International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7399
***Article Received**: 04 May 2023 **Revised:** 26 June 2023 **Accepted:** 19 July 2023*

An Optimized Node Level Lightweight Security Algorithm for Cloud Assisted-IoT

Mr. S. Sumahasan[*1], Dr. D. Rajyalakshmi[2]
[*1]Research Scholar
JNTUK, Kakinada
GVP College of Engineering for Women , Visakhapatnam-530048
Andhra Pradesh, India
sumahasan@gvpcew.ac.in
[2]Professor, Dept. of CSE
University College of Engineering Vizianagaram
JNTU-GV
Andhra Pradesh, India
rajyalakshmi.cse@jntukucev.ac.in

Abstract— The fastest-evolving technology, the Internet of Things (IoT), will advance the fields of agriculture, defense, and medical electronics. IoT is focused on giving every object a purpose. IoT with cloud assistance offers a potential remedy for the issue of data expansion for individual objects with restricted capabilities. With the increasing use of cloud technology, the Internet of Things (IoT) has encountered additional security hurdles when it comes to exchanging data between two parties. To address this issue, a thorough investigation was conducted into a secure cloud-assisted strategy for managing IoT data, which ensures the safety of data during its collection, storage, and retrieval via the cloud, while also considering the growing number of users. To achieve this, a lightweight security mechanism that is optimized at the node level is implemented in the proposed system. By utilizing our technology, a secure IoT infrastructure can be established to prevent the majority of data confidentiality threats posed by both insiders and outsiders. Using a heartbeat sensor and a node MCU, we create a heartbeat monitoring system. At the node MCU level, giving security to the patient's health data and preventing unauthorized users from attacking it. Smaller key sizes and lightweight security techniques for IoT devices with minimal power, lower power and memory consumption and Execution time, transmission capacity reserve is used to achieve security. In order to achieve this. The performance of the RSA and ECC algorithms in terms of execution time, power consumption, and memory use have been tabulated for this experimental arrangement. The ECC method occurs to produce the best results in tiny devices.

Keywords- Execution Time, Memory consumption, IoT, Cloud, Node, Security, RSA, ECC, Node MCU.

I. INTRODUCTION

Data transmission, which is the exchange of data between two or more connected networked devices, is one of the most fundamental parts of human existence. Data consists of emails, business related information, private data etc., if data reaches to the hackers or Man-in-the middle attacks could be harmed. So, it is essential to safeguard the data against malware and manipulation. Secure Data transformation techniques called encryption is provided by the cryptosystem to ensure data protection from misuses with the help of keys. If the encryption and decryption can be done with the same key called Symmetric cryptography. Both parties in public key cryptography use two different keys known as the public key and private key to prevent this and increase security. One of the most well-known algorithms in public key cryptography, known as RSA (after its creators Rivest, Shamir, and Adleman), is used for certain security services. RSA has grown to be the most popular algorithm because it uses both keys. The factorization of huge integers is where the RSA method struggles. Finding the product of two numbers is simple, but figuring out the initial prime number is difficult. It is quite impossible to find two numbers whose product is given. As there is slow signing, key generation, and decryption, which are slightly tricky to implement RSA securely.

To avoid this an alternative technique and powerful cryptography approach called Elliptical Curve Cryptography (ECC) is introduced. ECC is a public key cryptography algorithm, which encrypts data using a key. ECC provides security for key pairs with the help of mathematics of elliptical curves, for present ECC is a plane curve over finite fields. Due to the smaller and equivalent key size of ECC and the ability to maintain the security ECC is gaining more popularity in recent times. It is also proven that ECC maintains high levels of performance and security. An ECC is more secure than

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7399
***Article Received**: 04 May 2023 **Revised:** 26 June 2023 **Accepted:** 19 July 2023*

RSA because of its same size as RSA is generally ten times slower than ECC.

For the ESP8266, a LUA-based open-source platform firmware known as Node MCU was developed. The TCP/IP protocol is used by the inexpensive Wi-Fi chip known as the Espressif ESP8266. Applications for the Internet of Things (IoT) are expanding nowadays, and connecting items is becoming increasingly crucial. The Wi-Fi protocols can be used in a variety of ways to connect things and enable data transfer. Here is another way of developing Node MCU with a well-known IDE that is Arduino IDE. We can also develop applications on Node MCU using the Esplorer IDE and Arduino IDE.

Data is saved online and managed and operated by a cloud computing provider in a process known as cloud storage. You can save money by avoiding the cost and hassle of purchasing and maintaining your own data storage infrastructure because to its on-demand nature, just-in-time pricing, and capacity. We use the cloud called Thing Speak IoT (Internet of Things) platform to store data to the cloud. Thing Speak is IoT analytics software that allows you to collect, visualize, and analyze live data streams. Thing Speak allows you to send data from your devices, create real-time visualizations of live data, and set alarms. After the data has been uploaded to the Thing Speak IoT platform, the end-user may log in and begin obtaining the data they require from the cloud.

