WINTER SEMESTER 2022-23

CSE 3502-Information Security Object

Slot : F1

Secure Communication For Smart IOT Objects

Submitted By

Arayan Katraria:20BCE0658

Akshat Jain:20BCE0675

Vishal Jain:20BCE0682

Submitted To

Prof. Murali S

School of Computer Science and Engineering

VIT, Vellore

VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

Index:

1. Abstract

The novelty of our project is to have secure channels of communication between IoT devices with one another and server or a router. There is a developing number of IoT gadgets and applications, and this prompts an expansion in the number and unpredictability of pernicious assaults. It is important to secure IoT systems against pernicious assaults, particularly to keep attackers from getting command over the gadgets. An enormous number of security research answers for IoT have been proposed in the most recent years, however the greater part of them is not standardized or interoperable. As the internet of things keeps on growing, the variety and multifaceted nature of IoT applications increments, such networks are defenseless against assaults that intend to take touchy information, assume responsibility for gadgets and disturb administrations. Numerous conventions and networking stacks for IoT have been created, some of them are standardized, and give interoperability among gadgets and availability over the web. They have been indicated by normalization bodies for example, IETF and IEEE or by industry coalitions, such likewise Rawan coalition and string gathering.

Smart-home IoT systems are growing in popularity thanks to their efficient functionality, be making many menial tasks easy. On the opposite hand, these smart home IoT devices becomes Vulnerable points of our privacy. Privacy of non-public data is usually a topmost priority of E-services. To tackle this pain point, we have used industry standard encryption algorithms for creating and using Secure channels for communication between IoT devices by Socket Programming.

2. Introduction

Our daily lives have significantly benefited from the Internet of Things (IoT), which offers several advantages like convenience, effectiveness, and better decision-making. The Internet of Things (IoT) is a huge network of interconnected sensors, systems, and devices that gather and transmit data to servers for management, analysis, and utilization. This information offers useful insights that can be applied to streamline processes, cut expenses, and raise standard of living in general.

But as IoT devices proliferate, security has grown to be a major worry. Smart gadgets are a common target for cybercriminals since they are simple to infiltrate and manipulate. As a result, for the IoT, security and privacy are essential, and assuring the accuracy of the data acquired is key. Knowledge analysis results are unreliable if the data has been manipulated with, which might have serious repercussions.

To guarantee the privacy, accuracy, and availability of the data, specific security issues posed by the IoT must be resolved. The sheer quantity of connected devices, each with unique security flaws, is a major obstacle. It is difficult to adequately monitor and safeguard all the gadgets due to their complexity.

Another issue is that many IoT devices have limited resources, which makes it challenging to deploy adequate security measures. Due to computational and power limitations, encryption, which is the best approach to protect communications, can be difficult to implement on low-resource devices.

Additionally, many IoT devices lack sufficient security protections in their design, making them prime targets for attackers. 98% of the 1.2 million IoT devices on corporate networks that Unit 42, a threat intelligence team, examined in a 2020 report did not have the ability to encrypt traffic. As a result, 57% of those IoT devices were susceptible to traffic manipulation and interception, among other things.

Establishing a secure authentication process is crucial to addressing the security issues posed by the IoT. Authentication is the process of confirming a user's or device's identity and ascertaining if they are authorized to access the system or data.

In the context of the IoT, authentication ensures that only authorized users can access the devices and data, preventing unauthorized access and data breaches. Therefore, it is crucial to develop a secure authentication system to guarantee the data's confidentiality and integrity.

In this project, we suggest using MongoDB for authentication needs and the SHA256 technique to hash passwords in order to prevent the database maintenance team from seeing the passwords in plain text. MongoDB is a document-oriented NoSQL database with strong scalability, flexibility, and security features. The SHA256 algorithm is a well-known cryptographic hash function that transforms an input (a password) into a fixed-size output (a hash) that cannot be undone.

We can make sure that only authorised people can access the IoT devices and data by using MongoDB authentication and SHA256 password hashing, and we can prevent the database administration team from seeing the passwords in plain text. By ensuring the data's confidentiality and integrity, this guards against hacker attacks and data breaches.

We first establish a MongoDB database to store the user credentials before implementing the suggested fix. The username and the password are then combined into a user collection using the SHA256 method. The system requires users to provide their credentials when they try to access it. The system then uses the SHA256 technique to hash the entered password and compare it to a previously stored hashed password in the database. The user is granted access to the system if the two hashes match.

3. Literature Survey

1. **A Secure and Intuitive IoT Architecture for Container Farm by Yun-Shuai Yu et al (2019)** proposed an IOT architecture to secure the communication between an open-source cloud platform and low-cost application development board. VPN tunnel, TLS 1.1, and TLS 1.2 along with other components were used to ensure secure message passing.

2. **Next Generation Lightweight Cryptography for Smart IoT Devices by Nilupulee A. Gunathilake et al (2019)** discussed the implementation, challenges, and futuristic applications of LWC Algorithm for smart IOT devices. Also, it describes LoRaWAN which is a communication protocol for low-power wide area network technologies.

3. **Secure Short-Packet Communications for Mission-Critical IoT Applications by Hui-Ming Wang et al (2019)** investigates the performance of secure short-packet communications in a mission-critical IoT system with an external multi-antenna eavesdropper. They first implemented it with a single AP and analysed the parameters, then later used these parameters to implement the same with MAP.

4. **Group-Based Key Exchange for Medical IoT Device-to-Device Communication (D2D) Combining Secret Sharing and Physical Layer Key Exchange by Uzma Mustafa and Nada Philip (2019)** presents a security design combining physical layer security technique with the cryptographic secret sharing approach. Also, a group key transfer protocol was proposed IoT D2D communication.

5. **IoT Node-Node Secure Communication Using RIPEMD-128 and DES by Quist-Aphetsi Kester et al (2019)** proposed that hybrid cryptographic algorithm and a hash function greatly enhanced the security for IoT node-node communications in a real time environment.

6. Blockchain Based Secure Communication for IoT Devices in Smart Cities by Ozgur Koray Sahingoz and Ramazan Yetis (2019) proposed an authorization system for IoT

devices which is implemented using the distributed node structure of Blockchain system and blocks kept in these nodes. And UDP protocol is used for communication.

7. **CKDAC: Cluster-Key Distribution and Access Control for Secure Communication in IoT by Padmashree M G et al (2020)** proposed a Cluster-Key Distribution and Access Control (CKDAC) for secure communication in IoT uses Publication Subscription architecture with the dynamic Cluster Head election to enhance the security and availability of the communicating IoT Devices. It outstands other traditional approaches.

8. **Machine learning and datamining methods for hybrid IoT intrusion detection by Abdellatif El Ghazi and Ait Moulay Rachid (2020)** proposed a hybrid IDS installed on the cloud powering another online and real time IDS on the fog to monitor the communication and detect attacks before it spreads. It is just a theoretical approach.

9. **Social Internet of Things: The collaboration of Social Network and Internet of Things and its Future by Dipraj et al (2020)** work aims to portray a plan for the Internet of things that consolidates the functionalities to facilitate things into relational association. The objectives being searched after by the SIoT perspective.

10. **Secure Communication Using Steganography in IoT Environment by M.I.M. Amjath and V. Senthooran (2020)** proposed a novel technique which encodes the secret data through QR code and embedded in low complexity cover images by applying image to image hiding fashion. It outstands the other available methods but works only images with .png extensions.

11. **SIC2: Securing Microcontroller Based IoT Devices with Low-cost Crypto Coprocessors by Bryan Pearson et al (2020)** proposed a framework termed Securing IoT with crypto coprocessors, for secure key provisioning that protects end users' private keys from both software attacks and untrustworthy manufacturers.

12. **MSIT: A Modified Lightweight Algorithm for Secure Internet of Things by Manoja Kumar Nayak and Prasanta Kumar Swain (2020)** modified a lightweight encryption and decryption algorithm called Modified Secure IoT (MSIT) for Secure data communication. This technique is secure and has less time complexity, but it increases the power consumption of the device leading to an unstable state.

13. **Enabling Secure RESTful Web Services in IoT using OpenStack by Zakaria Benomar et al (2020)** introduced an innovative approach for exposing services running on IoT devices to the Web so that they become reachable using globally resolvable Uniform Resource Locators. It uses HTTPS protocol for communication but failed to tackle with the vulnerabilities in the protocol.

14. **Secure Short-Packet Communications in Cognitive Internet of Things by Yong Chen et al (2020)** investigates the secrecy performance of short-packet communication in cognitive IoT wiretap networks. The accuracy of the proposed approximations was verified numerically.

15. **Multi-Access Edge Computing and Blockchain-based Secure Telehealth System Connected with 5G and IoT by Tharaka Hewa et al (2020)** propose a novel Multi-access Edge Computing (MEC) and blockchain based service architecture utilizing the lightweight ECQV (Elliptic Curve Qu-Vanstone) certificates for the real-time data privacy, integrity, and authentication.

16. **Transmit Power Minimization for Secure Short-packet Transmission in a Mission-Critical IoT Scenario by Hong Ren et al (2020)** proposed the resource allocation for a secure mission critical IoT communication system with URLLC, where the security capacity formula under finite block length is adopted.

17. **On the Security of IIoT Deployments: An Investigation of Secure Provisioning Solutions for OPC UA by FLORIAN KOHNHÄUSER et al (2021)** proposed an

investigation of contemporary and emerging secure device provisioning solutions for OPC UA, including an outlook into the future, based on solutions from the IoT domain.

18. **Survey on Delegated and Self-Contained Authorization Techniques in CPS and IoT by SREELAKSHMI VATTAPARAMBIL SUDARSAN et al (2021)** suggested authorization techniques with respect to two different contributions: general contributions and special contributions. He also proposed a high-level evaluation of access control models, including an analysis of the strengths and weaknesses of different approaches and access management standards based on our three-dimensional classification.

19. **Secured and High-Quality Steganography Using Intelligent Hybrid Optimization Algorithms for IoT by SACHIN DHAWAN et al (2021)**, IoT-based Secured and high-quality Steganography is proposed using hybrid algorithms for Big Data. Steganography technique is proposed for communicating secret data based on encryption. In this work, a grayscale image is used as a cover image.

20. **On the Security of a Secure and Lightweight Authentication Scheme for Next Generation IoT Infrastructure by ASHOK KUMAR DAS et al (2021)** proposed Rana et al.'s scheme and pointed out several security weaknesses like stolen smart card attack, privileged-insider attack, user impersonation attack, password change attack and ESL attack.

21. **Lightweight, Single-Clock-Cycle, Multilayer Cipher for Single-Channel IoT Communication: Design and Implementation by SHAHZAD MUZAFFAR et al (2021)** They proposed secure, single-channel communication system exploits the unique features of the ECS protocol and adds multiple layers of security to the transmission with low impact on ECS data rate and power performance.

22. **Secure ABE Scheme for Access Management in Blockchain-Based IoT by JIANSHENG ZHANG et al (2021)** by using KP-ABE scheme and blockchain technology, we design a secure access management scheme for IoT. In this new scheme,

KP-ABE implements fine-grained access control in IoT, and blockchain provides data security. Through the signature verification of blockchain, we realize the secure and reliable authentication of IoT devices, to ensure the communication security of devices in IoT.

23. **Secure Efficient Revocable Large Universe Multi-Authority Attribute-Based Encryption for Cloud-Aided IoT by KAIQING HUANG (2021)**, proposed an efficient revocable large universe multi-authority attribute-based encryption based on prime order bilinear groups. The proposed scheme supports user-attribute revocation.

24. **Design and Implementation of Trusted Sensing Framework for IoT Environment by Sungjin Park et al (2021)** designed and implemented the end-to-end trusted sensing framework for the IoT environment and showed the feasibility of our approach. Also evaluated and compared our framework with the hypervisor-based trusted sensing framework.

