**NODE LEVEL POWER AWARE SECURITY ALGORITHMS FOR CLOUD ASSISTED-IoT**

A PROJECT REPORT SUBMITTED IN PARTIAL FULFILMENT OF THE

REQUIREMENTS FOR THE AWARD OF THE DEGREE OF

BACHELOR OF TECHNOLOGY IN COMPUTER SCIENCE AND ENGINEERING

by

**Batch** – **A4**

|  |  |  |
| --- | --- | --- |
| Gandi Dhanusha (19JG1A0539) | Anjali Kumari (19JG1A0503) | |
| Dantuluri Durga Bhavani (19JG1A0528) A N L S Prasanna(20JG5A0501) | |

Under the esteemed guidance of

**Mr. S. Sumahasan**

Assistant Professor

CSE Department

**Department of Computer Science and Engineering**

**GAYATRI VIDYA PARISHAD COLLEGE OF ENGINEERING FOR WOMEN**

[Approved by AICTE NEW DELHI, Affiliated to JNTUK Kakinada]

[Accredited by National Board of Accreditation (NBA) for B.Tech. CSE, ECE & IT – Valid from 2019-22 to 2022-25]

[Accredited by National Assessment and Accreditation Council [NAAC] with A Grade – Valid from 2022-27]

Kommadi, Madhurawada, Visakhapatnam – 530048

**2019 – 2023**

**GAYATRI VIDYA PARISHAD COLLEGE OF ENGINEERING FOR WOMEN**

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**CERTIFICATE**

****

This is to certify that the project report titled **“NODE LEVEL POWER AWARE SECURITY ALGORITHMS FOR CLOUD ASSISTED-IoT”** is a bonafide work of following IV B.Tech. students in the Department of Computer Science and Engineering, Gayatri Vidya Parishad College of Engineering for Women affiliated to JNT University, Kakinada during the academic year 2021- 2022, in fulfilment of the requirement for the award of the degree of Bachelor of Technology of this university.

|  |  |
| --- | --- |
| Gandi Dhanusha (19JG1A0539) | Anjali Kumari (19JG1A0503) |
| Dantuluri Durga Bhavani (19JG1A0528) A N L S Prasanna (20JG1A0501) | |

|  |  |
| --- | --- |
| **Mr. S. Sumahasan** | **Dr. P. V. S. Lakshmi Jagadamba** |
| Assistant Professor | Professor |
| (Internal Guide) | (Head of the department) |

**External Examiner**

# **ACKNOWLEDGEMENT**

The satisfaction that accompanies the successful completion of any task would be incomplete without the mention of people who made it possible and whose constant guidance and encouragement crown all the efforts with success.

We feel elated to extend our sincere gratitude to **Mr. S. Sumahasan,** Asssistant Professor for encouragement all the way during analysis of the project. Her annotations, insinuations and criticisms are the key behind the successful completion of the thesis and for providing us all the required facilities.

We express our deep sense of gratitude and thanks to **Dr. P. V. S. Lakshmi Jagadamba**, Professor and Head of the Department of Computer Science and Engineering for her guidance and for expressing her valuable and grateful opinions in the project for its development and for providing lab sessions and extra hours to complete the project.

We would like to take the opportunity to express our profound sense of gratitude to the revered Principal, **Dr. R. K. Goswami** for allowing us to utilize the college resources thereby facilitating the successful completion of our thesis.

We would like to take this opportunity to express our profound sense of gratitude to Vice Principal, **Dr. G. Sudheer** for allowing us to utilize the college resources thereby facilitating the successful completion of our thesis and not but the least we are also thankful to both teaching and non-teaching faculty of the Department of Computer Science and Engineering for giving valuable suggestions for our project.

# **TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| **TOPICS** | **Page No.** | |
| ABSTRACT | i | |
| LIST OF FIGURES | ii | |
| LIST OF TABLES | iii | |
| LIST OF SCREENS | iv | |
| 1. **INTRODUCTION** | **1** | |
| * 1. Motivation of the Project | 1 | |
| * 1. Problem Definition | 1 | |
| * 1. Objective of the Project | 2 | |
| * 1. Limitations of the Project | 2 | |
| * 1. Organisation of the Project | 2 | |
| 1. **LITERATURE SURVEY** | **3** | |
| 1. Introduction | 3 | |
| 1. Existing System | 16 | |
| 2.3 Disadvantages of Existing System | 16 | |
| 1. Proposed System | 17 | |
| 1. System Architecture | 18 | |
| 1. Conclusion | 18 | |
| 1. **REQUIREMENT ANALYSIS** | **19** | |
| 1. System Overview | 19 | |
| 1. Software Requirements | 19 | |
| 1. Hardware Requirements | 21 | |
| 1. **METHODOLOGY** | **23** | |
| 1. Introduction | 23 | |
| 1. Modules Identified | 23 | |
| 1. Conclusion | 26 | |
| 1. **IMPLEMENTATION AND RESULTS** | **27** | |
| 5.1 Introduction | | 27 | |
| 5.2 Output Screens | | 27 | |
| 5.2.1. Algorithm Implementation | | 27 | |
| 5.2.2. Node Connection | | 29 | |
| 5.2.3. Frontend | | 30 | |
| 5.3 Conclusion | | 31 | |
| 1. **FUTURE WORK** | **32** | |
| 1. **REFERENCES** | **33** | |

# 

# **ABSTRACT**

# The Internet of Things, which is the fastest-growing technology, will advance in defense, agriculture and medical electronics as well. IoT is now faced with new security issues for data mutuality between two parties as a result of the cloud's influence, which are novel in this study and have not yet been resolved by conventional methods. In order to ensure data security when collecting, storing, and accessing IoT data via the cloud while taking into consideration the ongoing rise in users, this work undertakes a methodical analysis using a secure cloud assisted IoT data management strategy. A node-level power-aware security mechanism is used in the proposed system. As a result, a secure IoT using our technology might withstand most data confidentiality threats from both insiders and outsiders of the IoT. Lightweight security methods for low-power IoT devices with smaller key sizes, lower power consumption and lower memory and transmission capacity reserve are used to achieve security.

Keywords— Encryption, Decryption, IoT, Cloud, Node, Security, Node MCU.

# **List of figures**

|  |  |  |  |
| --- | --- | --- | --- |
| **S.No.** | **Figure No.** | **Figure Name** | **Page No.** |
| 1 | Figure No:1 | Man-in-the-Middle Attack | 16 |
| 2 | Figure No:2 | Proposed System | 17 |
| 3 | Figure No:3 | System Architecture | 18 |
| 4 | Figure No:4 | Pulse Sensor | 21 |
| 5 | Figure No:5 | Node MCu | 22 |
| 6 | Figure No:6 | Heart Monitoring System | 24 |
| 7 | Figure No:7 | Application of Algorithms | 25 |
| 8 | Figure No:8 | Node Connection | 29 |

# **List of Tables**

|  |  |  |  |
| --- | --- | --- | --- |
| **S.No.** | **Table No.** | **Figure Name** | **Page No.** |
| 1 | Table No:1 | A Comparative Study of Various Related Works | 8 |

# **LIST OF SCREENS**

|  |  |  |  |
| --- | --- | --- | --- |
| **S.No.** | **Screen No.** | **Screen Name** | **Page No.** |
| 1. | Screen 1. | Output Screen 1 | 30 |
| 2. | Screen 2. | Output Screen 2 | 30 |
| 3. | Screen 3. | Output Screen 3 | 31 |

# **INTRODUCTION**

**1.1 MOTIVATION OF THE PROJECT**

In many nations, heart disease is one of the leading causes of mortality, accounting for approximately 15 million fatalities yearly. In addition, cardiovascular illness disables a large number of people. The time between the onset of the first sign of any heart problem and the need for medical help varies greatly across people and can be deadly. One critical inference drawn from epidemiological data is that deployment of resources for early detection and treatment of heart disease has a higher potential of reducing fatality associated with cardiac disease than improved care after hospitalization. Hence new strategies are needed in order to reduce time before treatment. Monitoring of patients is one possible solution. This project can be used in hospitals (Calling Ambulance.) and also for patients who can be under continuous monitoring while traveling from place to place (using heart rate band).