A person's heartbeat is discovered and converted into electrical pulses and impulses by the heart rate sensor [6]. Modern heart rate monitors typically employ one of two techniques to record heart impulses (electrical and optical). Either signal type can provide the same crucial heart rate information. A network of actual physical things or people that are outfitted with electronics, software, networks, sensors, and other devices to gather and share data is known as the Internet of Things (IoT) [7]. Human connectedness is essential to the Internet of Things (IoT), which enables interaction, contribution, and collaboration with our surroundings. IoT may be used to improve security, reduce the need for human labour, better utilize resources, and save time. The foundation of the Internet of Things is connectivity. Connecting various devices to the platform, analysing the data gathered and utilising it to deliver business insight, and combining various models to improve user experience are all significant IoT components. By preventing cyber attacks, security in IoT systems helps to guarantee a secure exchange of data in a private, trustworthy, and accessible way. As a result, the first step in preventing attacks, managing trust, and ensuring security in the IoT world is to categorise the numerous hazards associated with each unique level of the overall IoT system architecture. In 2021, the number of data breaches disclosed reached an all-time high, up 68 percent from the year before. The Identity Theft Resource Centre's 2021 Data Breach Report states that in order to create safe communication, consideration must be given to the network security factors of confidentiality, integrity, authentication, privacy, availability, and non-repudiation.

There are a total of six sections in the suggested paper. The work is briefly introduced in Section I. In Section II, the Literature Review is covered. The project's whole methodology, including every module in detail, is provided in Section III. Section IV contains the project's outcomes or results. The future scope and conclusion of the essay are discussed in Section V, and Section VI, which also includes a list of the sources utilized, concludes the study.

II. LITERATURE SURVEY

This article compares RSA, ECC, DES, and AES [8] on a low-end Smartphone to determine how quickly a typical user in a smart city can use them. Smartphone’s are frequently used in smart cities. On smart phones with constrained settings, this research examines the temporal complexity of these cryptographic techniques.

The goal of this experiment is to determine how much time these typical techniques take on a device with limited runtime memory and processing power. The RSA, ECC, DES, and AES algorithms are run, and comparative analysis and proof of the evaluation are carried out on the Android platform using Android Studio. A Smartphone called the Android Virtual Device is used in a smart city with limited resources. The outcomes demonstrate that the ECC is suitable for entry-level devices. When applied to low-power devices, conventional cryptography techniques are highly computationally expensive.

A Secure and Efficient Lightweight Symmetric Encryption Scheme for Text File Transfer between Embedded IoT Devices. This study introduced a Novel Tiny Symmetric Encryption Algorithm (NTSA), which can be used by all current IoT applications and improves file transmission security [4, 29].

It is also possible to use the Tiny Encryption Algorithm (TEA), even though it employs a constant encryption key throughout. Because it increases the security features of TEA by introducing more key confusions, NTSA is regarded as an advanced algorithm. At each level of encryption, a new key will be generated in NTSA, and the files will be transferred via the IoT network [14]. In comparison to other existing algorithms, NTSA is shown to be substantially more secure and efficient. The Hybrid Cryptography Algorithm-Based Privacy-Preserving Cloud Storage in Medical IOT [12, 34] provided an application that continuously updates and

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7399
***Article Received**: 04 May 2023 **Revised:** 26 June 2023 **Accepted:** 19 July 2023*

monitors heart rate on an IoT platform. Because a single algorithm might lead to security breaches, it cannot ensure high-level protection. The symmetric key techniques AES, 3DES, and Blowfish are used in this suggested system. For key encryption, the RSA method is employed, and for double encryption, the AES and Blowfish algorithms are used. The LSB method is used to implement key information security. The data is subsequently encrypted and transferred to the cloud. Data that has been decrypted can be viewed by downloading the file from the cloud. Hybrid encryption is defined as the combination of two or more encryption techniques in [5, 31] this work. Combining symmetric and asymmetric encryptions can increase security. Security is the most crucial element in cloud computing.

This work introduced a hybrid encryption method that combines the RSA and AES algorithms to improve data security. It focused mostly on secure data uploading to the cloud and secure data downloads to ensure data integrity.

The study "Elliptic Curve Cryptosystems" [3] examines a mechanism for public-key cryptosystems based on elliptic curves over finite fields that makes use of the multiplicative group of a finite field. It considers the problem of primitive points on an elliptic curve modulo p. The order of the cyclic subgroup generated by a global point is not smooth, according to a theorem.

Strong authentication policies employing a modified Kerberos Authentication Protocol are used in cloud computing environments. In [10, 32] this work, a cloud environment is created for better data service authentication utilizing the Kerberos protocol for authentication. When a client requests data, the RSA and ECC algorithms are combined with Kerberos. The Kerberos Algorithm, RSA, and ECC were used to offer a higher and more robust level of security. Elliptic Curve Cryptography on Android Devices for Secure Communication. This work [11][20] established ECCSMS to stop assaults (Elliptic Curve Cryptography Short Message Service).