25. **Practical Identity Based Online/Off-Line Signcryption Scheme for Secure Communication in Internet of Things by VANKAMAMIDI SRINIVASA NARESH et al (2021)** An Identity based OOSC scheme was proposed, allows the IoT devices such as sensors, servers can communicate in a secured manner.

26. **A Lightweight and Secure IoT Remote Monitoring Mechanism Using DNS with Privacy Preservation by Yong Jin et al (2021)** proposed a lightweight and secure IoT remote monitoring mechanism using DNS and evaluated the prototype system over a name-bound virtual network.

27. **Data Security System for IoT Applications by Shahed Mohammed et al (2021)** proposed protocol that merges between the feature of symmetric and asymmetric algorithms that provided best effective and efficient solution.

28. **Enhancing Indoor IoT Communication with Visible Light and Ultrasound by Michael Haus et al (2021)** have developed the communication modules and evaluated them in testbed environments. Proposed study sheds light on how to apply those technologies in practice and illustrates pragmatic use cases to augment various IoT services.

29. **Anomaly Based Intrusion Detection for IoT with Machine Learning by Addison Shaver et al (2021)** evaluated different models and classification schemes with the optimal ratio of highest accuracy to least execution time to improve anomaly detection.

30. **Validation of IoT secure communication gateway for constrained devices by Peter Peniak et al(2021)** alternative approach is proposed to use the additional device, IoT Secure gateway, to secure communication of constrained devices with external systems and servers via Cloud.

31. **An Efficient Trust Management Technique Using ID3 Algorithm With Blockchain in Smart Buildings IoT by FATHE JERIBI et al** presents a trust management method for use in IoT (Internet of Things) systems for smart buildings that combines the blockchain with ID3 (Iterative Dichotomiser 3) algorithm. By fusing the ID3 algorithm's ability to make decisions based on data with the decentralised, secure nature of blockchain technology, the objective is to boost the effectiveness and security of these systems.

32. **Security in IoT Mesh Networks Based on Trust Similarity by ATHOTA KAVITHA et al** proposes a trust-based strategy that focuses on security in mesh networks for the Internet of Things (IoT). The research's objective is to offer a workable solution to security issues in IoT mesh networks, which are essential for many applications, including smart homes and cities, industrial automation, and environmental monitoring.

33. **A Survey on Secure Group Communication Schemes With Focus on IoT Communication by THOMAS PRANTL et al** offers a thorough analysis of secure

group communication protocols with a focus on IoT communication, study includes key management, secrecy, integrity, and authentication across a wide range of secure group communication techniques and protocols.

34. **Efficient Implementation of Lightweight Hash Functions on GPU and Quantum Computers for IoT Applications by WAI-KONG LEE et al** research focuses on the effective implementation of lightweight hash functions on GPUs and quantum computers and assesses their performance against conventional hash functions. Additionally, the authors assess the security of the light-weight hash functions and their resistance to assaults such collision and preimage attacks.

35. **Towards Blockchain-Based Secure Storage and Trusted Data Sharing Scheme for IoT Environment by ZIA ULLAH et al** proposed scheme makes use of blockchain technology to offer an IoT device data storage and sharing mechanism that is secure and trusted. The research's objective is to offer a workable solution for secure and trusted data storage and sharing in IoT environments, which will support the creation of trustworthy and dependable IoT applications.

36. **Light-Weight Secure Aggregated Data Sharing in IoT-Enabled Wireless Sensor Networks by GHAWAR SAID** offers a compact, secure data-sharing method for IoT-compatible wireless sensor networks. The goal of the search is to offer a workable remedy for secure and energy-efficient data sharing in IoT-enabled wireless sensor networks, which will aid in the creation of safe and secure IoT applications.

37. **A Secure Blockchain Platform for Supporting AI-Enabled IoT Applications at the Edge Layer by SUBHI M. AL RUBEI et al** provides a secure blockchain infrastructure for enabling edge-layer IoT applications using AI. A secure and reliable data processing system for IoT devices at the edge layer is offered by the proposed platform, which combines blockchain technology with AI algorithms.

38. **An Energy-Efficient Data Aggregation Mechanism for IoT Secured by Blockchain by ADEEL AHMED et al** The suggested mechanism aggregates the data before it is communicated to the sink node, resulting in a reduction in the energy consumption of the IoT devices and an increase in the security of the data transmission.

39. **A Secure and Efficient Trust Model for Wireless Sensor IoTs Using Blockchain b y NADEEM JAVAID et al** In order to ensure data integrity, privacy, and security as well as the efficient operation of the system, a secure and effective trust model employing blockchain can assist address some of the major difficulties faced by wireless sensor IoT systems.

40. **A Lightweight Anonymous Authentication and Secure Communication Scheme for Fog Computing Services by CHI-YAO WENG et al** Due to its ability to process data closer to the network's edge, fog computing services have grown in popularity in recent years. A scheme can be created to enable users to access fog computing services anonymously while also ensuring the confidentiality and integrity of the data transmitted over the network.

41. **Improved Blowfish Algorithm-Based Secure Routing Technique in IoT-Based WSN by MAJID ALOTAIBI et al** In an upgraded Blowfish algorithm-based secure routing technique, the Blowfish algorithm is used to encrypt the data transported between nodes in the WSN. Blowfish is a symmetric-key encryption algorithm that offers a high level of security, making it well suited for use in secure routing.

42. **Novel ECC-Based RFID Mutual Authentication Protocol for Emerging IoT Applications by SOUHIR GABSI et al** Using an Elliptic Curve Cryptography (ECC)-based mutual authentication protocol is one way to improve the security of RFID systems in IoT applications. The public-key cryptography system ECC offers a high level of security, making it suitable for use in RFID systems. To secure the privacy of the data communicated between the reader and tag, the ECC-based protocol can include mutual authentication in addition to encryption.

43. **Lightweight Three-Factor-Based Privacy Preserving Authentication Scheme for IoT-Enabled Smart Homes by SUNGJIN YU et al** Utilising a simple three-factor authentication strategy with privacy protection is one way to improve the security and privacy of IoT-enabled smart homes. Three authentication factors are included in this type of method, In addition to providing authentication, the scheme's privacy-preserving component aids in preserving user privacy by encrypting sensitive information and using privacy-improving technologies, like homomorphic encryption, to secure the privacy of the user's biometric data.

44. **Steganographic Secret Sharing With GAN-Based Face Synthesis and Morphing for Trustworthy Authentication in IoT by SISHENG CHEN et al** a reliable and secure authentication method for the Internet of Things can be achieved utilising a steganographic secret sharing technique based on face synthesis and morphing using Generative Adversarial Networks (GAN). The secret sharing mechanism serves as the authentication component of this scheme, as only parties with the proper morphological transformation procedure may extract the secret information from the synthesised face images that were formed by the GAN. Inadvertent access to the information is thereby reduced.

45. **Ping Flood Attack Pattern Recognition Using a K-Means Algorithm in an Internet of Things (IoT) Network by DERIS STIAWAN et al** IoT networks are the subject of Ping Flood attacks, a sort of Distributed Denial of Service (DDoS) attack. In a Ping Flood attack, the attacker floods the target network with ping queries, overloading it and rendering it inaccessible to authorised users, The K-Means technique can be used to launch a reaction after the attack pattern has been discovered, such as blocking the source IP addresses or capping the quantity of incoming ping requests. This may lessen the likelihood that the network may be harmed by the assault.

4. Proposed Methodology

4.1 Objectives

Objective 1: Creating a secure communication channel for communication between lot devices using socket programming

Objective 2: Implementing a robust cryptographic algorithm The RSA Algorithm for encrypting and the data to be transferred

Objective 3: Using MongoDB correct for authentication purposes and SHA256 arm lar encrypting the stored data

Objective4: Using Industry Standard Guideline issued by IETF for creating and Implementing the secured channel

4.2 System Architecture

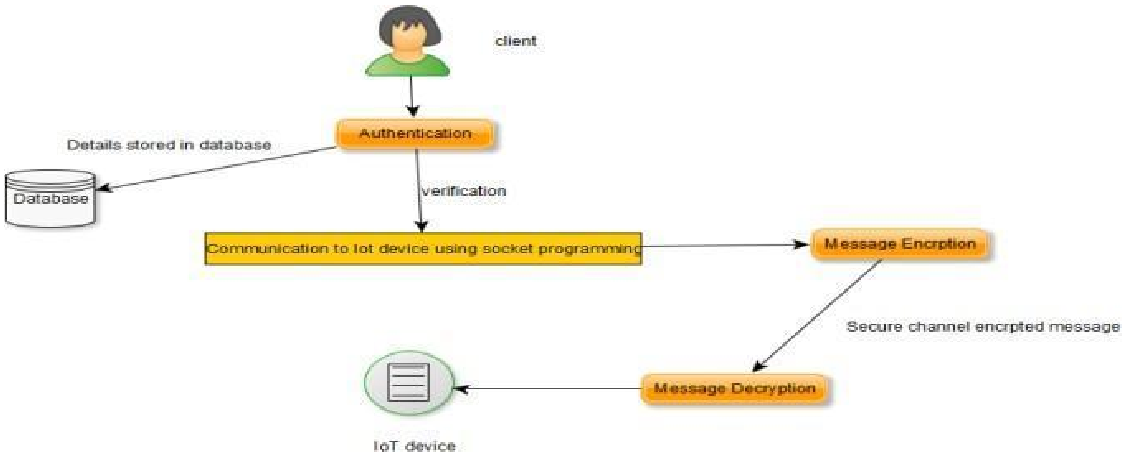

client
Authentication
Details stored in database
Database
verification
Communication to Iot device using socket programming
Message Encrption
Secure channel encrpted message
Message Decryption
IoT device

Figure 4.2.1:System Architecture

A proposed model for Secure Communication for Smart IoT Devices project can be designed using socket programming, MongoDB, and RSA algorithm for encryption. The proposed model can be outlined as follows:

Establish a secure connection using socket programming: The first step is to establish a secure connection between the IoT device and the server. This can be achieved by using socket programming to create a secure socket connection.

Authenticate the IoT device: Once the connection is established, the IoT device needs to be authenticated before sending and receiving data. This can be done by using a unique device ID and a shared secret key generated using SHA 256 algorithm.

Encrypt the data using RSA algorithm: To ensure that the data sent from the IoT device to the server is secure, it needs to be encrypted using a secure encryption algorithm. The RSA algorithm can be used for this purpose, as it is a widely used asymmetric encryption algorithm that provides high levels of security.

Store the encrypted data in MongoDB: After the data is encrypted, it can be stored in MongoDB, which is a popular NoSQL database that provides high scalability and performance.

Decrypt the data at the server end: When the server receives the encrypted data from the IoT device, it needs to be decrypted before it can be processed. This can be done using the private key of the RSA algorithm. Once the data is decrypted, it can be analyzed and processed by the server.

Encrypt the response data: After the server has processed the data, it needs to send the response back to the IoT device. This response data can also be encrypted using the RSA algorithm to ensure that it is secure.

Store the encrypted response data in MongoDB: Finally, the encrypted response data can be stored in MongoDB for future reference.