**1.2 PROBLEM DEFINITION**

According to the WHO, CVD (Cardiovascular disease) kills 17.9 million people worldwide, accounting for 31% of all deaths. More than four out of five CVD deaths are due to heart attacks and strokes, and one third of these deaths occur prematurely in people under 70 years of age. Therefore, a method to prevent or assist in the reduction of human life losses. Heat stroke can swiftly harm your brain, heart, kidneys, and muscles if left untreated. The longer you wait to get treatment, the more severe the damage will be, increasing your risk of developing major complications or passing away. The IoT ecosystem has significant challenges related to secure communication, including data integrity and data confidentially in the current trends in cloud-based IOT. To address the security challenges and operate with low-powered, compact devices at the end point (Node) level in a Cloud-based IoT ecosystem, there is a significant need for node-level power-aware security algorithms. Once the data is stored on the cloud, only then is cryptography employed. However, while the raw data is being sent from the node to the cloud, data breaches can occur and there is a possibility of Man-in-the-Middle attack (MiTM).

**1.3 OBJECTIVE OF THE PROJECT**

We achieve this goal by developing the power-aware security to the data at the node itself where the data is captured and stored. We implement certain encryption algorithms in the node level itself to encrypt the data and then send it to the cloud for storage. When the user wants to receive the data the data is decrypted at the users side and then the requested data is shown to the user.

* 1. **LIMITATIONS OF THE PROJECT**
* Even a small mistake in configuration or coding may result in a diminishment of some or all of the cryptographic security.
* There needs to be very careful attention paid to any hybrid cryptographic implementation in order to ensure that it does not make us less secure.

**1.5 ORGANIZATION OF DOCUMENTATION**

The report is structured as follows:

Chapter 1 contains the Introduction of the project, and it contains an overview of the project.

Chapter 2, provides a literature study, and crucial variables for making stronger contributions are indicated.

Chapter 3, the need of requirement analysis for hardware and software requirements is underlined.

Chapter 4, documents the methodology employed in the project.

Chapter 5, contains the implementation and results.

Chapter 6, describes the additional work that must be added to the project.

# **2. LITERATURE SURVEY**

**2.1 INTRODUCTION**

John A. Stankovic, Research Directions for the Internet of Things, concluded that new research problems arise due to the large scale of devices, the connection of the physical and cyber worlds, the openness of the systems, and continuing problems of privacy and security [1].

Tarun Kumar Goyal et al., Lightweight Security Algorithm for Low Power IoT devices, observed that in today’s era of the omnipresent computing, the Internet has turned into the primary method of information correspondence. In such a domain, giving security to gadgets, Elliptic Curve Diffie Hellman (EC-DH) Algorithm has received achieved significance in view of its features like low power, lightweight & robustness, which is reasonable for IoT gadgets [2]. We have performed comparisons with respect to power, area, and timing etc. for various algorithms like Diffie-Hellman, Rivest-Shamir-Adleman and ECDH. The Diffie-Hellman plan is one of the exchanging key cryptosystems.

Ravi Kishore Kodali et al., ECDH based Security Model for IoT using ESP8266, concluded that implementing an algorithm like Elliptic Curve Diffie Hellman Key exchange algorithm on a potential device like ESP8266 adds to the advantage [3]. With the IoT going to be the next Industrial Revolution, secure and low-cost Wi-Fi device plays a vital role. This can be used in many applications such as Mesh networks, Home automation, Smart power meters, Wearable devices, Security ID tags and Sensor networks.

Aditya Poduval et al., Secure File Storage on Cloud using Hybrid Cryptography, observed that cloud storage issues of data security are solved using cryptography and steganography techniques [4]. Data security is achieved using RC6, 3DES and AES algorithm. Key information is safely stored using LSB technique (Steganography).

Sreeja Rajesh et al., A Secure and Efficient Lightweight Symmetric Encryption Scheme for Transfer of Text Files between Embedded IoT Devices, proposed that a novel tiny symmetric encryption algorithm (NTSA) provides enhanced security for the transfer of text files through the IoT network by introducing additional key confusions dynamically for each round of encryption [5]. Experiments are carried out to analyze the avalanche effect, encryption and decryption time of NTSA in an IoT network including embedded devices. The results show that the proposed NTSA algorithm is much more secure and efficient compared to state-of-the-art existing encryption algorithms.

Joao Mesquita et al., Assessing the ESP8266 WiFi module for the Internet of Things, showed how the automatic interaction with the WiFi infrastructure and its configuration in terms of beacon interval and DTIM period affects the power consumption and the effectiveness of the sleep modes [6].

Vishwanath S Mahalle at al., Enhancing the data security in cloud by implementing hybrid (RSA & AES) encryption algorithm, this paper mainly focuses on the following key tasks: 1. Secure Upload of data on cloud such that even the administrator is unaware of the contents. 2. Secure Download of data in such a way that the integrity of data is maintained. 3. Proper usage and sharing of the public, private and secret keys involved for encryption and decryption [7]. The use of a single key for both encryption and decryption is very prone to malicious attacks. But in hybrid algorithm, this problem is solved by the use of three separate keys each for encryption as well as decryption. Out of the three keys one is the public key, which is made available to all, the second one is the private key which lies only with the user. In this way, both the secure upload as well as secure download of the data is facilitated using the two respective keys. Also, the key generation technique used in this paper is unique in its own way. This has helped in avoiding any chances of repeated or redundant key.

Zengqiang Wu et al., ElGamal Algorithm for Encryption of Data Transmission, this paper proposes one security mode to transmit important information [8]. At the same time, security of data transmission is improved by text encryption and image encryption implemented in ElGamal public key encryption algorithm.

Sanaz Amanlou, Lightweight Security Mechanism over MQTT Protocol for IoT Devices, proposed a lightweight authentication and encryption mechanism for IoT constrained devices [9] . This mechanism uses ECDHE-PSK which is the Transport Layer Security (TLS) authentication algorithm over Message Queuing Telemetry Transport (MQTT) Protocol.

Aliasghar Azma et al., Research and Development on Cloud Computing, concluded that cloud computing can surely make the business world more convenient and efficient and it is even potential to bring about revolutionary changes to the human society, people would use more and more ‘Web-Based’ applications instead of the current ‘Desktop-Based’ ones [10].

Jorg Henkel et al., Ultra-Low Power and Dependability for IoT Devices, discussed and summarized the IoT paradigm with a special focus on energy consumption and methodologies for its minimization [11]. IoT covers an ever-increasing range of applications, e.g., health-care monitoring, smart homes and buildings, etc.

Neal Koblitz, Elliptic Curve Cryptosystems, discussed analogs based on elliptic curves over finite fields of public key cryptosystems which use the multiplicative group of a finite field [12]. These elliptic curve cryptosystems may be more secure, because the analog of the discrete logarithm problem on elliptic curves is likely to be harder than the classical discrete logarithm problem, especially over GF (2").

Xianping Wu et al., The Design and Implementation of a Smartphone Payment System based on Limited-used Key Generation Scheme, proposed a new security enhancement on smart phone using the Limited used Key generation technique based on the KSL protocol [13].