Digital signatures are therefore used to guarantee information security. The message is encrypted at user1 and sent to user2, who decrypts it using his key. Since the message can only contain string values, each character in the message must first be transformed into bytes, then into points of type x, y, and finally, the points must be encoded by mapping each of them with each point on the elliptic curve.

IoT Security Model Using ESP8266, ECDH and EC Elgamal [1, 30] [19, 35]. The suggested smart gadgets in this study are Internet of Things (IoT)-based and provide remote access. The communication between smart devices is the most crucial element of this. This work examines the creation of ECDH key exchange for safe communication between ESP8266 modules using Node MCU [24, 33, 36]. A low-cost, high-performance embedded Wi-Fi module is the ESP8266. ECC has proven to be more efficient than RSA in a variety of situations. ECC has become the optimal solution for IoT device authentication and authorization thanks to the storage capacity of the ESP8266. ECDH is a secure authentication mechanism that outperforms both RSA and AES in terms of security. You can make a secure and inexpensive Wi-Fi device with the ESP8266 and ECDH.

Low-power IoT device security algorithm that is lightweight. This study [2, 28] is based on Elliptic Curve Diffie-Hellman (EC-DH) Algorithm, a well-liked and efficient public-key cryptosystem, low-power security techniques for IoT devices. In key exchange systems like the Diffie-Hellman Key Agreement Scheme, elliptic curves are frequently used.

Elliptic Curve Cryptography (ECC) offers equivalent security to conventional cryptosystems like RSA (Rivest-Shamir-Adleman), but with smaller key sizes, requiring less power [22], faster computations, and less memory and transmission capacity (bandwidth) reserve [21]. This work aims to develop a lightweight, low-power key exchange algorithm for encryption and decryption.

In order to efficiently calculate the modulus of fractional numbers, ECDH was used, and ECC was used to give the same security with a shorter key length. RSA was used as a baseline for comparison. We compared various algorithms such as Diffie-Hellman, RSA, and ECDH in terms of power, area, and timing, among other things. The findings lead to the conclusion that ECDH outperforms other algorithms in terms of power and area.

A tunnelling service for WebRTC and IoT devices that is accessible on demand for hospitals. This work provides cancer patients receiving home care with IT-based assistance. According to this concept, the patient's home furnishings are dynamically positioned around a linked "hub" device, such as infusion pumps and medical sensors. Hospital employees and patients can connect with one another by swiftly deploying WebRTC data plane traffic with little configuration over limited networks with strong firewall constraints.

This is based on latest mobile health application based on IoT that are used for diabetes management. This diabetes patient monitoring uses a sensor support system contains registration of new members and people with diabetes. Different sensors are connected like temperature sensor to measure the body temperature of the patient etc. to a hub. All the readings have to be monitored using the Arduino and E-health sensor shield. These readings compared with database values. So that it will predict the normal or above normal condition of the patient.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7399
***Article Received**: 04 May 2023 **Revised:** 26 June 2023 **Accepted:** 19 July 2023*

The article "Authenticated Encryption towards Next-Generation Algorithms" [13] describes how to construct IoT security. IoT security helps with the secure transport of data in a trustworthy, accessible, and private way by preventing cryptographic attacks. In order to stop assaults, maintain trust, and ensure security in the IoT world, it is crucial to characterize the many hazards connected to each distinct level of the overall IoT system model. Authenticated Encryption (AE) algorithms will have confidentiality and integrity by combining two separate primitives -a conventional encryption algorithm to ensure confidentiality and a Message Authentication Code (MAC) for integrity. This paper provides standard AE algorithms, security models for AE.

In this work ―Financial Cryptography and data security‖ [15], introduces an advanced app-store concept called thing store. Thing store services three categories of users- Thing providers, Software developers and the End users. Elliptic Curve Cryptography (ECC) is asymmetric, based on public key technology, and uses two keys—public and private. Compared to non-ECC algorithms, it offers comparable security with a reduced key size. Elliptic curves are used in it, RSA- 1024 key length and ECC- 160 key length

The restricted utilized key generation strategy based on the KCL protocol is suggested as a novel security enhancement for smart phones in "Identity, location, sickness and more: inferring your secrets from android public resources" [17]. The right password must be entered each time to access the smart client utility for this user to begin a new transaction. The performance of the RSA and ECC algorithms is satisfactory. Transactions with RSA complete faster than those with ECC.

In ―A Survey on Security for Smart Phone Device‖ [18], developed ECCSMS (Elliptic Curve Cryptography Short Message Service), to prevent attacks. Since the message can only contain string values, each character in the message must first be converted into bytes, then into points of the form of x, y, before the points must be encoded by mapping each of them with a point on the elliptic curve. Finally, the encoded points must be converted back into bytes, then into strings, in order to provide the security of information using digital signatures [16]. Encryption takes place at the user1, and the message is sent to the user2, who uses his key to decrypt it and read it. This paper discussed that for the public data there no security, there may be a leak in data of Smartphone. The mitigation strategy described in this paper describes how to keep the legitimate parties' use of public data while limiting how an adversary can use it to obtain user secrets. In this initial step, they gather all the information from Wi-Fi connections made at various locations. And in this data, they run the query mechanism. They were able to successfully locate each of these places using Navizon. However, they discovered that not all hotspots could be utilized for this reason, as the Navizon database is still far from full. This discusses the categories of attacks (i.e., old and new attacks), and solutions to provide the security for the Smartphone. There are many ways to provide security to Smartphone like pattern, face lock or password but these can be attacked by brute force method or guessing.