4.3 Data Flow Diagram

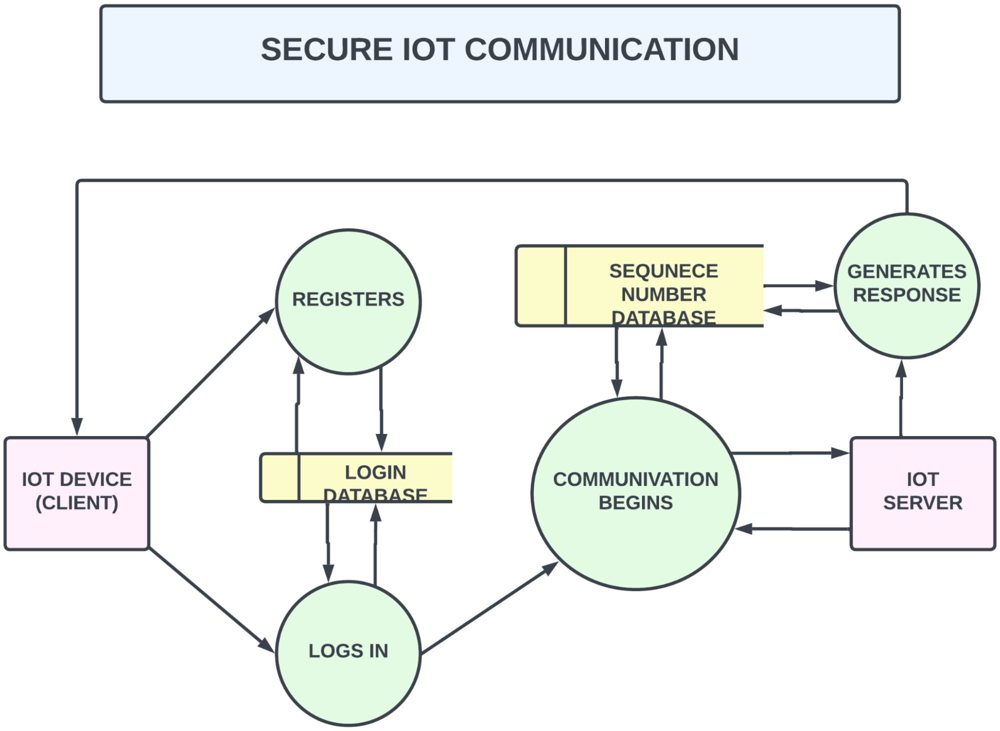


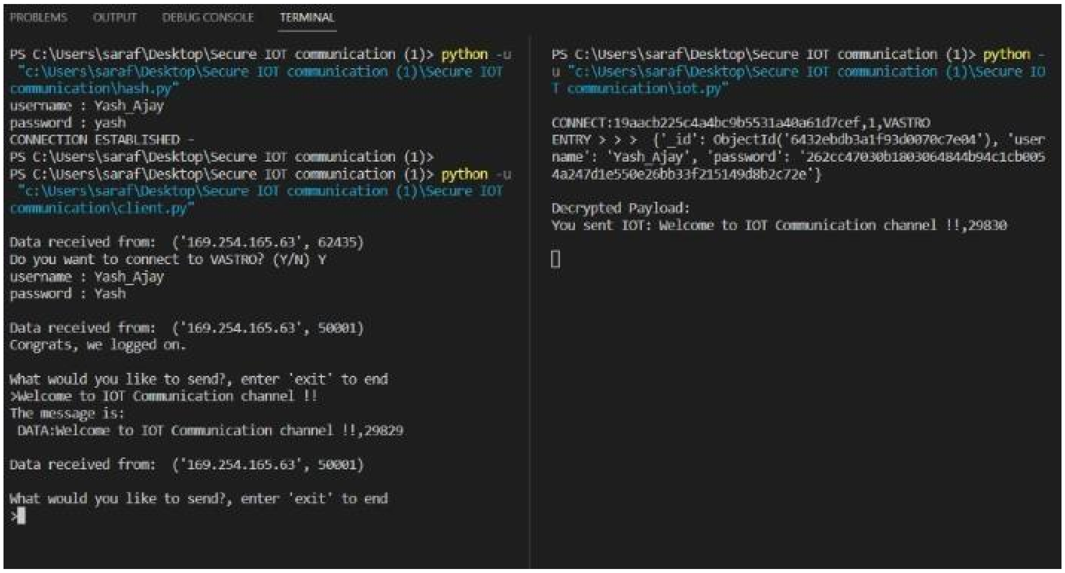
Figure 4.3.1: Data flow Diagram

In secure communication channel we first make a request from client end through IOT to register and login on web of Responsibility project, where data of all users stored in Login Database, used to verify and validate user accessing the site, after login communication process begins, we also sequence number database to store user-ids and its responses, communication takes place b/w server and client, where on request, server generates response which is accessed by client device.

4.4 Implementations

Objective 1: Creating a secure communication channel for communication between Iot devices using socket programming

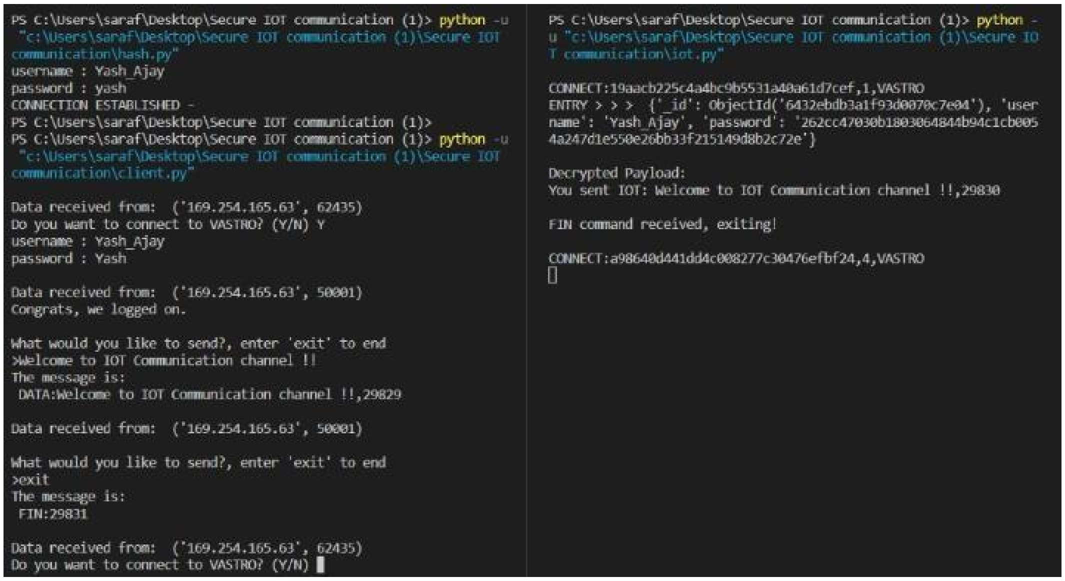
Through the use of encryption techniques and secure communication protocols like TLS or SSL, socket programming can be utilised to create a secure communication channel between IoT devices. Public and private keys for authentication, integrity verification, and confidentiality can be used, as well as certificates, to secure communication. In order to prevent unauthorised parties from intercepting and reading the data exchanged between the devices, the SSL/TLS protocol offers end-to-end encryption. The security of the communication route can also be improved by putting in place auditing and access control systems. To make sure that the communication is protected against any flaws and dangers, it is crucial to routinely upgrade the security procedures.



```
PS C:\Users\saraf\Desktop\Secure IOT communication (1)> python -u
 "c:\Users\saraf\Desktop\Secure IOT communication (1)\Secure IOT
communication\hash.py"
username : Yash_Ajay
password : yash
CONNECTION ESTABLISHED -
PS C:\Users\saraf\Desktop\Secure IOT communication (1)>
PS C:\Users\saraf\Desktop\Secure IOT communication (1)> python -u
 "c:\Users\saraf\Desktop\Secure IOT communication (1)\Secure IOT
communication\client.py"

Data received from:  ('169.254.165.63', 62435)
Do you want to connect to VASTRO? (Y/N) Y
username : Yash_Ajay
password : Yash

Data received from:  ('169.254.165.63', 50001)
Congrats, we logged on.

What would you like to send?, enter 'exit' to end
>Welcome to IOT Communication channel !!
The message is:
 DATA:Welcome to IOT Communication channel !!,29829

Data received from:  ('169.254.165.63', 50001)

What would you like to send?, enter 'exit' to end
>
```

```
PS C:\Users\saraf\Desktop\Secure IOT communication (1)> python -
u "c:\Users\saraf\Desktop\Secure IOT communication (1)\Secure IO
T communication\iot.py"

CONNECT:19aacb225c4a4bc9b5531a40a61d7cef,1,VASTRO
ENTRY > > >  {'_id': ObjectId('6432ebdb3a1f93d0070c7e04'), 'user
name': 'Yash_Ajay', 'password': '262cc47030b1803064844b94c1cb005
4a247d1e550e26bb33f215149d8b2c72e'}

Decrypted Payload:
You sent IOT: Welcome to IOT Communication channel !!,29830

```

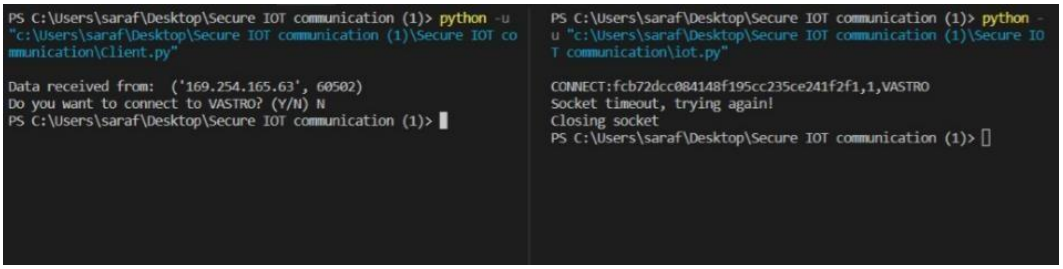
Figure 4.4.1.1: Running simultaneously client.py and server.py files



```
PS C:\Users\saraf\Desktop\Secure IOT communication (1)> python -u
 "c:\Users\saraf\Desktop\Secure IOT communication (1)\Secure IOT
communication\hash.py"
username : Yash_Ajay
password : yash
CONNECTION ESTABLISHED -
PS C:\Users\saraf\Desktop\Secure IOT communication (1)>
PS C:\Users\saraf\Desktop\Secure IOT communication (1)> python -u
 "c:\Users\saraf\Desktop\Secure IOT communication (1)\Secure IOT
communication\client.py"

Data received from:  ('169.254.165.63', 62435)
Do you want to connect to VASTRO? (Y/N) Y
username : Yash_Ajay
password : Yash

Data received from:  ('169.254.165.63', 50001)
Congrats, we logged on.

What would you like to send?, enter 'exit' to end
>Welcome to IOT Communication channel !!
The message is:
 DATA:Welcome to IOT Communication channel !!,29829

Data received from:  ('169.254.165.63', 50001)

What would you like to send?, enter 'exit' to end
>exit
The message is:
 FIN:29831

Data received from:  ('169.254.165.63', 62435)
Do you want to connect to VASTRO? (Y/N)
```

```
PS C:\Users\saraf\Desktop\Secure IOT communication (1)> python -
u "c:\Users\saraf\Desktop\Secure IOT communication (1)\Secure IO
T communication\iot.py"

CONNECT:19aacb225c4a4bc9b5531a40a61d7cef,1,VASTRO
ENTRY > > >  {'_id': ObjectId('6432ebdb3a1f93d0070c7e04'), 'user
name': 'Yash_Ajay', 'password': '262cc47030b1803064844b94c1cb005
4a247d1e550e26bb33f215149d8b2c72e'}

Decrypted Payload:
You sent IOT: Welcome to IOT Communication channel !!,29830

FIN command received, exiting!

CONNECT:a98640d441dd4c008277c30476efbf24,4,VASTRO
```