Syed Farhan Alam Zaidi et al., in A Survey on Security for Smartphone Device, reviewed the threats, vulnerabilities, attacks and their solutions over the period of 2010-2015 with a special focus on smartphones [14]. Attacks are categorized into two types, i.e., old attack and new attacks. With this categorization, they aimed to provide an easy and concise view of different attacks and the possible solutions to improve smartphone security. Secondly, analysed their findings and estimate the market growth of different operating systems for the smartphone in coming years. Furthermore, we estimate the malware growth and forecast the world in 2020.

Ms. Moonmoon Karmakar et al., Authentication Using Kerberos It is designed in the form of architecture and models, and categorized in the form of types and services [15]. The service provider provides service and user also access the services, this all needs some security so that data cannot be loss or damage. In our work we will be studying about the strong security in cloud environment using Kerberos authentication protocol.

Eman Shaikh et al., Internet of Things (IoT): Security and Privacy Threats, put forward the different security and privacy concerns that an IoT environment is facing and the existing mechanisms used for its protection [16]. The paper mainly focuses on the IoT privacy and security features such as the IAS-octave security requirements, security and privacy threats and the solutions that need to be maintained to avoid these security and privacy threats.

Sarmad Nozad Mahmood et al., ESP 8266 Node MCU Based Weather Monitoring System, primarily blends two-study fields based on control systems with data acquisition methodology and builds a database system to produce the data according to the chosen attributes [17]. The sensors for weather station were used to quantify and store data about temperature, humidity, and wind speed. The collected data can be represented as direct and indirect in two forms owing to the regular reading and preservation of the data as a specific database system respectively. The new technologies for the development of databases are considered the main challenge of this research.

Ullah, S., & Zahilah, R. (2021). Curve25519 based lightweight end-to-end encryption in resource constrained autonomous 8-bit IoT devices. Cybersecurity, 4(1). doi:10.1186/s42400-021-00078-6, Curve25519 based lightweight end-to-end encryption in resource constrained autonomous 8-bit IoT devices, presents an encryption technique, implemented on a resource constrained IoT device (AVR ATmega2560) through utilizing fast execution and less memory consumption properties of curve25519 in a novel and efficient lightweight hash function [18]. The hash function utilizes GMP library for multi-precision arithmetic calculations and pre-calculated curve points to devise a good cipher block using ECDH based key exchange protocols and large random prime number generator function.

G. Ismaeel and M. Q. Kamal, Worldwide auto-mobi: Arduino IoT home automation system for IR devices, this paper proposed an Internet of Things (IoT ) home automated system in two categories [19] , the hardware via a device named Worldwide Automobi and software has been designed to automate a favorite used devices such as TV, SAT, DVD addition to any other devices that can be controlled by an IR signal, locally and anywhere (wide world) via a hybrid mobile application will reduce the number of used controllers in the house by using a single mobile software that control devices using Internet via a WiFi module ESP8266 based on Arduino UNO.

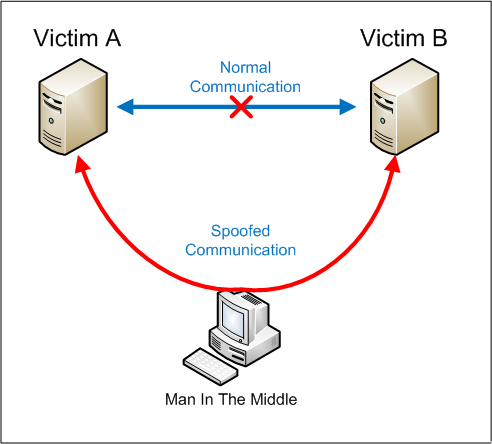
Chunlu Wang et al., CB-CDP: A Cloud Based Continuous Data Protection System, describes the architecture of CB-CDP, its feather set and the usage of distributed storage on CDP [20]. Taking advantage of MooseFS, CB-CDP will have unlimited storage. To make this feature come true, this system takes in some new features.

**Table 1: Table for Literature Survey**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Author** | **Year of Publication** | **Title** | **Proposed Framework** | **Outcome** |
| John A. Stankovic et al. | 2014 | Research Directions for the Internet of Things | To provide a basis for discussing open research problems in IoT, a vision for how IoT could change the world in the distant future and eight key research topics are enumerated and research problems within these topics are discussed. | Knowledge of what are the problems in IoT. |
| Tarun Kumar Goyal et al. | 2016 | Lightweight Security Algorithm for Low power IoT Devices | ECDH and Diffie-Hellman algorithms are compared on the basis of power, area and performance. The comparison is based on metrics obtained, after implementing the algorithms using 90 nm UMC Faraday library. The ECDH algorithm is found to be better than others as far as power and area are concerned. | Comparison between ECDH and ElGamal Algorithm |
| Ravi Kishore Kodali et al. | 2016 | ECDH based Security Model for IoT using ESP8266 | In this paper, ECDH key exchange on NIST P-192 curve for secured communication between ESP8266 modules has been discussed and implemented using NodeMCU. |  |
| Aditya Poduval et al. | 2019 | Secure File Storage on Cloud Hybrid Cryptography | Major concern regarding storage of data online that is on the cloud is the Security. A single technique or algorithm alone cannot provide high-level security. In this proposed system 3DES (Triple Data Encryption Standard), RC6 (Rivest Cipher 6) and AES (Advanced Encryption Standard) algorithms are used to provide security to data. | A single technique or algorithm alone cannot provide high-level security |
| Sreeja Rajesh et al. | 2019 | A Secure and Efficient Lightweight Symmetric Encryption Scheme for Transfer of Text Files between Embedded IoT Devices | This paper proposes a novel tiny symmetric encryption algorithm (NTSA) which provides enhanced security for the transfer of text files through the IoT network by introducing additional key confusions dynamically for each round of encryption. | Knowledge of security techniques. |
| Joao Mesquita et al. | 2014 | Assessing the ESP8266 WiFi module for the Internet of Things | The blockchain encryption algorithm is used. The most important features are Easy and quick communication, Data immutability, Censorship resistance, Decentralized storage, Data Security. | Data immutability, Censorship resistance, Decentralized storage, Data Security. |
|  | 2014 | Enhancing the Data Security in Cloud by Implementing Hybrid (RSA & AES) Encryption Algorithm | This paper presents Hybrid (RSA & AES) encryption algorithm to safeguard data security in Cloud. | Knowledge to safeguard data security |
| Zengqiang Wu et al. | 2014 | ElGamal Algorithm for Encryption of Data Transmission | This article explores ElGamal public key encryption algorithm that is put practice into information transmission. Base on it, it also aims to achieve the text encryption and decryption, image encryption and decryption so as to guarantee information transmission. | Achieved the text encryption and decryption, image encryption and decryption so as to guarantee information transmission. |
| Sanaz Amanlou et al. | 2020 | Lightweight Security Mechanism over MQTT Protocol for IoT Devices | The main objective of this paper is to propose a lightweight authentication and encryption mechanism for IoT constrained devices. | Lightweight authentication and encryption mechanism for IoT constrained devices. |
| Aliasghar Azma et al. | 2021 | Research And Development on Cloud Computing | In this article, characteristics of cloud computing will be discussed with several examples, in order to show that how cloud computing will make the business world simpler, more efficient, and more specialized. | Showed that how cloud computing will make the business world simpler, more efficient, and more specialized. |
| Jorg Henkal et al. | 2017 | Ultra-Low Power and Dependability for IoT Devices | This paper discuss and summarize the IoT paradigm with a special focus on energy consumption and methodologies for its minimization. Furthermore, it also discuss about reliability in the context of IoT devices | Power-Aware Mechanisms |
| Neal Koblitz | 1987 | Elliptic Curve Cryptosystems | This paper discussed analogs based on elliptic curves over finite fields of public key cryptosystems which use the multiplicative group of a finite field. | Knowledge of Elliptic Curve Cryptography |
| Xianping Wu et al. | 2006 | The Design and Implementation of a Smartphone Payment System based on Limited-used Key Generation Scheme | This paper proposes a new security enhancement on smart phone using the Limited-used Key generation technique based on the KSL protocol. | Knowledge of protocols. |
| Syed Farhan Alam Zaidi et al. | 2016 | A Survey on Security for Smartphone Device | This paper firstly, review the threats, vulnerabilities, attacks and their solutions over the period of 2010-2015 with a special focus on smartphones. Secondly, analyse findings and estimate the market growth of different operating systems for the smartphone in coming years. Furthermore, it estimates the malware growth and forecast the world in 2020 | Estimates the malware growth and forecast the world |
| Shubhangi Verma et al. | 2018 | Strong Authentication Policy for Cloud Computing Environment Modified Kerberos Authentication Protocol | The problem and algorithm proposed is based on security of data in cloud environment. Where, modified algorithm of Kerberos is used. Along with-it RSA and ECC is also used this approach is used for encryption and decryption. | . it shows the affects and lifestyle of every individual rendered with IOT smart devices or the home automated system |
| Eman Shaikh et al. | 2019 | Internet of Things (IoT): Security and Privacy Threats | The paper mainly focuses on the IoT privacy and security features such as the IAS-octave security requirements, security and privacy threats and the solutions that need to be maintained to avoid these security and privacy threats. | It uses kill tag method and Faraday net to eliminate RFID |
| Sarmad Nozad Mahmood et al. | 2020 | ESP 8266 Node MCU Based Weather Monitoring System | This paper primarily blends two-study fields based on control systems with data acquisition methodology and builds a database system to produce the data according to the chosen attributes. The sensors for weather station were used to quantify and store data about temperature, humidity, and wind speed. | It uses NET PI web server to show the output and can be adjust to the suitable gauges. |
| Shafi Ullah et al. | 2021 | Curve25519 based lightweight end-to-end encryption in resource constrained autonomous 8-bit IoT devices | This article presents an encryption technique, implemented on a resource constrained IoT device through utilizing fast execution and less memory consumption properties of curve25519 in a novel and efficient lightweight hash function. | It uses NET PI web server to show the output and can be adjust to the suitable gauges. |
| Ayad Ghany Ismaeel et al. | 2017 | Worldwide Auto-mobi: Arduino IoT Home Automation System for IR Devices | This paper proposed an Internet of Things (IoT) home automated system in two categories, the hardware via a device named Worldwide Auto-mobi and software has been designed to automate a favorite used device | The mobile cloud app has been built to protect the home automated system according to what signal is been provided. |
| Chunlu Wang et al. | 2013 | CB-CDP: A Cloud Based Continuous Data Protection System | This paper describes the architecture of CB-CDP, its feather set and the usage of distributed storage on CDP. | It uses “Rsync Algorithm” virtually taking less storage with improved storage method to provide fast recovery and uses MooseFS to overcome defects of traditional CDS |