They initially discussed the present issues with data protection, privacy, and authentication in this study [9, 37]. Investigated the weaknesses of cell phones and potential assaults on them. Second, they focused on the causes of assaults and how they affected smart phones in order to describe detected attacks in opposition to those devices.

III. METHODOLOGY

To achieve effective security for low power IoT devices, a node-level implementation of the public key cryptosystem, RSA and Elliptic Curve Cryptography, in which ECC was the efficient algorithm based on research, is being implemented. The work to implement the node level lightweight security algorithm has been divided into four modules:

1. Creating a system for tracking heartbeats.
2. Providing node-level security
3. Cloud storage of encrypted data.
4. Web page access to the decrypted data.

1) Creating a system for tracking heartbeats.

The heart rate sensor is used to gather the patient's heartbeat data, and the Node MCU is used to store the data obtained from the patient. The heart rate sensor has three pins: analogue, digital, and ground. The Node MCU's A0 port is where the analogue pin is connected. The digital pin is connected to the eve port, while the ground pin is connected to the Node MCU's GND port. When the Heart Rate sensor is coupled to the Node MCU, the two devices work together as a single device known as "Node." This sensor is used to detect the patient's heart rate, and the data is gathered by the Node MCU, which then encrypts it and sends it to the cloud shown in fig 1.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7399
***Article Received**: 04 May 2023 **Revised:** 26 June 2023 **Accepted:** 19 July 2023*

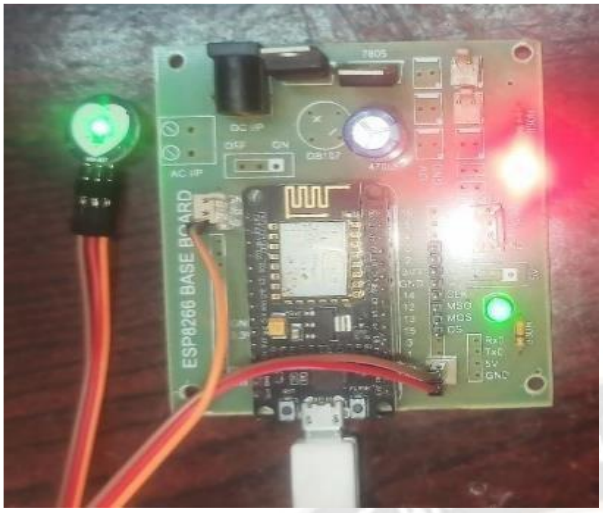

Fig. 1. Node MCU is connected to a heartbeat sensor

2) Providing node level security

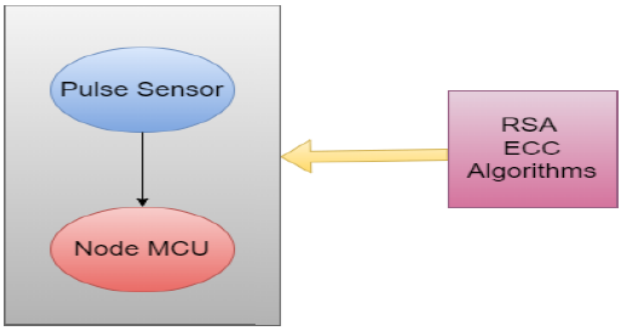

Fig.2. Encryption applied at node level

The data should be encrypted in the node itself after the heart rate sensor is linked to the Node MCU and the patient's heart rate is detected. Elliptic curve cryptography (ECC) and the Rivest-Shamir-Adelman (RSA) algorithms are used for this. Two parties will be able to generate a shared secret across an unsafe channel by employing a public-private key pair using RSA and ECC. This common understanding can be used to generate new keys or serve as a key by itself. Elliptic Curve Cryptography cannot be understood without a thorough comprehension of the Elliptic Curve's underlying principles. A planar algebraic curve with the following equation is an elliptic curve: $y^2=x^3 - ax + b$. The graph of the curve is non-singular, indicating that it is devoid of cusps and self-intersections (when the characteristic of the Co-efficient field is equal to 2 or 3). An elliptic curve typically resembles the image below. When a straight line crosses an elliptic curve, it can do so in nearly three places.

It can be shown that the elliptic curve is symmetric around the x-axis. The success of the algorithm depends on this property.

RSA Algorithm

For Key Generation

Pick p and q, two separate large prime numbers.

Calculate n = p*q. Calculate φ (n) = (p-1) (q-1).

Select integer e such that gcd (φ (n), e) =1;1<e< φ (n).