Figure 4.4.1.2: Communicate using Messages between client and server



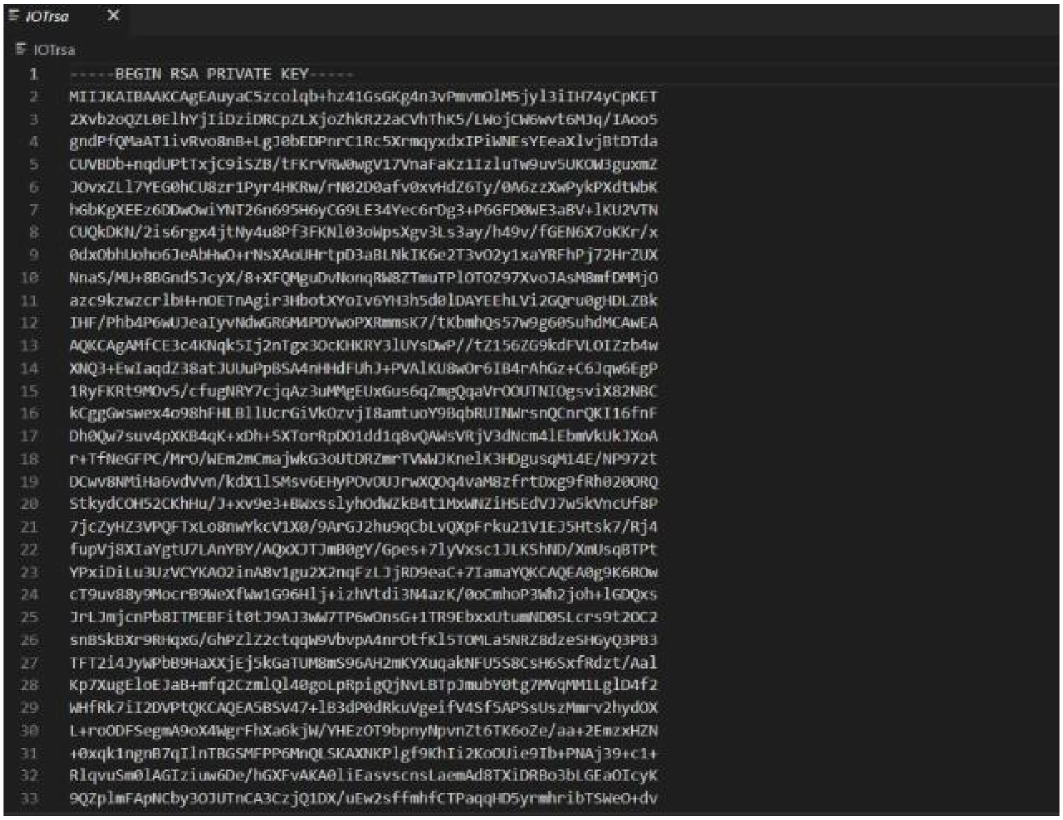
```
PS C:\Users\saraf\Desktop\Secure IOT communication (1)> python -u
"c:\Users\saraf\Desktop\Secure IOT communication (1)\Secure IOT co
mmunication\Client.py"

Data received from:  ('169.254.165.63', 60502)
Do you want to connect to VASTRO? (Y/N) N
PS C:\Users\saraf\Desktop\Secure IOT communication (1)>
```

```
PS C:\Users\saraf\Desktop\Secure IOT communication (1)> python -
u "c:\Users\saraf\Desktop\Secure IOT communication (1)\Secure IO
T communication\iot.py"

CONNECT:fcb72dcc084148f195cc235ce241f2f1,1,VASTRO
Socket timeout, trying again!
Closing socket
PS C:\Users\saraf\Desktop\Secure IOT communication (1)>
```

Figure 4.4.1.3: Server Exit

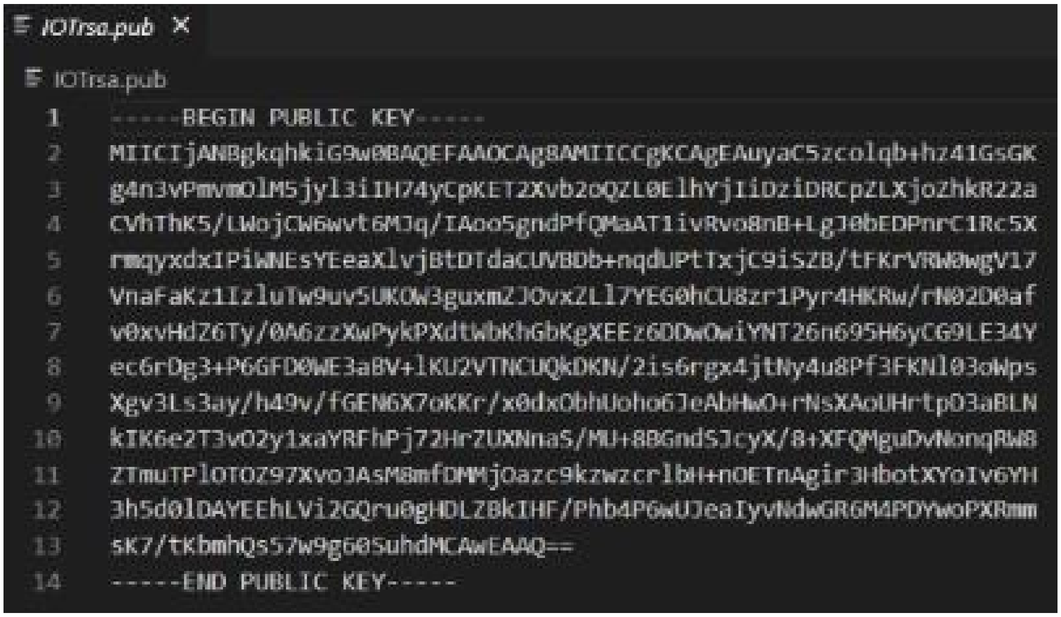
Objective 2: Implementing a robust cryptographic algorithm The RSA Algorithm for encrypting and the data to be transferred

To prevent the attacks to steal the messages and data we need to encrypt the messages such that it should be hard to the hackers to decrypt the traffic. Here in this project we are using RSA algorithm for encrypting the data the algorithm is almost impossible to break. It is Asymmetric key cryptographic algorithm based on public key encryption.



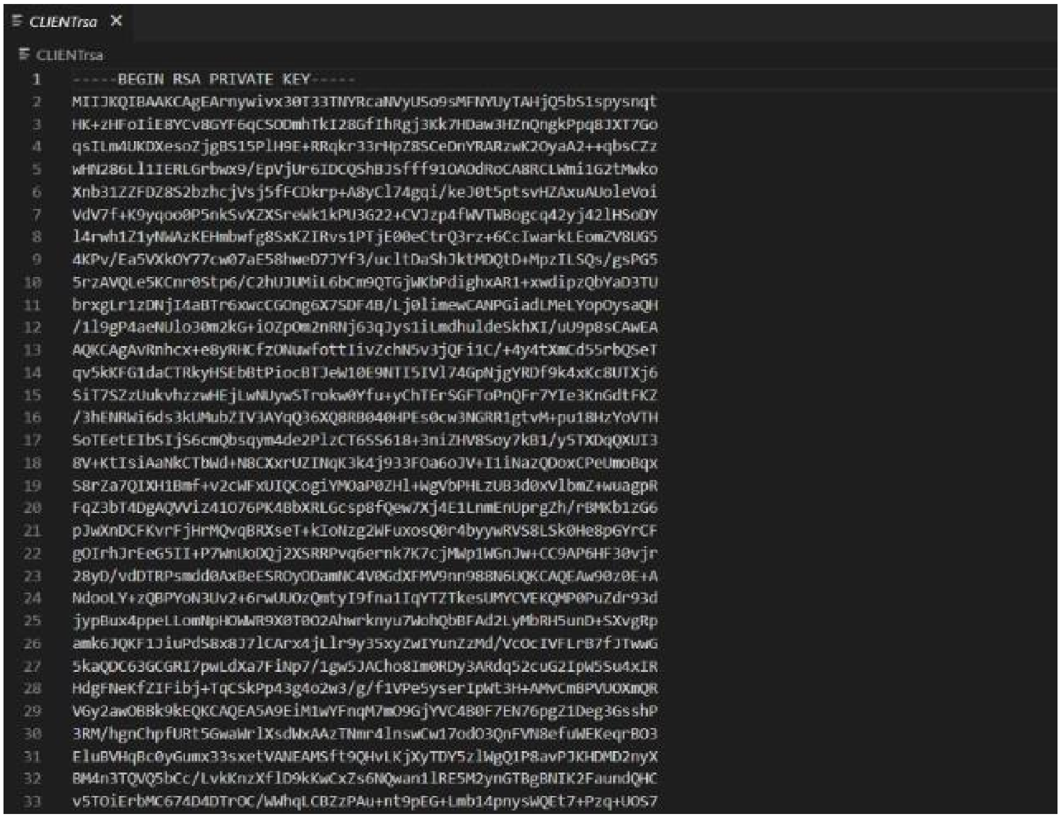
```
-----BEGIN RSA PRIVATE KEY-----
MIIJKAIBAAKCAgEAuyaC5zcolqb+hz41GsGKg4n3vPmvmOlM5jyl3iIH74yCpKET
2Xvb2oQZL0ElhYjIiDziDRCpZLXjoZhkR22aCVhThK5/LWojCW6wvt6MJq/IAoo5
gndPfQMaAT1ivRvo8nB+LgJ0bEDPnrC1Rc5XrmqyxdxIPiWNEsYEeaXlvjBtDTda
CUVBDb+nqdUPtTxjC9iSZB/tFKrVRW0wgV17VnaFaKz1IzluTw9uv5UKOW3guxmZ
JOvxZLl7YEG0hCU8zr1Pyr4HKRw/rN02D0afv0xvHdZ6Ty/0A6zzXwPykPXdtWbK
hGbKgXEEz6DDwOwiYNT26n695H6yCG9LE34Yec6rDg3+P6GFD0WE3aBV+lKU2VTN
CUQkDKN/2is6rgx4jtNy4u8Pf3FKNl03oWpsXgv3Ls3ay/h49v/fGEN6X7oKKr/x
0dxObhUoho6JeAbHwO+rNsXAoUHrtpD3aBLNkIK6e2T3vO2y1xaYRFhPj72HrZUX
NnaS/MU+8BGndSJcyX/8+XFQMguDvNonqRW8ZTmuTPlOTOZ97XvoJAsM8mfDMMjO
azc9kzwzcrlbH+nOETnAgir3HbotXYoIv6YH3h5d0lDAYEEhLVi2GQru0gHDLZBk
IHF/Phb4P6wUJeaIyvNdwGR6M4PDYwoPXRmmsK7/tKbmhQs57w9g60SuhdMCAwEA
AQKCAgAMfCE3c4KNqk5Ij2nTgx3OcKHKRY3lUYsDwP//tZ156ZG9kdFVLOIZzb4w
XNQ3+EwIaqdZ38atJUUuPp8SA4nHHdFUhJ+PVAlKU8wOr6IB4rAhGz+C6Jqw6EgP
1RyFKRt9MOv5/cfugNRY7cjqAz3uMMgEUxGus6qZmgQqaVrOOUTNIOgsviX82NBC
kCggGwswex4o98hFHLBllUcrGiVkOzvjI8amtuoY9BqbRUINWrsnQCnrQKI16fnF
Dh0Qw7suv4pXKB4qK+xDh+5XTorRpDO1dd1q8vQAWsVRjV3dNcm4lEbmVkUkJXoA
r+TfNeGFPC/MrO/WEm2mCmajwkG3oUtDRZmrTVWWJKnelK3HDgusqM14E/NP972t
DCwv8NMiHa6vdVvn/kdX1lSMsv6EHyPOvOUJrwXQOq4vaM8zfrtDxg9fRh020ORQ
StkydCOH52CKhHu/J+xv9e3+BWxsslyhOdWZkB4t1MxWNZiH5EdVJ7w5kVncUf8P
7jcZyHZ3VPQFTxLo8nwYkcV1X0/9ArGJ2hu9qCbLvQXpFrku21V1EJ5Htsk7/Rj4
fupVj8XIaYgtU7LAnYBY/AQxXJTJmB0gY/Gpes+7lyVxsc1JLKShND/XmUsqBTPt
YPxiDiLu3UzVCYKAO2inA8v1gu2X2nqFzLJjRD9eaC+7IamaYQKCAQEA0g9K6ROw
cT9uv88y9MocrB9WeXfWw1G96Hlj+izhVtdi3N4azK/0oCmhoP3Wh2joh+lGDQxs
JrLJmjcnPb8ITMEBFit0tJ9AJ3wW7TP6wOnsG+1TR9EbxxUtumND0SLcrs9t2OC2
snB5kBXr9RHqxG/GhPZlZ2ctqqW9VbvpA4nrOtfKl5TOMLa5NRZ8dze5HGyQ3PB3
TFT2i4JyWPbB9HaXXjEj5kGaTUM8mS96AH2mKYXuqakNFU5S8CsH6SxfRdzt/Aal
Kp7XugEloEJaB+mfq2CzmlQl40goLpRpigQjNvLBTpJmubY0tg7MVqMM1LglD4f2
WHfRk7iI2DVPtQKCAQEA5BSV47+lB3dP0dRkuVgeifV4Sf5APSsUszMmrv2hydOX
L+roODFSegmA9oX4WgrFhXa6kjW/YHEzOT9bpnyNpvnZt6TK6oZe/aa+2EmzxHZN
+0xqk1ngnB7qIlnTBGSMFPP6MnQLSKAXNKPlgf9KhIi2KoOUie9Ib+PNAj39+c1+
RlqvuSm0lAGIziuw6De/hGXFvAKA0liEasvscnsLaemAd8TXiDRBo3bLGEaOIcyK
9QZplmFApNCby3OJUTnCA3CzjQ1DX/uEw2sffmhfCTPaqqHD5yrmhribTSWeO+dv
```