* 1. **EXISTING SYSTEM**

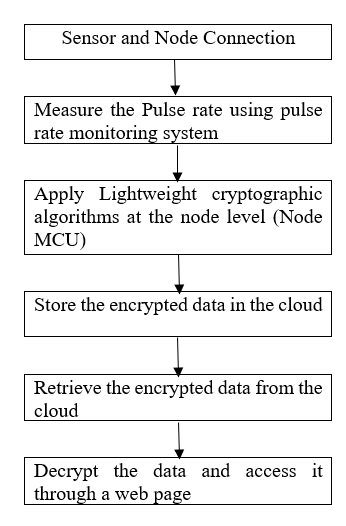
The security is provided to the data in the cloud when data is transferred from one point to the other. Data is encrypted using various symmetric cryptographic algorithms. The encryption is performed only at the cloud level. This can lead to security breaches while uploading the data to the cloud. Also, the power consumption is high in the existing system.



**Fig 1:** Man-in-the-Middle Attack

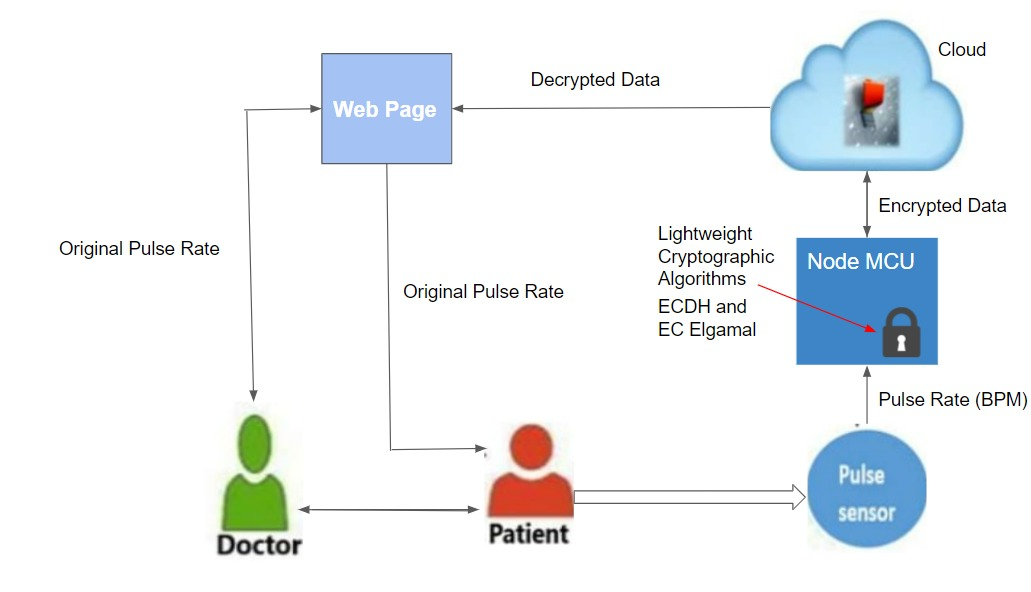
* 1. **DISADVANTAGES OF EXISTING SYSTEM**
* The consumption of power in the existing system is high and so it is not power- aware.
* Security to the data is provided after reaching the cloud leading to Man-in-the-middle Attack.
* Even a small mistake in configuration or coding may result in a diminishment of some or all of the cryptographic security.
  1. **PROPOSED SYSTEM**

The proposed system is mainly divided into four parts: Designing a pulse monitoring system, providing security at node level, uploading encrypted data into cloud, accessing the data through webpage.

****

**Fig. 2**: Flow of Proposed System

**2.5 SYSTEM ARCHITECTURE**



**Fig.3**: System Architechure

**2.6 CONCLUSION**

Different papers along with knowledge resources are researched and thus the proposed system is made by incorporating different features from the survey of research papers.

# **3. REQUIREMENT ANALYSIS**

**3.1 INTRODUCTION**

The system requirements can be hardware and software. These system requirements are also known as prerequisites. Each computer system requires certain hardware components or software resources to be present on a computer. The need for system requirements increases with the increase in demand for higher processor power and resources of newer versions.

* 1. **SOFTWARE REQUIREMENTS**
* PostgreSQL
* Firebase
* Python
* PyCharm
* Django

1. **PostgreSQL**

PostgreSQL is a powerful object-relational database system that is free and open source. It has over 20 years of active development and a proven architecture, earning it a strong reputation for dependability, data integrity, and correctness. PostgreSQL is compatible with all major operating systems, including Linux, UNIX, and Windows. It can handle text, images, sounds, and video, and has programming interfaces for C/C++, Java, Perl, Python, Ruby, and Open Database Connectivity (ODBC). Many web, mobile, and analytics applications use PostgreSQL as their primary data store or data warehouse. PostgreSQL has a long history of supporting advanced data types, and it offers the same level of performance optimization as its commercial database counterparts, such as Oracle and SQL Server.

