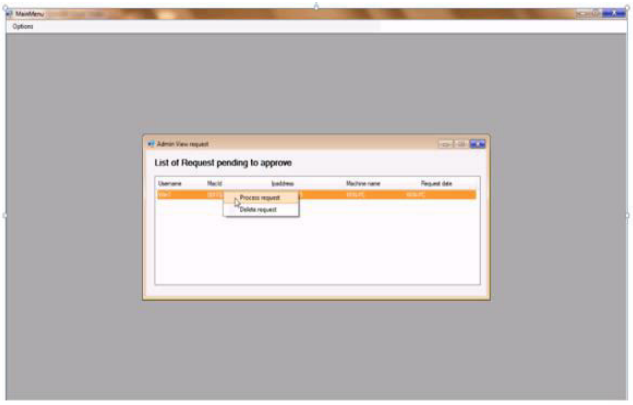

Figure 10. Approval Process

The above snapshot 9 describes the User Registration Request Form containing attributes (username, Mac ID, IP address, machine name and date time) and Radio buttons (send request and close). The user information is auto fetched from the system and sends the request to the admin. The message will be displayed as "Your request submitted successfully, please wait until approved". And can close the form.

The above snapshot 10 describes the Main Menu for Approval Process. The attributes of the user process which are auto filled are displayed in the screen. The approval process consists of two options such as process request and delete request. The request can be processed otherwise it can be deleted. The delete request is used when the public common IP is used.

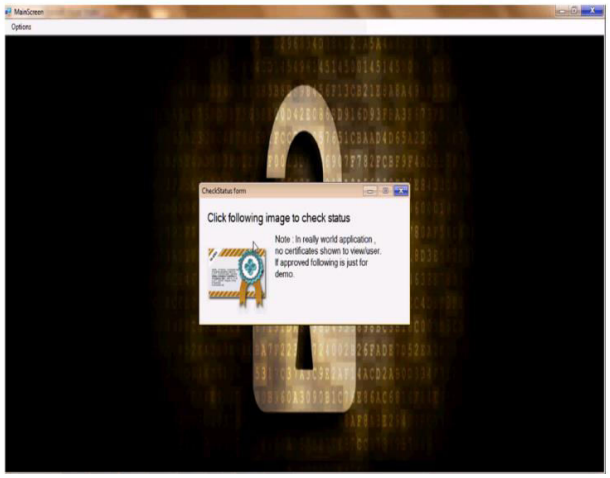

Figure 11. Check Status

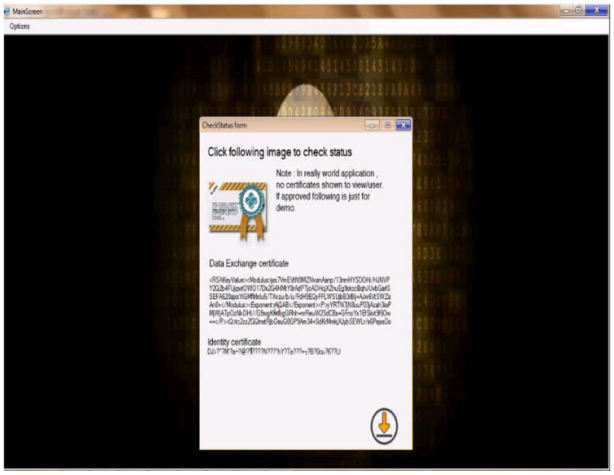

Figure 12. Certificate Download

The above snapshot 11 describes the User Check Status Form. The user has already requested and to know the status of user request the above screen is used. It has an option called as "Click following image to check status". If the request is approved then the message will be displayed as "Download Certificate" or if the request is not approved then the message will be as "Not Approved."

The above snapshot 12 describes Certificate Download Form with a download option. The downloaded certificate will be in the form of cipher text and the message will be displayed as "Private Key Downloaded Successfully".

[| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203129 |

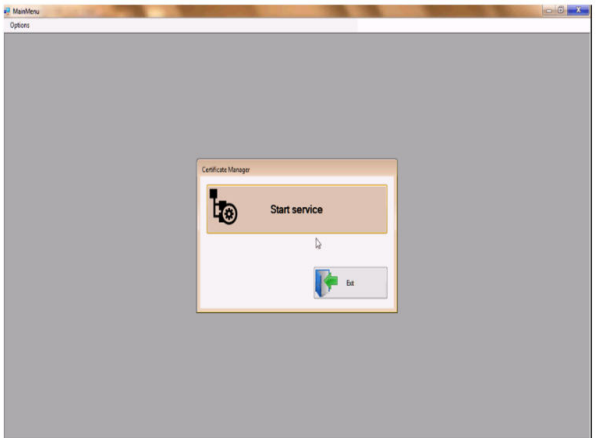

Figure 13. Certificate Manager

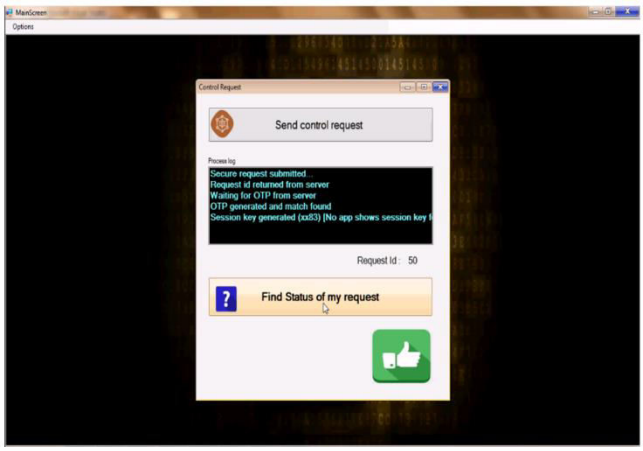

Figure 14. Request to Control

The above snapshot 13 describes Service Manager Interface. The only two options are start and stop service. When the service starts it will be always running on back ground and waits for any request to come from client.

The above snapshot 14 describes Control Request Form. When the control request is clicked internally the request is submitted, the request will be handled by service manager. The request will be accepted by server and generates all certificate matching and checks whether approved or not. Once everything is done an OTP is generated and also it is examined in background. When the user check the status of his/her request a session key is generated with Request Id to control the IOT device.

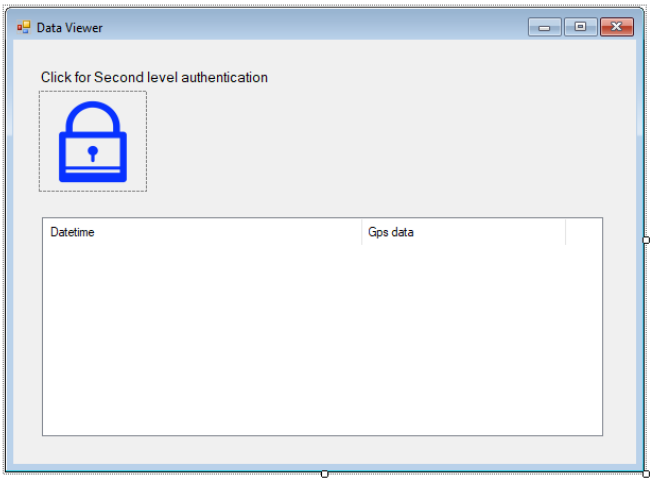

Figure 15. IOT Data viewer Screen

The above snapshot 15 describes Environment Control Panel. When the admin grant the permission to access the IOT the control screen will be displayed to view GPS data along with date time.

REFERENCES

[1] G[1] Paul Brous, Marijn Janssen, and Paulien Herder. The dual effects of the internet of things (iot): A systematic review of the benefits and risks of iot adoption by organizations. International Journal of Information Management, 51:101952, 2020.

[2] In Lee and Kyoochun Lee. The internet of things (iot): Applications, investments, and challenges for enterprises. Business horizons, 58(4):431–440, 2015.

[3] Mohiuddin Ahmed and Al-Sakib Khan Pathan. False data injection attack (fdia): an overview and new metrics for fair evaluation of its countermeasure. Complex Adaptive Systems Modeling, 8(1):1–14, 2020.

[| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203129 |

[4] Shamneesh Sharma, Manoj Manuja, and Keshav Kishore. Vulnerabilities, attacks and their mitigation: An implementation on internet of things (iot). Int. J. Innov. Technol.Explor. Eng, 8(10):146–150, 2019.

[5] Murat Kuzlu, Corinne Fair, and Ozgur Guler. Role of artificial intelligence in the internet of things (iot) cybersecurity. Discover Internet of things, 1:1–14, 2021.

[6] Willian A Dimitrov and Galina S Panayotova. The impacts of dns protocol security weaknesses. J. Commun., 15(10):722–728, 2020.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details