Figure 4.4.2.1: IOT-RSA private keys



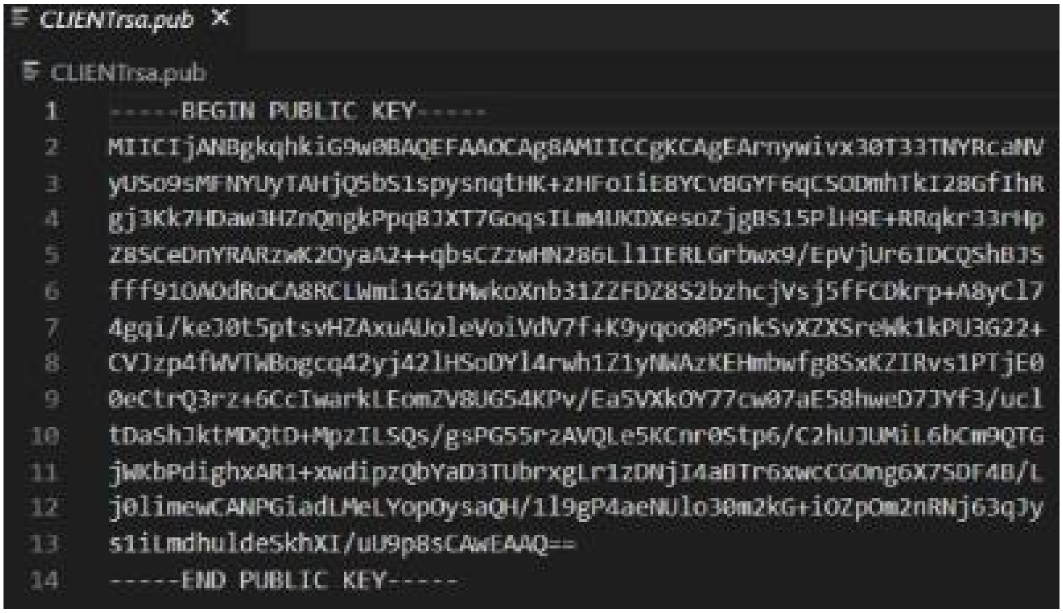
```
-----BEGIN PUBLIC KEY-----
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAuyaC5zcolqb+hz41GsGK
g4n3vPmvmOlM5jyl3iIH74yCpKET2Xvb2oQZL0ElhYjIiDziDRCpZLXjoZhkR22a
CVhThK5/LWojCW6wvt6MJq/IAoo5gndPfQMaAT1ivRvo8nB+LgJ0bEDPnrC1Rc5X
rmqyxdxIPiWNEsYEeaXlvjBtDTdaCUVBDb+nqdUPtTxjC9iSZB/tFKrVRW0wgV17
VnaFaKz1IzluTw9uv5UKOW3guxmZJOvxZLl7YEG0hCU8zr1Pyr4HKRw/rN02D0af
v0xvHdZ6Ty/0A6zzXwPykPXdtWbKhGbKgXEEz6DDwOwiYNT26n695H6yCG9LE34Y
ec6rDg3+P6GFD0WE3aBV+lKU2VTNCUQkDKN/2is6rgx4jtNy4u8Pf3FKNl03oWps
Xgv3Ls3ay/h49v/fGEN6X7oKKr/x0dxObhUoho6JeAbHwO+rNsXAoUHrtpD3aBLN
kIK6e2T3vO2y1xaYRFhPj72HrZUXNnaS/MU+8BGndSJcyX/8+XFQMguDvNonqRW8
ZTmuTPlOTOZ97XvoJAsM8mfDMMjOazc9kzwzcrlbH+nOETnAgir3HbotXYoIv6YH
3h5d0lDAYEEhLVi2GQru0gHDLZBkIHF/Phb4P6wUJeaIyvNdwGR6M4PDYwoPXRmm
sK7/tKbmhQs57w9g60SuhdMCAwEAAQ==
-----END PUBLIC KEY-----
```

Figure 4.4.2.2: IOT-RSA public keys



```
-----BEGIN RSA PRIVATE KEY-----
MIIJKQIBAAKCAgEArnywivx30T33TNYRcaNVyUSo9sMFNYUyTAHjQ5bS1spysnqt
HK+zHFoIiEBYCv8GYF6qCSODmhTkI28GfIhRgj3Kk7HDaw3HZnQngkPpq8JXT7Go
qsILm4UKDXesoZjgBS15PlH9E+RRqkr33rHpZ8SCeDnYRARzwK2OyaA2++qbsCZz
wHN286Ll1IERLGrbwx9/EpVjUr6IDCQShBJSfff91OAOdRoCA8RCLWmi1G2tMwko
Xnb31ZZFDZ8S2bzhcjVsj5fFCDkrp+A8yCl74gqi/keJ0t5ptsvHZAxuAUoleVoi
VdV7f+K9yqoo0P5nkSvXZXSreWk1kPU3G22+CVJzp4fWVTWBogcq42yj42lHSoDY
l4rwh1Z1yNWAzKEHmbwfg8SxKZIRvs1PTjE00eCtrQ3rz+6CcIwarkLEomZV8UG5
4KPv/Ea5VXkOY77cw07aE58hweD7JYf3/ucltDaShJktMDQtD+MpzILSQs/gsPG5
5rzAVQLe5KCnr0Stp6/C2hUJUMiL6bCm9QTGjWKbPdighxAR1+xwdipzQbYaD3TU
brxgLr1zDNjI4aBTr6xwcCGOng6X7SDF4B/Lj0limewCANPGiadLMeLYopOysaQH
/1l9gP4aeNUlo30m2kG+iOZpOm2nRNj63qJys1iLmdhuldeSkhXI/uU9p8sCAwEA
AQKCAgAvRnhcx+e8yRHCfzONuwfottIivZchN5v3jQFi1C/+4y4tXmCd55rbQSeT
qv5kKFG1daCTRkyHSEbBtPiocBTJeW10E9NTI5IVl74GpNjgYRDf9k4xKc8UTXj6
SiT7SZzUukvhzzwHEjLwNUywSTrokw0Yfu+yChTErSGFToPnQFr7YIe3KnGdtFKZ
/3hENRWi6ds3kUMubZIV3AYqQ36XQ8RB040HPEs0cw3NGRR1gtvM+pu18HzYoVTH
SoTEetEIbSIjS6cmQbsqym4de2PlzCT6SS618+3niZHV8Soy7kB1/y5TXDqQXUI3
8V+KtIsiAaNkCTbWd+N8CXxrUZINqK3k4j933FOa6oJV+I1iNazQDoxCPeUmoBqx
S8rZa7QIXH1Bmf+v2cWFxUIQCogiYMOaP0ZHl+WgVbPHLzUB3d0xVlbmZ+wuagpR
FqZ3bT4DgAQVVi241O76PK4BbXRLGcsp8fQew7Xj4E1LnmEnUprgZh/rBMKb1zG6
pJwXnDCFKvrFjHrMQvqBRXseT+kIoNzg2WFuxosQ0r4byywRVS8LSk0He8pGYrCF
gOIrhJrEeG5II+P7WnUoDQj2XSRRPvq6ernk7K7cjMWp1WGnJw+CC9AP6HF30vjr
28yD/vdDTRPsmdd0AxBeESROyODamNC4V0GdXFMV9nn988N6UQKCAQEAw90z0E+A
NdooLY+zQBPYoN3Uv2+6rwUUOzQmtyI9fna1IqYTZTkesUMYCVEKQMP0PuZdr93d
jypBux4ppeLLomNpHOWWR9X8TBO2Ahwrknyu7WohQbBFAd2LyMbRH5unD+SXvgRp
amk6JQKF1JiuPdS8x8J7lCArx4jLlr9y35xyZwIYunZzMd/VcOcIVFLrB7fJTwwG
5kaQDC63GCGRI7pwLdXa7FiNp7/1gw5JACho8Im0RDy3ARdq52cuG2IpW5Su4xIR
HdgFNeKfZIFibj+TqCSkPp43g4o2w3/g/f1VPe5yserIpWt3H+AMvCmBPVUOXmQR
VGy2awOB8k9kEQKCAQEA5A9EiM1wYFnqM7mO9GjYVC480F7EN76pgZ1Deg3GsshP
3RM/hgnChpfURt5GwaWrlXsdWxAAzTNmr4lnswCw17odO3QnFVN8efuWEKeqrBO3
EluBVHqBc0yGumx33sxetVANEAMSft9QHvLKjXyTDY5zlWgQ1P8avPJKHDMD2nyX
BM4n3TQVQ5bCc/LvkKnzXflD9kKwCxZs6NQwan1lRESM2ynGTBgBNIK2FaundQHC
v5TOiErbMC674D4DTrOC/WWhqLCBZzPAu+nt9pEG+Lmb14pnysWQEt7+Pzq+UOS7
```