1. **Firebase**

Follow the below steps to install Firebase

**Step 1:** Create a Firebase project and register your app

**Step 2:** Install the SDK and initialize Firebase

1. **Python**

Python is a high-level, interpreted scripting language created in the late 1980s by Guido van Rossum at the Netherlands National Research Institute for Mathematics and Computer Science. The first version was posted to the alt. sources newsgroup in 1991, and version 1.0 was released in 1994. Python 2.0 was released in 2000, and the 2.x versions were the most common until December 2008. At the time, the development team decided to release version 3.0, which included a few relatively minor but significant changes that were not backward compatible with the 2.x versions. Python 2 and 3 are very similar, and some Python 3 features have been backported to Python 2. However, they are still incompatible in general. Python 2 and 3 have both been maintained and developed, with both receiving periodic release updates.

1. **Django**

Django is a Python-based web framework, free and open-source, that follows the model–template–views architectural pattern. It is maintained by the Django Software Foundation, an independent organization established in the US as a 501 non-profit.  Django is a high-level Python web framework that enables rapid development of secure and maintainable websites. Built by experienced developers, Django takes care of much of the hassle of web development, so you can focus on writing your app without needing to reinvent the wheel.

**3.3 HARDWARE REQUIREMENTS**

* Pulse Sensor
* NodeMCU
* Connecting Wires

1. **Pulse Sensor**

Pulse sensor in Fig. 13. is an open-source heart rate monitor used to monitor non-invasive heart rate. It monitors real-time pulses and calculates BPM using Arduino algorithms. This sensor has two sides, the front of which is shaped like a heart and is the side that will be connected to the skin. As illustrated in the diagram below, the pulse sensors have three pins.



**Fig. 4:** Pulse Sensor

If the front side is facing you, the most left pin is GND, while the center one is the input voltage, which will be connected to the Arduino's +5v. The final one will be used to output electricity and will be connected to the Arduino's analogue pins.

The pulse sensor turns physical PPG signals into electrical signals. The sensor generates a raw signal of analogue voltage variations, which it amplifies and normalizes at v/2. With each pulse, a pulse wave passes along the arteries to the tissues where the pulse sensor is connected.

1. **NodeMCU**

NodeMCU is an open-source LUA based firmware developed for the ESP8266 wifi chip. By exploring functionality with the ESP8266 chip, NodeMCU firmware comes with the ESP8266 Development board/kit i.e. NodeMCU Development board.



**Fig. 5.** NodeMCU

# **METHODOLOGY**

* 1. **INTRODUCTION**

To make things easier, complex things are usually divided into sample codes called "modules.". A module is a file with the extension .py and contains executable Python code. A module contains several Python statements and expressions. Most modules are designed to be concise and unambiguous, and they are intended to solve specific developer problems.

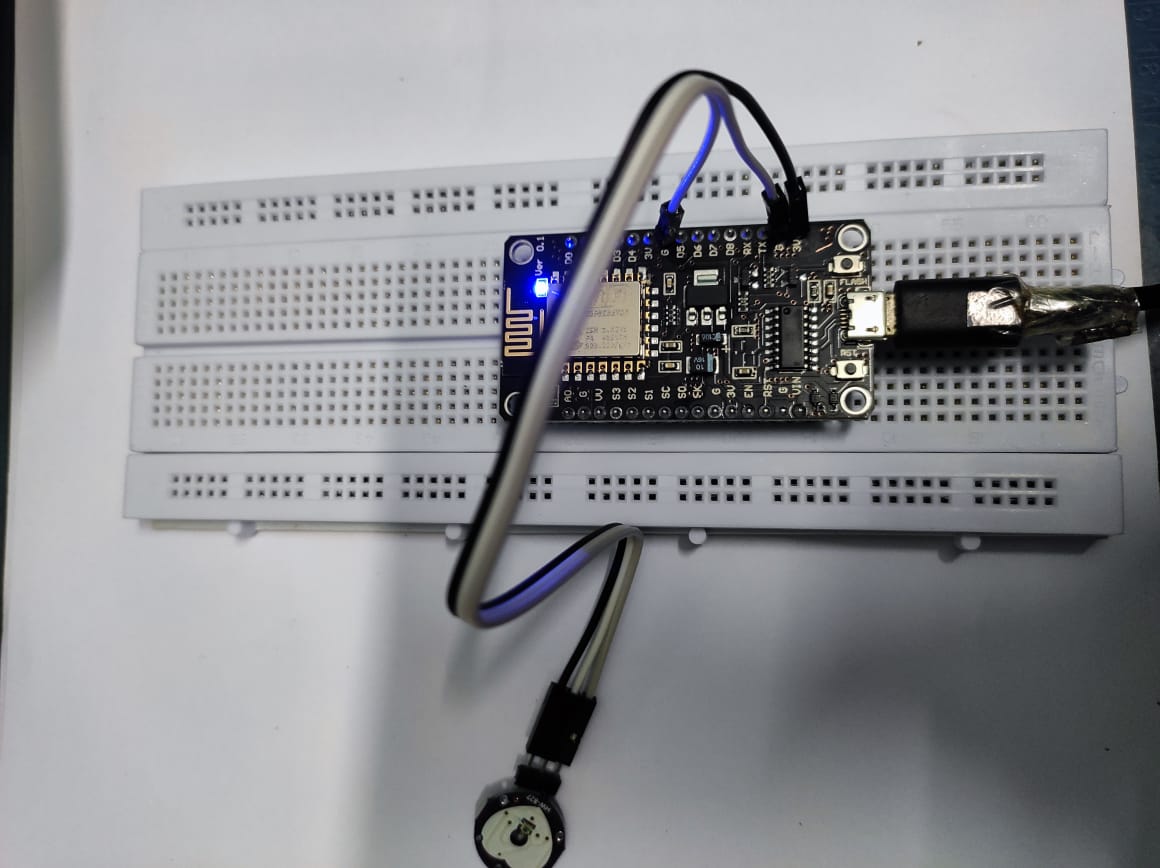
* 1. **MODULES IDENTIFIED**

This work is mainly divided into four parts:

* Designing a pulse monitoring system.
* Providing security at node level.
* Uploading encrypted data into cloud.
* Accessing the data through webpage.

**Part1: Pulse monitoring system**

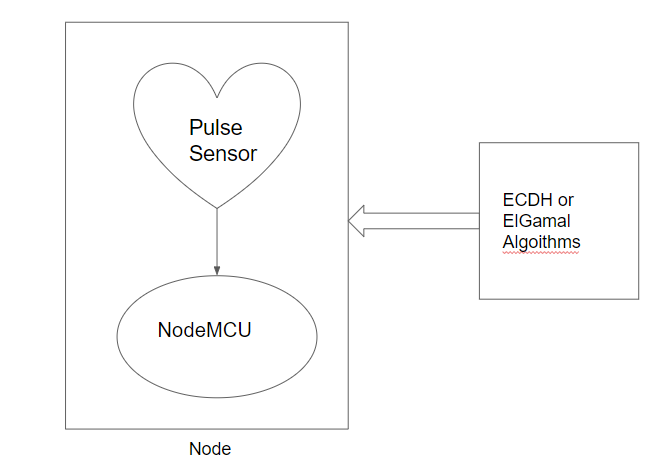
A pulse sensor is an electronic device that measures the heart rate, or the pace at which the heart beats. The main things we do to stay healthy are monitor our body temperature, heart rate, and blood pressure. To monitor the Arterial Pressure or Blood Pressure, we utilise thermometers and a sphygmomanometer to measure the body temperature. Heart rate can be measured in two ways: one by manually checking the pulse at the wrists or neck, and the other by using a Pulse Sensor. We created a Heart Rate Monitor System in Fig. 10. with NodeMCU and a Pulse Sensor in this project.