Calculate d where d ≡ (e^ (-1)) *mod φ (n).

Public Key is denoted by KU.

Private key is denoted by KR.

KU = {e, n}.

KR = {d, n}.

Encryption

Plaintext M<n. Cipher text C = (M^(e)) (mod n)

Decryption

Cipher text C

Plaintext M = (C^ d) *(mod n).

ECC Algorithm

ECC is a form of public key encryption that uses elliptic curve theory to produce cryptographic keys more rapidly, efficiently, and in smaller sizes. ECC generates keys utilizing the properties of an elliptic curve equation rather than the traditional approach of generation as the product of large prime numbers. The points on the graph can be expressed using the following equation from a cryptographic perspective:

$y^2=x^3 - ax + b$

ECC Key Exchange

Global Public Elements

Eq (a, b) elliptic curve with parameters a, b and q.

q: prime number or an integer of form 2m.

G: point on the elliptic curve whose order is very large value of n.

G<q

User A Key Generation

Select private key XA XA<q

Calculate public key YA, YA= (XA*G) mod q

User B Key Generation

Select private key XB, XB<q

Calculate public key YB, YB= (XB*G) mod q

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7399
Article Received: 04 May 2023 Revised: 26 June 2023 Accepted: 19 July 2023

Calculate secret key

User A secret key

K=XA*YB

User B secret key

K=XB*YA

Encryption

M is the message.

Create an elliptic curve point from this message M first.

Let this point be Pm.

Now this point pm is encrypted.

Select a positive random integer k for encryption. Cipher point Cm = {k*G, Pm + k*PB}

Decryption

Multiply pair's first point with the receiver's private key kG*XB

The subtract it from second point that is pm + (kPB - kG*XB)

So = pm + k, XB*G – k*XB*G

= pm (original point)

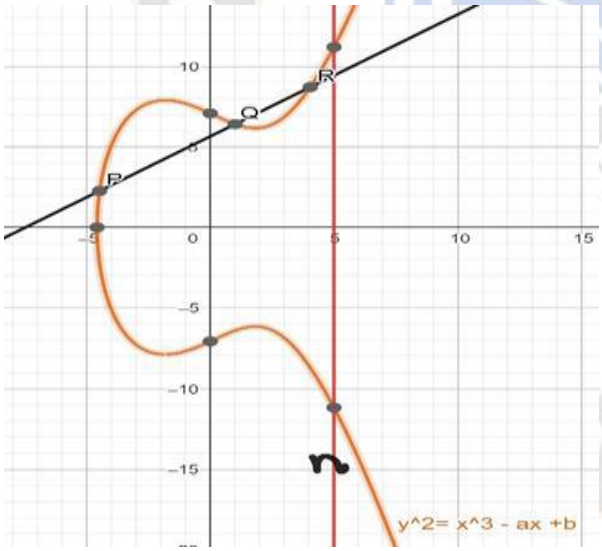

Fig. 3. Elliptic Curve Equation

3) Cloud storage of encrypted data

The encrypted data must be stored in the cloud after the Heart Rate has been determined and encrypted using the RSA and ECC procedures. Data is saved online and managed and operated by a cloud computing provider in a process known as cloud storage. You can save money by using it on demand, with just-in-time capacity and pricing, and by forgoing the need to buy and maintain your own data storage infrastructure.

We use the cloud called Thing Speak IoT (Internet of Things) platform to store data to the cloud. Thing Speak is IoT analytics software that allows you to collect, visualize, and analyze live data streams. Thing Speak allows you to send data from your devices, create real-time visualizations of live data, and set alarms. After the data has been uploaded to the Thing Speak IoT platform, the end-user may log in and begin obtaining the data they require from the cloud shown in fig 4..

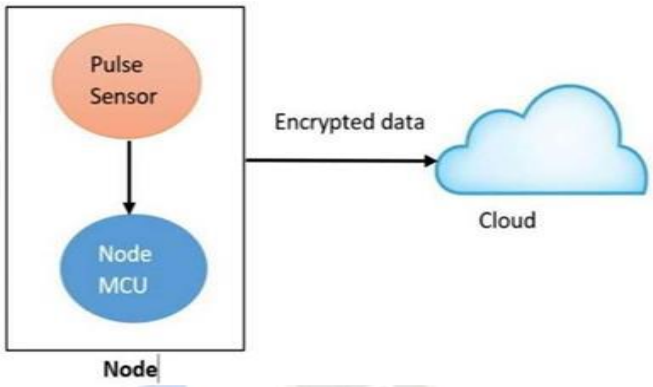

Fig.4. Data upload to cloud platform

4) Web page access to the decrypted data

A registration page will be available in this module, where the end-user (doctor or patient's relatives) will authenticate and register. Only the registered end-user has access to the patient's information. In the interface

via which the end-user gets the data, the decryption is done using the RSA and ECC methods. The end-user submits a request to the interface, which is received and processed, after which the specific data is decrypted and made available to the end-user via the interface.