Figure 4.4.2.3: Client-RSA private keys

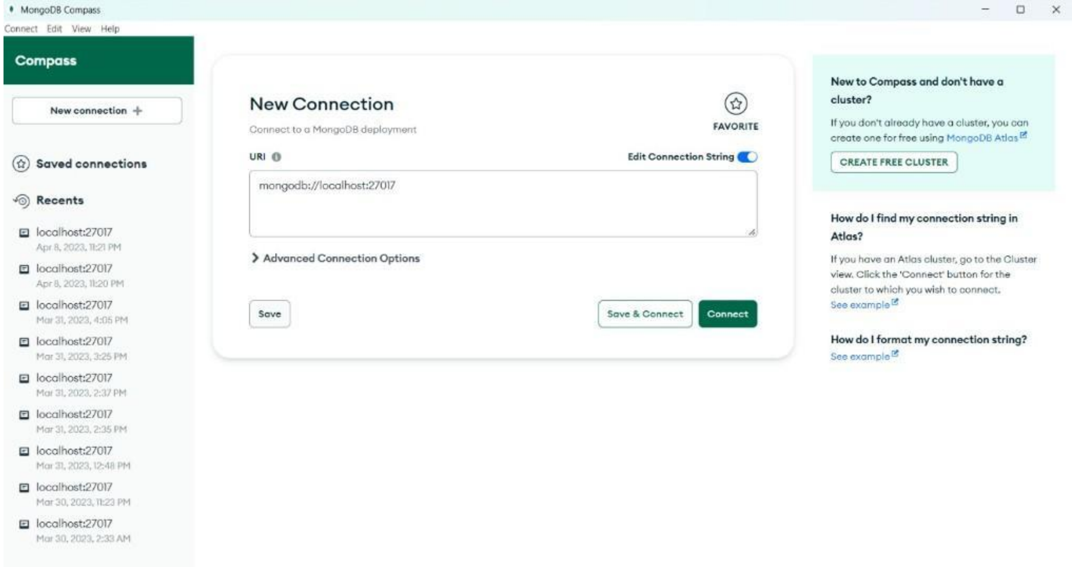


```
-----BEGIN PUBLIC KEY-----
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEArnywivx30T33TNYRcaNV
yUSo9sMFNYUyTAHjQ5bS1spysnqtHK+zHFoIiEBYCv8GYF6qCSODmhTkI28GfIhR
gj3Kk7HDaw3HZnQngkPpq8JXT7GoqsILm4UKDXesoZjgBS15PlH9E+RRqkr33rHp
Z8SCeDnYRARzwK2OyaA2++qbsCZzwHN286Ll1IERLGrbwx9/EpVjUr6IDCQShBJS
fff91OAOdRoCA8RCLWmi1G2tMwkoXnb31ZZFDZ8S2bzhcjVsj5fFCDkrp+A8yCl7
4gqi/keJ0t5ptsvHZAxuAUoleVoiVdV7f+K9yqoo0P5nkSvXZXSreWk1kPU3G22+
CVJzp4fWVTWBogcq42yj42lHSoDYl4rwh1Z1yNWAzKEHmbwfg8SxKZIRvs1PTjE0
0eCtrQ3rz+6CcIwarkLEomZV8UG54KPv/Ea5VXkOY77cw07aE58hweD7JYf3/ucl
tDaShJktMDQtD+MpzILSQs/gsPG55rzAVQLe5KCnr0Stp6/C2hUJUMiL6bCm9QTG
jWKbPdighxAR1+xwdipzQbYaD3TUbrxgLr1zDNjI4aBTr6xwcCGOng6X7SDF4B/L
j0limewCANPGiadLMeLYopOysaQH/1l9gP4aeNUlo30m2kG+iOZpOm2nRNj63qJy
s1iLmdhuldeSkhXI/uU9p8sCAwEAAQ==
-----END PUBLIC KEY-----
```

Figure 4.4.2.4: Client-RSA public keys

Objective 3: Using MongoDB correct for authentication purposes and SHA256 arm lar encrypting the stored data

The secure storage of user credentials, such as usernames and passwords, enables MongoDB to be utilised for authentication purposes. To do this, the passwords can be hashed using SHA256 encryption before being entered into the database. A user's identity can be confirmed by hashing their password and comparing it to a previously stored hash value when they log in. The necessity to encrypt sensitive data can also be met by using MongoDB as a storage solution. To accomplish this, encrypt the data before putting it in the database using an encryption algorithm like AES or RSA. Because of this, even if the database is compromised, the data will still be protected. To keep the data safe from any threats and weaknesses, it is crucial to routinely upgrade the encryption techniques.



New Connection

Connect to a MongoDB deployment

URI: mongodb://localhost:27017

Edit Connection String

localhost:27017
Apr 8, 2023, 11:21 PM
localhost:27017
Apr 8, 2023, 11:20 PM
localhost:27017
Mar 31, 2023, 4:05 PM
localhost:27017
Mar 31, 2023, 3:25 PM
localhost:27017
Mar 31, 2023, 2:37 PM
localhost:27017
Mar 31, 2023, 2:35 PM
localhost:27017
Mar 31, 2023, 12:48 PM
localhost:27017
Mar 30, 2023, 11:23 PM
localhost:27017
Mar 30, 2023, 2:33 AM

New to Compass and don't have a cluster?

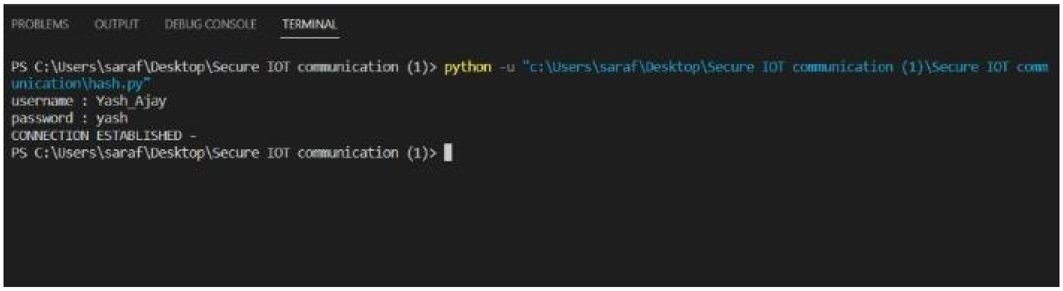
If you don't already have a cluster, you can create one for free using MongoDB Atlas

How do I find my connection string in Atlas?

If you have an Atlas cluster, go to the Cluster view. Click the 'Connect' button for the cluster to which you wish to connect.
See example

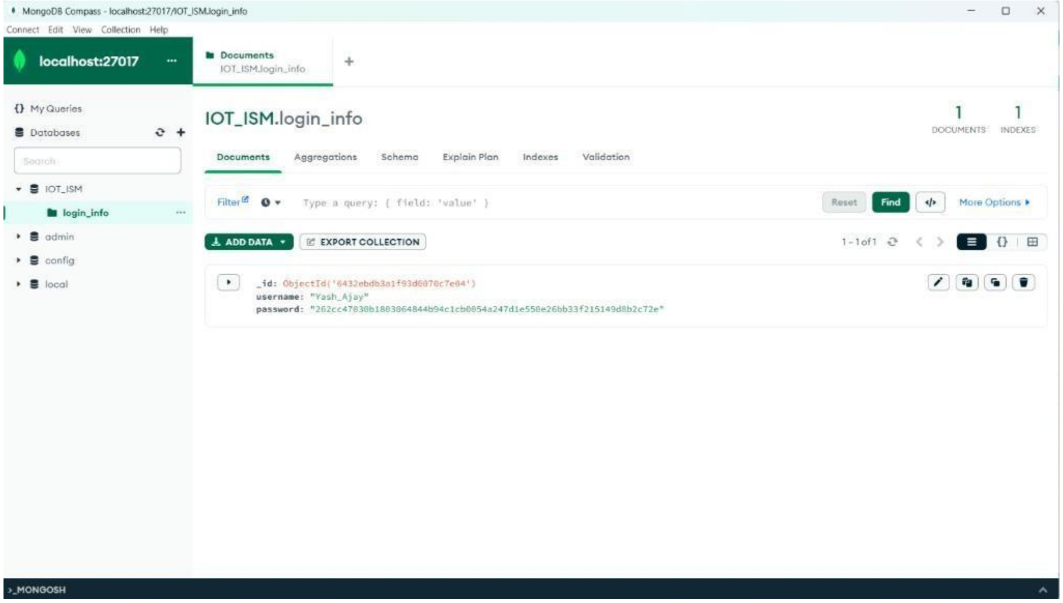
How do I format my connection string?
See example

Figure 4.4.3.1: Mongo DB interface before server connection



```
PS C:\Users\saraf\Desktop\Secure IOT communication (1)> python -u "c:\Users\saraf\Desktop\Secure IOT communication (1)\Secure IOT comm
unication\hash.py"
username : Yash_Ajay
password : yash
CONNECTION ESTABLISHED -
PS C:\Users\saraf\Desktop\Secure IOT communication (1)>
```

Figure 4.4.3.2 :connect to the MongoDB database which is hosted on localhost/27017



```
_id: ObjectId('6432ebdb3a1f93d6070c7e04')
username: "Yash_Ajay"
password: "262cc47030b1803064844b94c1cb0054a247d1e550e26bb33f215149d8b2c72e"
```

Figure 4.4.3.3:After connection to server

Objective4: Using Industry Standard Guideline issued by IETF for creating and Implementing the secured channel

For the development and implementation of secure communication channels, the Internet Engineering Task Force (IETF) has released a variety of industry-standard guidelines. These recommendations cover the usage of authentication methods like digital certificates and encryption protocols like TLS and SSL. Other suggestions include employing secure ciphers, setting up access controls and audit trails, and routinely checking and updating security measures to make sure they continue to be effective against prospective threats. By adhering to these recommendations, businesses can build secure communication channels that guard against unauthorized access, data alteration, and eavesdropping, thereby improving the general security of their systems and networks.

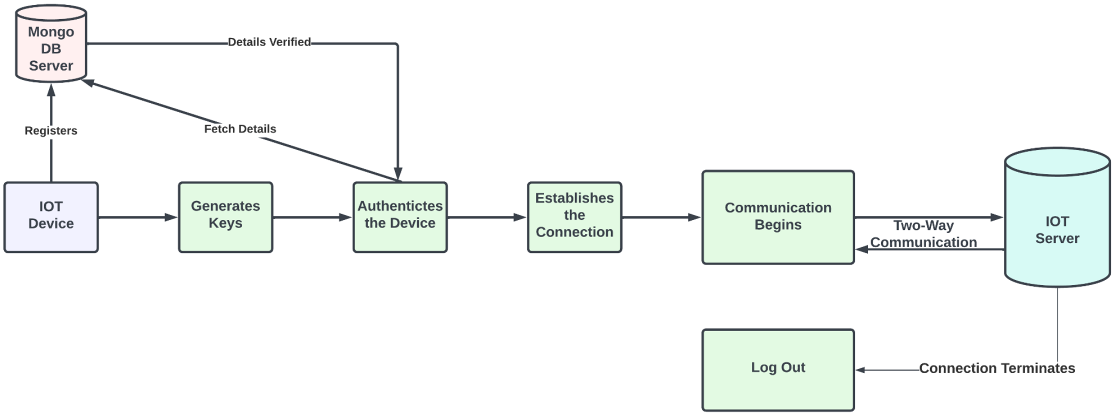


Figure: 4.4.4.1: Execution flow of Programs as per IETF Guidelines

4.5 Real World Application:

Introduction:

The Responsibility project is a web application designed to facilitate donations to non-profit organizations. It offers a donor database and integrated online giving forms as core functionalities. The platform is easy to use, accessible 24/7, and supports various fundraising strategies. It features state-of-the-art design and customization options for users. The goal of the project is to provide non-profit organizations with tools to automate key processes and offer donors an easy platform for contributions. The implementation focuses on secure IoT communication, input validation, processing, and storage of donation details. It ensures confidentiality and integrity of data using encryption algorithms like RSA and SHA256. Confirmation and acknowledgment messages are sent to users for successful donations. Overall, Responsibility aims to make donation processes efficient, secure, and user-friendly for non-profit organizations and donors.

Implementation:

The implementation process of making a donation on the Responsibility platform via an IoT device using secure communication involves several steps.

Secure IoT Communication: The IoT device communicates securely with the server using socket programming and the RSA algorithm for encryption and decryption of data. This ensures that the communication between the IoT device and the server is protected from unauthorized access and tampering.

GUI Integration: The GUI of the Responsibility platform is incorporated into the IoT device, allowing users to input the necessary donation details such as the charity name, amount to be donated, username, and password.