**Fig. 6:** Heart Monitoring System

In Fig.6, node comprises of the NodeMCU, pulse sensor, a bread board and some connectors. NodeMCU is an open-source LUA based firmware developed for the ESP8266 wifi chip. By exploring functionality with the ESP8266 chip, NodeMCU firmware comes with the ESP8266 Development board/kit i.e. NodeMCU Development board.A pulse wave is the change in the volume of a blood vessel that occurs when the heart pumps blood, and a detector that monitors this volume change is called a pulse sensor. The heart-beat sensor collects data and stores it in the Raspberry PI. Here we implement data encryption algorithms like Elliptic curve Cryptographic Algorithm (ECC), Elliptic-curve Diffie–Hellman (ECDH) and encrypt the data at the Node and then send the data to the cloud.

**Part 2: Providing security at the node level**

****

**Fig 7:** Application of Algorithms

**Part 3: Uploading Encrypted data into the cloud**

Data encryption is a way of translating data from plaintext (unencrypted) to ciphertext (encrypted). Users can access encrypted data with an encryption key and decrypted data with a decryption key in Fig. 12. Protecting your data. We use Firebase cloud for storing data. Firebase is a platform developed by Google for creating mobile and web applications. It was originally an independent company founded in 2011. In 2014, Google acquired the platform and it is now their flagship offering for app development. Once the data is encrypted at the node, the data is uploaded to the cloud which is stored in the form of tables that can be retrieved by the user whenever needed or necessary.

**Part 4: Accessing the data through the web page**

Decryption is taking encoded or encrypted text or other data and converting it back into text you or the computer can read and understand. The recipient of decryption receives a prompt or window in which a password can be entered to access the encrypted data. For decryption, the system extracts and converts the garbled data and transforms it into words and images that are easily understandable not only by a reader but also by a system. Decryption can be done manually or automatically. The user requests specific data through the web page.

* 1. **CONCLUSION**

Every system has its own advantages and disadvantages. As the proposed system we have chosen is objective specific, it is dependent on the factor we need to justify and criticality of the system. Here the proposed system is more secure in providing data storage than the existing system.

**5. IMPLEMENTATION & RESULTS**

**5.1 INTRODUCTION**

The project's implementation stage is when the theoretical design is translated into a workable system. As a result, it can be seen as the most crucial stage in ensuring the success of a new system and giving the user confidence that the system will work and be effective. The implementation step entails meticulous planning, research of the existing system and its implementation limitations, designing of changeover methods, and evaluation of changeover methods.

**5.2 OUTPUT SCREENS**

**5.2.1. Algorithm Implementation**

**#ECDH Algorithm Implementation**

from tinyec import registry

import secrets

def compress(pubKey):

return hex(pubKey.x) + hex(pubKey.y % 2)[2:]

curve = registry.get\_curve('brainpoolP256r1')

alicePrivKey = secrets.randbelow(curve.field.n)

alicePubKey = alicePrivKey \* curve.g

print("Alice public key:", compress(alicePubKey))

bobPrivKey = secrets.randbelow(curve.field.n)

bobPubKey = bobPrivKey \* curve.g

print("Bob public key:", compress(bobPubKey))

print("Now exchange the public keys (e.g. through Internet)")

aliceSharedKey = alicePrivKey \* bobPubKey

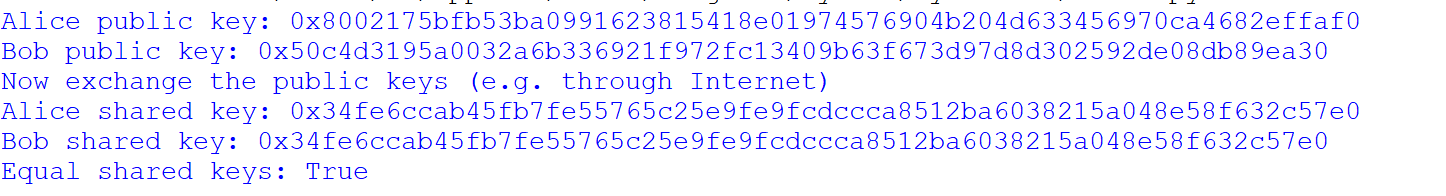
print("Alice shared key:", compress(aliceSharedKey))

bobSharedKey = bobPrivKey \* alicePubKey

print("Bob shared key:", compress(bobSharedKey))

print("Equal shared keys:", aliceSharedKey == bobSharedKey)

**#Output:**



**#DH Algorithm Implementation**

from random import randint

if \_\_name\_\_ == '\_\_main\_\_':

P = 23

G = 9

print('The Value of P is :%d'%(P))

print('The Value of G is :%d'%(G))

a = 4

print('The Private Key a for Alice is :%d'%(a))

x = int(pow(G,a,P))

b = 3

print('The Private Key b for Bob is :%d'%(b))

y = int(pow(G,b,P))

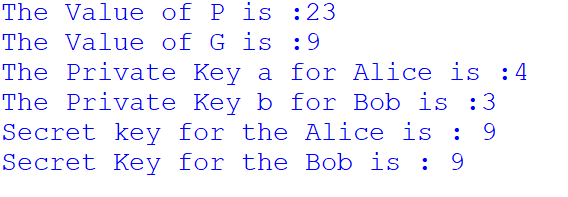
ka = int(pow(y,a,P))

kb = int(pow(x,b,P))

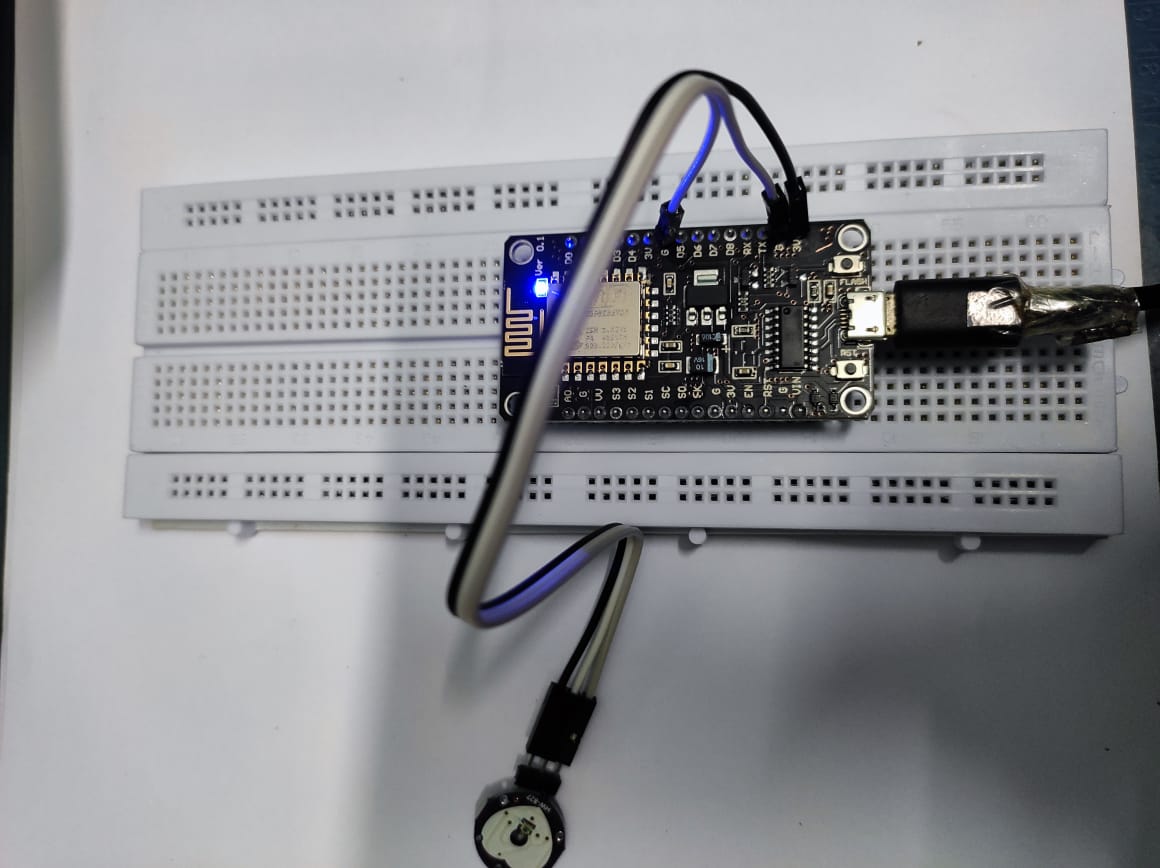
print('Secret key for the Alice is : %d'%(ka))

print('Secret Key for the Bob is : %d'%(kb))