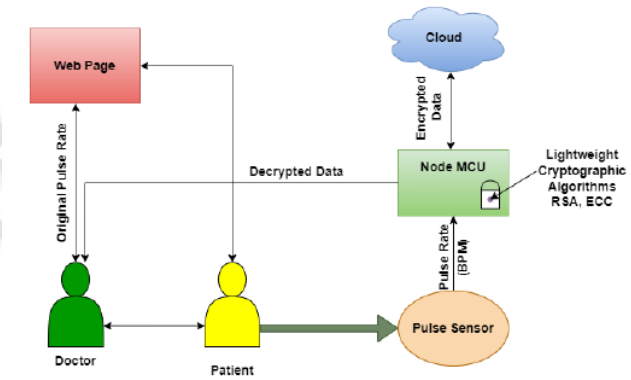

Fig.5. System Architecture

The proposed resource-constrained IoT endpoints as well as computationally intensive devices can both use the proposed lightweight node level security techniques. So, it offers better and more comprehensive options for producing the result. For effective viewing of the decrypted data, the output of the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7399
***Article Received**: 04 May 2023 **Revised:** 26 June 2023 **Accepted:** 19 July 2023*

model can be shown either on the serial monitor or can be ported to the custom webpage shown in fig 5.

IV. RESULTS

The output for creating a system for tracking heartbeats. Which deals with designing a heartbeat monitoring system, is listed below. The connecting cables on the board are used to establish connections throughout the system. The pulse sensor connected to the Node MCU is known as Node. The ESP8266 board contains an analog-to-digital converter, which translates analogue data and displays it as digital data. The Node MCU receives a power supply, enabling the node to accept input shown in fig 6.

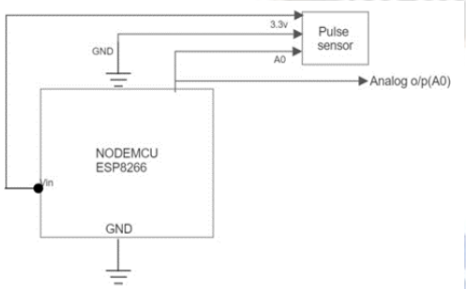

Fig.6. Creating a system for tracking heartbeats.

Below is the output for cloud storage of encrypted data, which entails uploading data to the cloud. Before being saved in the cloud, the patient's data is extracted from the node and encrypted there using the RSA and ECC protocols shown in fig 7.

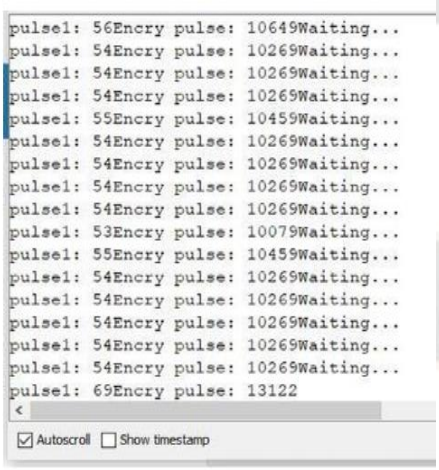

Fig.7. Cloud storage of encrypted data

Below is the output for web page access to the decrypted data, which deals with obtaining cloud data. The decryption procedure is handled by this module. The patient's file that is kept in the Thing Speak cloud can be decrypted by the user shown in fig 8.

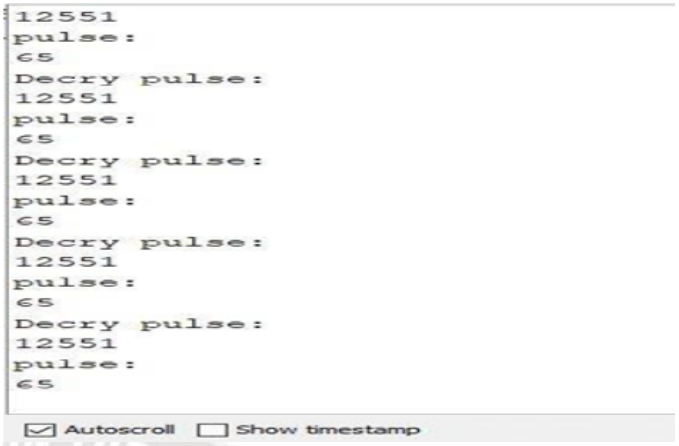

Fig.8. Web page access to the decrypted data

Energy Issues' Impact on RSA and ECC Execution File Comparison:

Execution time:

The execution time depends on the key values. The overall programme execution time includes both the encryption and data transfer times shown in fig 9.