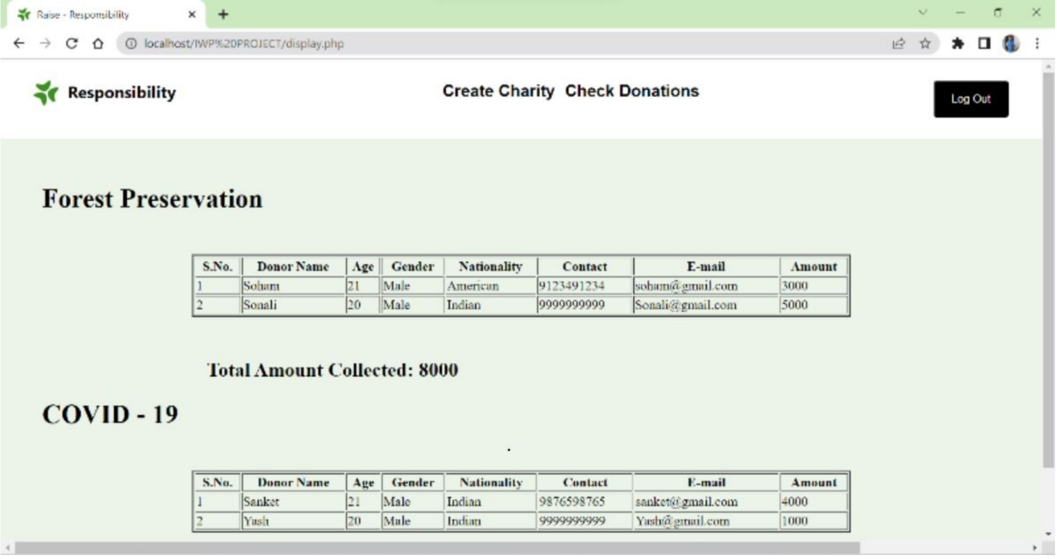
Input Validation: The input provided by the user on the IoT device is validated to ensure that it meets the required criteria, such as checking for the presence of all mandatory fields, validating the format of the amount to be donated, and verifying the username and password for authentication.

Donation Submission: Once the input is validated, the donation details are securely transmitted from the IoT device to the server using the secure communication channel established in step 1. The donation details are encrypted using the RSA algorithm to protect the confidentiality of the data.

Processing and Storage: The server receives the encrypted donation details and decrypts them using the RSA algorithm. The decrypted data is then processed, and the donation is recorded in the Responsibility platform's donor database. The donation amount is securely stored using the SHA256 algorithm for encryption to ensure the integrity of the data.

Acknowledgment and Confirmation: After the donation is processed and stored, a confirmation and acknowledgment message is sent back to the IoT device to inform the user that the donation has been successfully made. This confirmation message is also encrypted using the RSA algorithm to maintain the confidentiality of the data during transmission.

Overall, the implementation process ensures that the donation made via an IoT device on the Responsibility platform is securely transmitted, validated, processed, and stored, providing a secure and efficient way for users to make donations while protecting the confidentiality and integrity of the data.



Forest Preservation

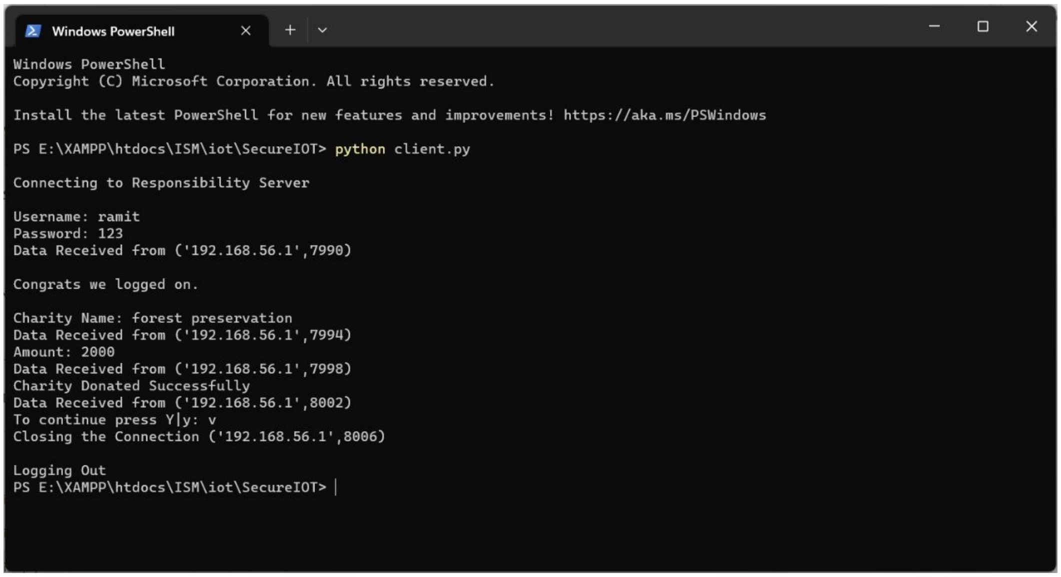
S.No.	Donor Name	Age	Gender	Nationality	Contact	E-mail	Amount
1	Soham	21	Male	American	9123491234	soham@gmail.com	3000
2	Sonali	20	Male	Indian	9999999999	Sonali@gmail.com	5000

Total Amount Collected: 8000

COVID - 19

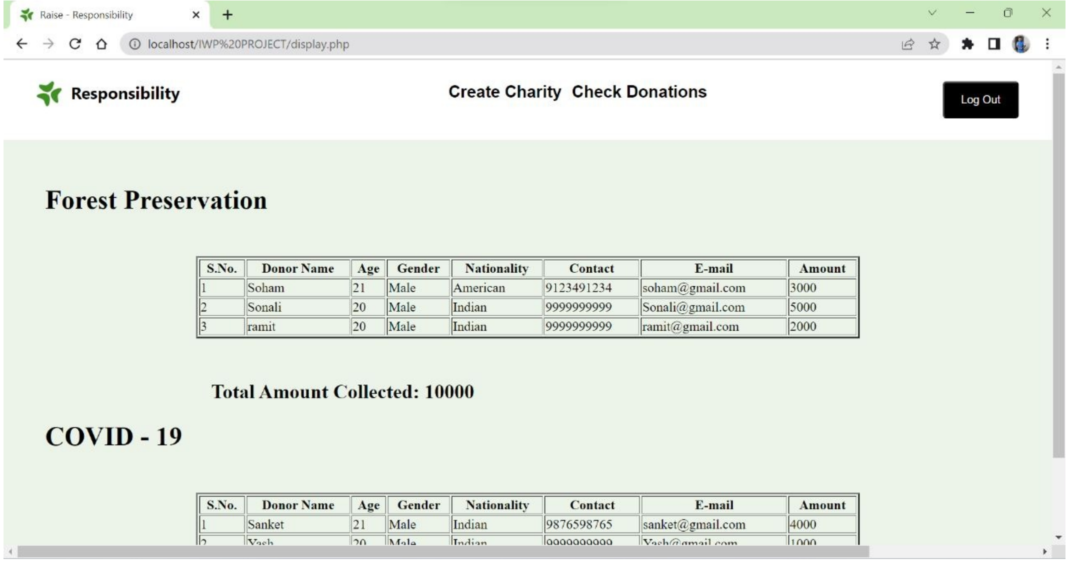
S.No.	Donor Name	Age	Gender	Nationality	Contact	E-mail	Amount
1	Sanket	21	Male	Indian	9876598765	sanket@gmail.com	4000
2	Yash	20	Male	Indian	99999999999	Yash@gmail.com	1000

Figure 4.5.1: Charity donation Page of Responsibility Project



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS E:\XAMPP\htdocs\ISM\iot\SecureIOT> python client.py

Connecting to Responsibility Server

Username: ramit
Password: 123
Data Received from ('192.168.56.1',7990)

Congrats we logged on.

Charity Name: forest preservation
Data Received from ('192.168.56.1',7994)
Amount: 2000
Data Received from ('192.168.56.1',7998)
Charity Donated Successfully
Data Received from ('192.168.56.1',8002)
To continue press Y|y: v
Closing the Connection ('192.168.56.1',8006)