**#Output**



**5.2.2. Node Connection**



**Fig 8:** Node Connection

**5.2.3. FRONTEND**

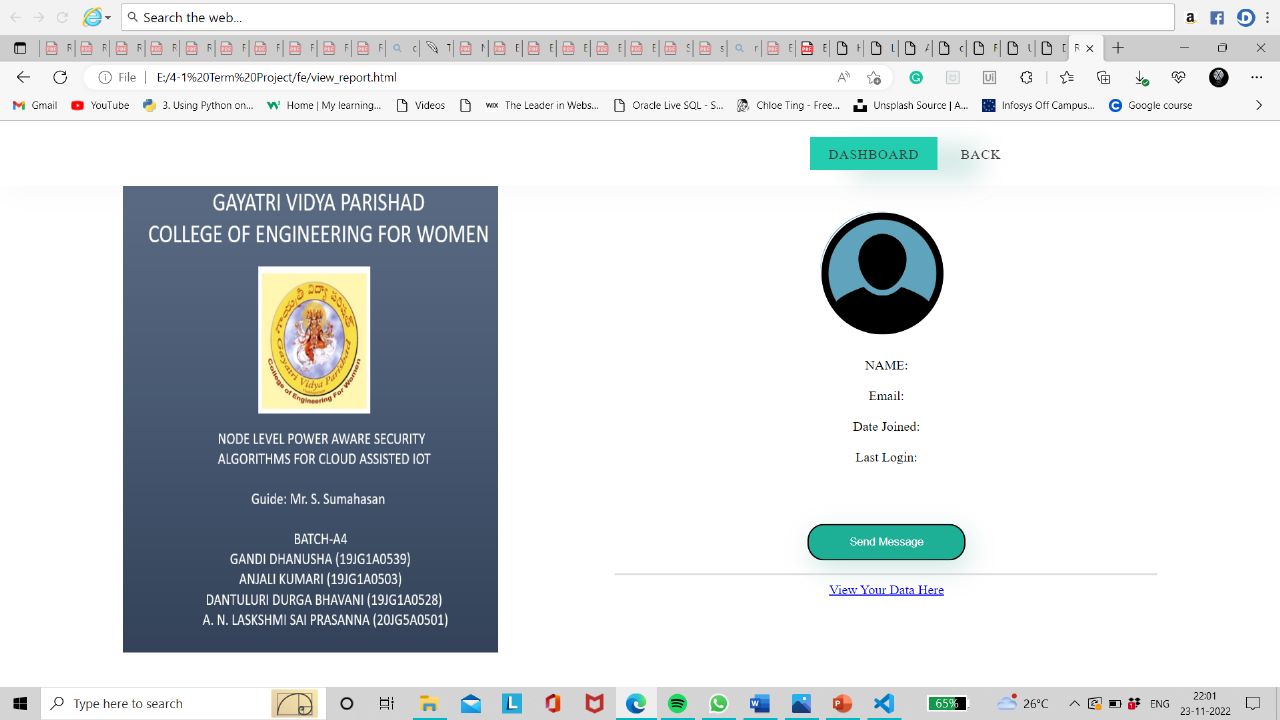


Fig. 9.: Output Screen

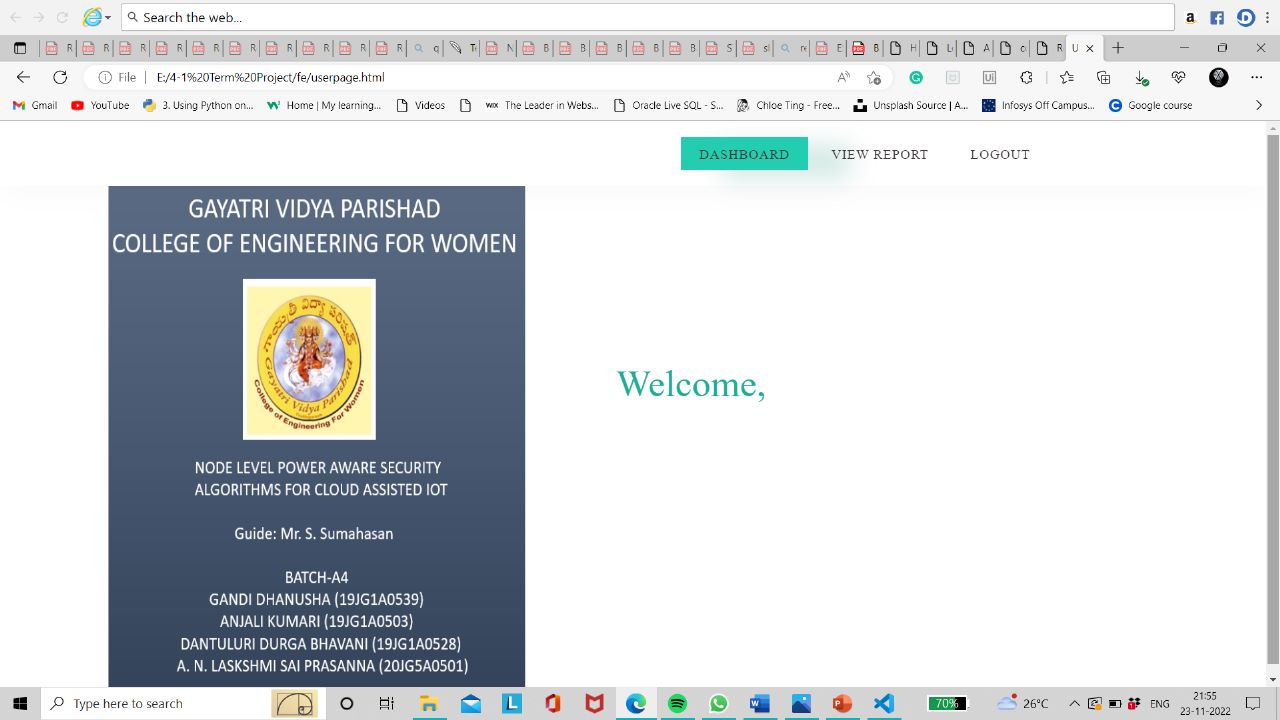


Fig 10: Output Screen

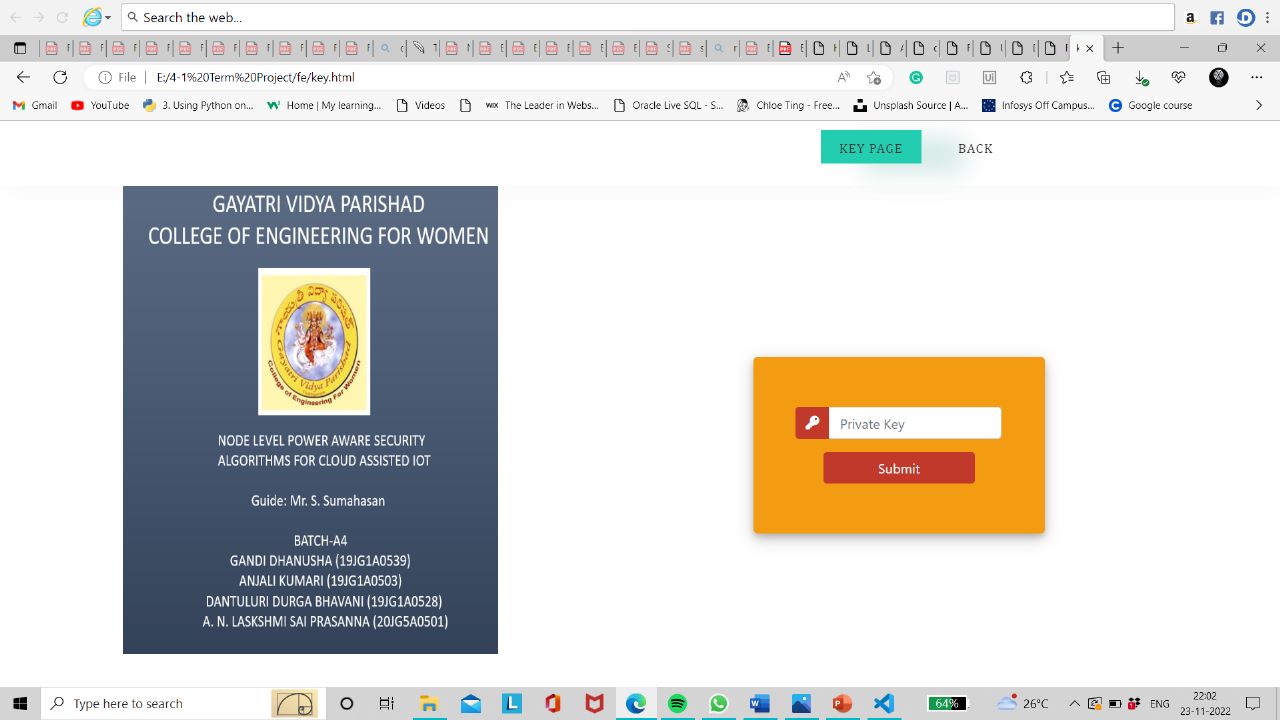


Fig 11: Output Screen

**5.3 CONCLUSION**

In this chapter we have discussed the result part of our project. It discusses some key functions and the introduction to the chapter. It also includes output screens of the parts of code implemented.

# **6. FUTURE WORK**

As already stated, our project aims to provide power aware security to any type of data eliminating the data breaches. In 4-1 semester, we have implemented the node connection, some part of frontend and DH and ECDH algorithms. In the next semester, we aim to the proposed system.

# **7. REFERENCES**

[1] Stankovic, John. (2014). Research Directions for the Internet of Things. Internet of Things Journal, IEEE. 1. 3-9. 10.1109/JIOT.2014.2312291.

[2] Goyal, Tarun Kumar and Vineet Sahula. “Lightweight security algorithm for low power IoT devices.” 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI) (2016): 1725-1729.

[3] Kodali, Ravi & Naikoti, Ashwitha. (2016). ECDH based security model for IoT using ESP8266. 629-633. 10.1109/ICCICCT.2016.7988026.

[4] Alsufaian, Raghad & Almoussa, Roa & Alghamdi, Rahaf & Alqahtani, Khaireya & Alajmi, Rana. (2022). Secure File Storage On Cloud Using Hybrid Cryptography.

[5] Rajesh S, Paul V, Menon VG, Khosravi MR. A Secure and Efficient Lightweight Symmetric Encryption Scheme for Transfer of Text Files between Embedded IoT Devices. Symmetry. 2019; 11(2):293. https://doi.org/10.3390/sym11020293.

[6] Mesquita, Joao & Guimarães, Diana & Pereira, Carlos & Santos, Frederico & Almeida, Luís. (2018). Assessing the ESP8266 WiFi module for the Internet of Things. 10.1109/ETFA.2018.8502562.

[7] V. S. Mahalle and A. K. Shahade, "Enhancing the data security in Cloud by implementing hybrid (Rsa & Aes) encryption algorithm," 2014 International Conference on Power, Automation and Communication (INPAC), 2014, pp. 146-149, doi: 10.1109/INPAC.2014.6981152.

[8] Wu, Zengqiang & Su, Di & Ding, Gang. (2014). ElGamal algorithm for encryption of data transmission. 1464-1467. 10.1109/ICMC.2014.7231798.

[9] Sanaz Amanlou and Khairul Azmi Abu Bakar, “Lightweight Security Mechanism over MQTT Protocol for IoT Devices” International Journal of Advanced Computer Science and Applications (IJACSA), 11(7), 2020.