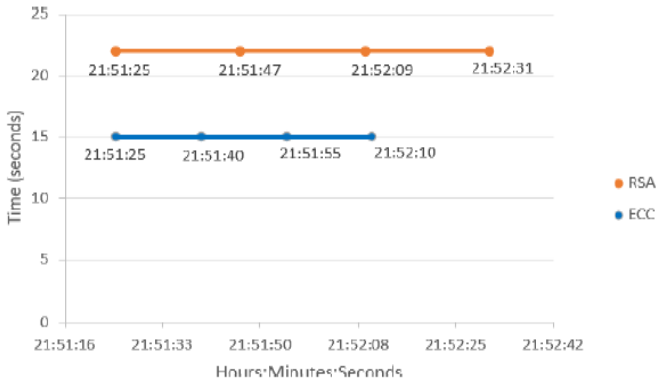

Fig.9.Execution Time (in seconds)

Memory Consumption:

How much memory a particular programme needs when it is running. The memory used reports how many bytes are needed to hold a key and its value in RAM. The amount of memory used is influenced by the size of the data and the difficulty of the corresponding algorithms shown in fig 10.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7399
***Article Received**: 04 May 2023 **Revised:** 26 June 2023 **Accepted:** 19 July 2023*

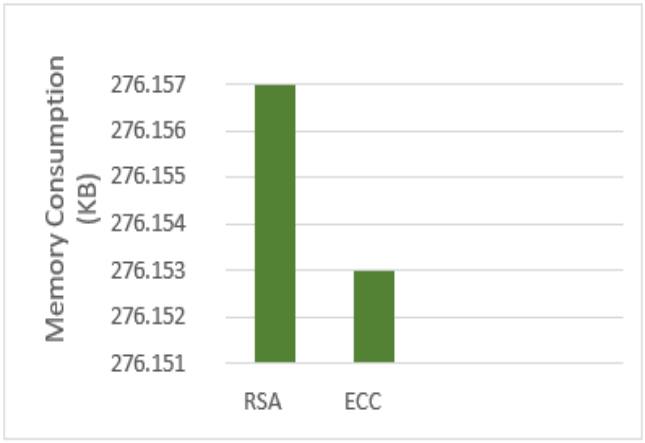

Fig.10.Memory Consumption (in KB)

Power Consumption:

The memory storage and retrieval of different cryptographic methods affect power consumption [25]. The suggested model's outcomes result in lower memory and power usage. In this work, we employed the Node MCU, which only requires 3.3v, which is lower than the Raspberry Pi's operating voltage [26,27]. Data transmission and acquisition are formed by nodes.

Data security is required during transmission, and encryption can be employed for that. This method of data protection protects data but increases system energy consumption due to rising programme complexity. The amount of data transferred and the algorithms that were employed both affect power consumption shown in fig 11.

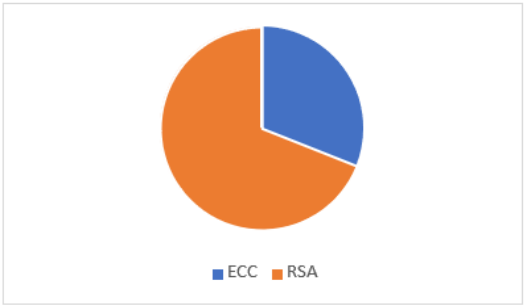

Fig.11.Power Consumption (in µJ)

V. FUTURE SCOPE AND CONCLUSION

In this paper, we developed an optimized node-level lightweight security mechanism. Here the method for transferring data safely without any data breaches is suggested. A piece of original text is encrypted using various simple encryption techniques like ECC and RSA to protect the data. Using one of these methods, each provide a public and private key. The public key is used by the parties with whom the messages are exchanged. The recipient's private key is used to decrypt the data once it has been encrypted and sent using the sender's public key. ECC is a technique for public-key encryption. ECC encryption allows for equivalent security to be attained with smaller keys when compared to non-EC encryption (based on simple Galois fields). The RSA key agreement process can be used to create a shared secret between two parties with different public-private key pairs across an unsafe channel.

ECC is discovered to be the optimum algorithm for this operation after comparing it to RSA for data encryption. ECC is shown to be more effective than RSA in terms of execution time, power usage, and memory usage. Data security is provided by our strong encryption techniques, which also gives protection against data breaches from all kinds of intrusion attempts. Our proposed system is helpful in healthcare, defense sectors etc., it handles patient's sensitive data in time of heart attacks.

The Internet of Things (IoT) has grown in importance worldwide. It gained popularity after a while. AI and ML have made internet of things device automation easy. Because of this, the Internet of Things (IoT) now applies to many commercial areas. We'll cover the internet of things' healthcare, defence, and agriculture applications. More Data Monitoring IoT security's biggest risk is sensitive data access and transmission. Stores all data until an approved user retrieves it. Future developments to this work include the use of improved microcontrollers with higher operating frequencies and lower power consumption, additionally, the Node-MCU and Arduino IDE are used to provide hybrid, lightweight security solutions at the node level.

Acknowledgments The authors acknowledge the help from the university teachers.

Author Contributions All authors listed have made a substantial, direct and intellectual contribution to the work, and approved it for publication.

Funding This research received no external funding.

Compliance with Ethical Standards

Conflict of Interest All authors declare that they have no conflict of interest.