Logging Out
PS E:\XAMPP\htdocs\ISM\iot\SecureIOT> |
```

Figure: 4.5.2: Client-ramit logging to Responsibility Project



Forest Preservation

S.No.	Donor Name	Age	Gender	Nationality	Contact	E-mail	Amount
1	Soham	21	Male	American	9123491234	soham@gmail.com	3000
2	Sonali	20	Male	Indian	9999999999	Sonali@gmail.com	5000
3	ramit	20	Male	Indian	9999999999	ramit@gmail.com	2000

Total Amount Collected: 10000

COVID - 19

S.No.	Donor Name	Age	Gender	Nationality	Contact	E-mail	Amount
1	Sanket	21	Male	Indian	9876598765	sanket@gmail.com	4000
2	Yash	20	Male	Indian	9999999999	Yash@gmail.com	1000

Figure 4.5.3: Data of ramit’s donation included in charity database

5. Result and Analysis:

In recent years, the use of secure communication with IoT devices has grown in popularity. Smart thermostats, security cameras, and other linked IoT (Internet of Things) devices are already commonplace in both homes and offices. These gadgets can gather, process, and share data, which makes them an excellent tool for a variety of uses. However, with the growth of IoT, the need for data transmission security and privacy has elevated to the top of the priority list.

In order to ensure that data exchanged between devices is safe and cannot be intercepted or altered, secure communication with smart IoT gadgets uses encryption methods. These algorithms offer a safe route for IoT device communication, guaranteeing the security of sensitive data like personal information, financial data, and medical records.

Smart IoT objects' capacity to connect to the internet and communicate with other devices in real-time is one of the key benefits of employing them for secure communication. As a result, data may be safely shared, processed swiftly, and used to give both organizations and consumers access to real-time insights and information. Additionally, using IoT devices for secure communication can aid in lowering the expenses associated with using conventional communication channels like telephone and mail services.

The use of intelligent IoT gadgets for secure communication is not without its difficulties, though. Making ensuring the gadgets are properly secured and protected from cyberattacks is one of the primary issues. Hackers frequently target IoT devices in an effort to acquire sensitive data by taking advantage of flaws in the hardware.

Manufacturers are attempting to create more secure IoT devices that are built with security in mind in order to address these issues. In order to guarantee that IoT devices are secure and that data is appropriately protected, governments and regulatory organizations are also developing legislation and standards.

6. Conclusion:

With an estimated 20 billion devices predicted to be in use by 2023, Internet of Things (IoT) gadgets have become a crucial component of contemporary living. It is essential to make sure that these devices have a high degree of authentication and permission because they gather and send sensitive data. This will help to prevent unauthorized access and data manipulation. Using socket programming and cryptography, we have created a secure channel communication protocol in this project between an IoT device and a client.

A network communication channel between devices can be created using socket programming. To create a secure communication between the IoT device and the client in our approach, we employed sockets. We have employed cryptography, a method of safeguarding communication and data by encrypting it, to ensure that the communication channel is secure.

We have encrypted the instructions transferred from the client device to the IoT device using the RSA (Rivest-Shamir-Adleman) method, a widely used encryption mechanism. A public key and a private key are used in the popular public-key encryption technique RSA to encrypt and decode data. In our implementation, the client device encrypts the commands using the public key, and the IoT device decrypts the commands using the private key.

We've chosen MongoDB as a database for authentication in order to guarantee that only authorized users can access the IoT device. Because it is a scalable and versatile database system that can handle massive volumes of data, MongoDB is a popular option for IoT device makers. For the purposes of our solution, we've kept track of user credentials like usernames and passwords in a MongoDB database. A user's credentials are compared to the database when they want to access an IoT device to make sure they have permission to do so.

Overall, combining socket programming and cryptography, our approach offers a reliable and secure communication channel between an IoT device and a client. It is a popular option for IoT device makers due to its simplicity of integration and the usage of MongoDB as a database for authentication.

7. References:

[1] Yu, Y. S., Chen, C. W., & Yu, P. Y. , “A Secure and Intuitive IoT Architecture for Container Farm”, In *2019 IEEE Eurasia Conference on IOT, Communication and Engineering (ECICE)* (pp. 475-477). IEEE, 2019- October

[2] Gunathilake, N. A., Buchanan, W. J., & Asif, R. ,”Next Generation Lightweight Cryptography for Smart IoT Devices”, 2019

[3] Wang, H. M., Yang, Q., Ding, Z., & Poor, H. V, “Secure short-packet communications for mission-critical IoT applications”. *IEEE Transactions on Wireless Communications*, *18*(5), 2565-2578, 2019

[4] Mustafa, U., & Philip, N, “Group-based key exchange for medical IoT Device-to-Device Communication (D2D) combining secret sharing and physical layer key exchange” ,In *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)* (pp. 1-7). IEEE, 2019- January

[5] Quist-Aphetsi, K., Asare, B. T., & Nana, L, “IoT node-node secure communication using RIPEMD-128 and des”, In *2019 International Conference on Cyber Security and Internet of Things (ICSIoT)* (pp. 62-65). IEEE, 2019- May

[6] Yetis, R., & Sahingoz, O. K, “Blockchain based secure communication for IoT devices in smart cities”,In *2019 7th international Istanbul smart grids and cities congress and fair (ICSG)* (pp. 134-138). IEEE, 2019,-April

[7] Padmashree, M. G., Ranjitha, S. K., Arunalatha, J. S., & Venugopal, K. R. “CKDAC: cluster-key distribution and access control for secure communication in IoT”, In 2020 IEEE 7th Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON) (pp. 1-6). IEEE, 2020-November

[8] El Ghazi, Abdellatif, and Ait Moulay Rachid. "Machine learning and datamining methods for hybrid IoT intrusion detection." In *2020 5th international conference on cloud computing and artificial intelligence: technologies and applications (CloudTech)*, pp. 1-6. IEEE, 2020.

[9] Vishwakarma, Sandeep, and Jeetu Singh. "Social Internet of Things: The collaboration of social network and Internet of Things and its future." In *2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*, pp. 535-539. IEEE, 2020.

[10] Amjath, M. I. M., and V. Senthooran. "Secure communication using steganography in IoT environment." In *2020 2nd International Conference on Advancements in Computing (ICAC)*, vol. 1, pp. 114-119. IEEE, 2020.

[11] Pearson, Bryan, Cliff Zou, Yue Zhang, Zhen Ling, and Xinwen Fu. "SIC 2: Securing Microcontroller Based IoT Devices with Low-cost Crypto Coprocessors." In *2020 IEEE 26th International Conference on Parallel and Distributed Systems (ICPADS)*, pp. 372-381. IEEE, 2020.

[12] Nayak, Manoja Kumar, and Prasanta Kumar Swain. "MSIT: A Modified Lightweight Algorithm for Secure Internet of Things." In *2020 IEEE International Symposium on Sustainable Energy, Signal Processing and Cyber Security (iSSSC)*, pp. 1-6. IEEE, 2020.

[13] Benomar, Zakaria, Francesco Longo, Giovanni Merlino, and Antonio Puliafito. "Enabling secure RESTful web services in IoT using OpenStack." In *2020 IEEE 17th international conference on mobile ad hoc and sensor systems (MASS)*, pp. 410-417. IEEE, 2020.

[14] Hewa, Tharaka, An Braeken, Mika Ylianttila, and Madhusanka Liyanage. "Multi-access edge computing and blockchain-based secure telehealth system connected with 5G and IoT." In *GLOBECOM 2020-2020 IEEE Global Communications Conference*, pp. 1-6. IEEE, 2020.

[15]Ren, Hong, Cunhua Pan, Yansha Deng, Maged Elkashlan, and Arumugam Nallanathan. "Transmit power minimization for secure short-packet transmission in a mission-critical IoT scenario." In *GLOBECOM 2020-2020 IEEE Global Communications Conference*, pp. 1-6. IEEE, 2020.

[16] Kohnhäuser, Florian, David Meier, Florian Patzer, and Sören Finster. "On the security of iiot deployments: An investigation of secure provisioning solutions for opc ua." *IEEE access* 9 (2021): 99299-99311.

[17] Sudarsan, Sreelakshmi Vattaparambil, Olov Schelén, and Ulf Bodin. "Survey on delegated and self-contained authorization techniques in CPS and IoT." *IEEE Access* 9 (2021): 98169-98184.

[18] Dhawan, Sachin, Chinmay Chakraborty, Jaroslav Frnda, Rashmi Gupta, Arun Kumar Rana, and Subhendu Kumar Pani. "SSII: secured and high-quality steganography using intelligent hybrid optimization algorithms for IoT." *IEEE Access* 9 (2021): 87563-87578.

[19] Das, Ashok Kumar, Basudeb Bera, Mohammad Wazid, Sajjad Shaukat Jamal, and Youngho Park. "On the security of a secure and lightweight authentication scheme for next generation IoT infrastructure." *IEEE Access* 9 (2021): 71856-71867.

[20] Muzaffar, Shahzad, Owais T. Waheed, Zeyar Aung, and Ibrahim M. Elfadel. "Lightweight, Single-Clock-Cycle, Multilayer Cipher for Single-Channel IoT Communication: Design and Implementation." *IEEE Access* 9 (2021): 66723-66737.

[21] Zhang, Jiansheng, Yang Xin, Yulong Gao, Xiaohui Lei, and Yixian Yang. "Secure abe scheme for access management in blockchain-based iot." *IEEE Access* 9 (2021): 54840-54849.

[22] Huang, Kaiqing. "Secure efficient revocable large universe multi-authority attribute-based encryption for cloud-aided IoT." *IEEE Access* 9 (2021): 53576-53588.

[23]Park, Sungjin, Jaemin Park, and Jisoo Oh. "Design and implementation of trusted sensing framework for IoT environment." *Journal of Communications and Networks* 23, no. 1 (2021): 43-52.

[24] Naresh, Vankamamidi Srinivasa, Sivaranjani Reddi, Saru Kumari, VVL Divakar Allavarpu, Sachin Kumar, and Ming-Hour Yang. "Practical Identity based online/off-line signcryption scheme for secure communication in Internet of Things." *IEEE Access* 9 (2021): 21267-21278.

[25] Jin, Yong, Masahiko Tomoishi, Kenji Fujikawa, and Ved P. Kafle. "A lightweight and secure iot remote monitoring mechanism using dns with privacy preservation." In *2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, pp. 1-2. IEEE, 2019.

[26] Shahid, Jahanzeb, Rizwan Ahmad, Adnan K. Kiani, Tahir Ahmad, Saqib Saeed, and Abdullah M. Almuhaideb. "Data protection and privacy of the internet of healthcare things (IoHTs)." *Applied Sciences* 12, no. 4 (2022): 1927.

[27] Haus, Michael, Aaron Yi Ding, Qing Wang, Juhani Toivonen, Leonardo Tonetto, Sasu Tarkoma, and Jorg Ott. "Enhancing indoor IoT communication with visible light and ultrasound." In *ICC 2019-2019 IEEE International Conference on Communications (ICC)*, pp. 1-6. IEEE, 2019.

[28]Shaver, Addison, Zhipeng Liu, Niraj Thapa, Kaushik Roy, Balakrishna Gokaraju, and Xiaohon Yuan. "Anomaly based intrusion detection for iot with machine learning." In *2020 IEEE Applied Imagery Pattern Recognition Workshop (AIPR)*, pp. 1-6. IEEE, 2020.

[29] Peniak, Peter, and Emília Bubeníková. "Validation of IoT secure communication gateway for constrained devices." In *2019 International Conference on Applied Electronics (AE)*, pp. 1-5. IEEE, 2019.

[30] Hewa, Tharaka, An Braeken, Mika Ylianttila, and Madhusanka Liyanage. "Multi-access edge computing and blockchain-based secure telehealth system connected with 5G and IoT." In *GLOBECOM 2020-2020 IEEE Global Communications Conference*, pp. 1-6. IEEE, 2020.

[31] Jeribi, Fathe, Rashid Amin, Mohammed Alhameed, and Ali Tahir. "An efficient Trust Management Technique using ID3 Algorithm with Blockchain in Smart Buildings IoT." *IEEE Access* (2022).

[32] Kavitha, Athota, Vijender Busi Reddy, Ninni Singh, Vinit Kumar Gunjan, Kuruva Lakshmanna, Arfat Ahmad Khan, and Chitapong Wechtaisong. "Security in IoT Mesh Networks based on Trust Similarity." *IEEE Access* 10 (2022): 121712-121724.

[33] Prantl, Thomas, Timo Zeck, Andre Bauer, Peter Ten, Dominik Prantl, Ala Eddine Ben Yahya, Lukas Ifflaender, Alexandra Dmitrienko, Christian Krupitzer, and Samuel Kounev. "A Survey on Secure Group Communication Schemes with Focus on IoT Communication." *IEEE Access* (2022).

[34] Lee, Wai-Kong, Kyungbae Jang, Gyeongju Song, Hyunji Kim, Seong Oun Hwang, and Hwajeong Seo. "Efficient Implementation of Lightweight Hash Functions on GPU and Quantum Computers for IoT Applications." *IEEE Access* 10 (2022): 59661-59674.

[35] Ullah, Zia, Basit Raza, Habib Shah, Shahzad Khan, and Abdul Waheed. "Towards blockchain-based secure storage and trusted data sharing scheme for IoT environment." *IEEE Access* 10 (2022): 36978-36994.

[36] Said, Ghawar, Anwar Ghani, Ata Ullah, Muhammad Azeem, Muhammad Bilal, and Kyung Sup Kwak. "Light-weight secure aggregated data sharing in IoT-enabled wireless sensor networks." *IEEE Access* 10 (2022): 33571-33585.

[37] AlRubei, Subhi M., Edward Ball, and Jonathan M. Rigelsford. "A secure blockchain platform for supporting AI-enabled IoT applications at the Edge layer." *IEEE Access* 10 (2022): 18583-18595.

[38] Ahmed, Adeel, Saima Abdullah, Muhammad Bukhsh, Israr Ahmad, and Zaigham Mushtaq. "An energy-efficient data aggregation mechanism for IoT secured by blockchain." *IEEE Access* 10 (2022): 11404-11419.

[39] Javaid, Nadeem. "A secure and efficient trust model for wireless sensor IoTs using blockchain." *IEEE Access* 10 (2022): 4568-4579.

[40] Weng, Chi-Yao, Chun-Ta Li, Chin-Ling Chen, Cheng-Chi Lee, and Yong-Yuan Deng. "A lightweight anonymous authentication and secure communication scheme for FOG computing services." *IEEE Access* 9 (2021): 145522-145537.

[41] Alotaibi, Majid. "Improved blowfish algorithm-based secure routing technique in IoT-based WSN." *IEEE Access* 9 (2021): 159187-159197.

[42] Gabsi, Souhir, Yassin Kortli, Vincent Beroulle, Yann Kieffer, Areej Alasiry, and Belgacem Hamdi. "Novel ECC-based RFID mutual authentication protocol for emerging IoT applications." *IEEE access* 9 (2021): 130895-130913.

[43] Yu, Sungjin, Namsu Jho, and Youngho Park. "Lightweight three-factor-based privacy-preserving authentication scheme for iot-enabled smart homes." *IEEE Access* 9 (2021): 126186-126197.

[44] Chen, Sisheng, Ching-Chun Chang, and Isao Echizen. "Steganographic secret sharing with GAN-based face synthesis and morphing for trustworthy authentication in IoT." *IEEE Access* 9 (2021): 116427-116439.

[45] Stiawan, Deris, Meilinda Eka Suryani, Mohd Yazid Idris, Muawya N. Aldalaien, Nizar Alsharif, and Rahmat Budiarto. "Ping flood attack pattern recognition using a K-means algorithm in an Internet of Things (IoT) network." *IEEE Access* 9 (2021): 116475-116484.