[10] Azma, Aliasghar & Kianfar, Nima & Chitsazi, Hossein. (2021). Research and Development on Cloud Computing.

[11] Henkel, Jorg & Pagani, Santiago & Amrouch, Hussam & Bauer, Lars & Samie, Farzad. (2017). Ultra-low power and dependability for IoT devices (Invited paper for IoT technologies). 954-959. 10.23919/DATE.2017.7927129.

[12] Koblitz, Neal. “Elliptic Curve Cryptosystems.” *Mathematics of Computation*, vol.48, no. 177, 1987, pp. 203–09. *JSTOR*, https://doi.org/10.2307/2007884. Accessed 23 Nov. 2022.

[13] Wu, Xianping & Dandash, Osama & Le, Phu. (2006). The Design and Implementation of a Smartphone Payment System based on Limited-used Key Generation Scheme. 2006. 458 - 463. 10.1109/ITNG.2006.128.

[14] Farhan, Syed & Zaidi, Syed Farhan & Munam, Ali & Shah, Munam & Kamran, Muhammad & Javaid, Qaisar & Zhang, Sijing. (2016). A Survey on Security for Smartphone Device. International Journal of Advanced Computer Science and Applications. 7. 206-219. 10.14569/IJACSA.2016.070426.

[15] Ms. Moonmoon Karmakar, Ms.Pooja Choudhari , Ms.Disha Mainani, 2014, Cloud Authentication Using Kerberos, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) ICIAC – 2014 (Volume 2 – Issue 09),

[16] E. Shaikh, I. Mohiuddin and A. Manzoor, "Internet of Things (IoT): Security and Privacy Threats," 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), 2019, pp. 1-6, doi: 10.1109/CAIS.2019.8769539.

[17] Reddy, Siva Nagendra & Vardhan, Dupakuntla & Reddy, K. & Pedamalla, Ajay. (2018). An IoT-Based Low-Cost Weather Monitoring and Alert System Using Node MCU. 10.1007/978-981-10-5544-7\_27.

[18] Ullah, S., Zahilah, R. Curve25519 based lightweight end-to-end encryption in resource constrained autonomous 8-bit IoT devices. *Cybersecur* **4**, 11 (2021). https://doi.org/10.1186/s42400-021-00078-6.

[19] A. G. Ismaeel and M. Q. Kamal, "Worldwide auto-mobi: Arduino IoT home automation system for IR devices," 2017 International Conference on Current Research in Computer Science and Information Technology (ICCIT), 2017, pp. 52-57, doi: 10.1109/CRCSIT.2017.7965533.

[20] C. Wang, A. Chai, Z. Wang and D. Ju, "CB-CDP: A cloud based continuous data protection system," 2013 3rd International Conference on Consumer Electronics, Communications and Networks, 2013, pp. 188-191, doi: 10.1109/CECNe