Ethical approval This article does not contain any studies with human participants or animals performed by any of the authors.

REFERENCES

[1] R. K. Kodali and A. Naikoti, ―ECDH based security model for IoT using ESP8266, ―2016 International Conference on Control Instrumentation, Communication and

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7399
***Article Received**: 04 May 2023 **Revised:** 26 June 2023 **Accepted:** 19 July 2023*

Computational Technologies (ICCICCT), 2016, bpp, 629-633,10.1109/ ICCICCT.2016.7988026.

[2] Goyal, Tarun & Sahula, Vineet. (2016). Lightweight security algorithm for low power IoTdevices.17251729.10.1109/ICACCI.2016.773 2296.

[3] Koblitz, Neal. ―Elliptic curve cryptosystems.‖ Mathematics of Computation 48 (1987): 203-209.

[4] Rao, M. N. . (2023). A Comparative Analysis of Deep Learning Frameworks and Libraries. International Journal of Intelligent Systems and Applications in Engineering, 11(2s), 337–342. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2707

[5] Rajesh, Sreeja & Paul, Varghese & Menon,Varun & Khosravi, Mohammad. (2019). A Secure and Efficient Lightweight Symmetric Encryption Scheme for Transfer of Text Files between Embedded IoT Devices. Symmetry. 11. 293. 10.3390/sym11020293.

[6] 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.

[7] J. Arora, Gagandeep, A. Singh, N. P. Singh, S. S.S. Rawat and G. Singh, "Heartbeat rate monitoring system by pulse technique using HB sensor," International Conference on Information Communication and Embedded Systems (ICICES2014), 2014, pp.1-5, doi: 10.1109/ICICES.2014.7033986.

[8] Skarmeta A., Moreno M.V. (2014) Internet of Things. In: Jonker W., Petković M. (eds) Secure Data Management. SDM 2013. Lecture Notes in ComputerScience, Vol 8425. Springer, Cham. https://doi.org/10.1007/978-3-319-06811-4_10

[9] M. Frustaci, P. Pace, G. Aloi and G. Fortino, "Evaluating Critical Security Issues of the IoT World: Present and Future Challenges," in IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2483-2495, Aug. 2018, doi: 10.1109/JIOT.2017.2767291.

[10] Y. Li, W. Dai, Z. Ming and M. Qiu, "Privacy Protection for Preventing Data Over-Collection in Smart City," in IEEE Transactions on Computers, vol. 65, no. 5, pp.1339-1350, 1 May 2016, doi: 10.1109/TC.2015.2470247.

[11] Shubhangi Verma et at., ―Strong Authentication policy for cloud computing environment using Modified Kerberos authentication protocol‖,IJTA 9 (2): 227-231(2017).

[12] Evaluation of Cryptographic Algorithms on Low Power Devices used in Smart City Muneer Ahmad Dar Scientist-C, National Institute of Electronics and Information Technology (NIELIT) Srinagar, (J&K), India. (Corresponding author: Muneer Ahmad Dar) (Received 29 September 2020, Revised 13 November 2020, Accepted 03 December 2020) (Published by Research Trend, Website: www.researchtrend.net).

[13] Mr. S. Sumahasan and Dr. D. Rajyalakshmi, "Privacy preserving Cloud storage in Medical IoT using Hybrid cryptography Algorithm," Solid State Technology, Vol. 64 No. 2 (2021).

[14] D. Maimut and R. Reyhanitabar, "Authenticated Encryption:TowardNext-Generation Algorithms," in IEEE Security & Privacy, vol. 12, no. 2, pp. 70-72, Mar.-Apr. 2014, doi: 10.1109/MSP.2014.19.

[15] Kutalmis Akpinar and Kien A. Hua and Kai, LiAkpinar2015ThingStoreAP,‖ThingStore: a platform forinternet-of-things application development and deployment‖.Journal- Proceedings of the 9th ACM International Conference on Distributed Event-Based Systems in Year 2015.

[16] Financial Cryptography and Data Security, 2014, Volume 8437 ISBN: 978-3-662-45471-8 Jopp W.Bos, J. Ale Halderman, NadiaHeninger, Jonathan Moore, MichaelNaehrig, EricWustrow.

[17] Xian ping Wu, O. Dan dash and Phu Dung Le, "The Design and Implementation of a Smartphone Payment System based on Limited- used Key Generation Scheme," Third International Conference on Information Technology: New Generations (ITNG'06), 2006, pp. 458-463, doi: 10.1109/ITNG.2006.128.

[18] Xiaoyong Zhou et al., "Identity, location, disease and more: inferring your secrets from android public resources",CCS '13: Proceedings of the 2013.ACM SIGSAC conference on Computer & communications security.

[19] 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.

[20] Mr. S. Sumahasan et al, ―A Node-Level Security Algorithm for Cloud Assisted-IoT‖, NeuroQuantology, Volume 20 Issue 11.September 2022.

[21] S.L. Keoha, S. S. Kumar and H. Tschofenig, ‖ Securing the Internet of Things:‖, in IEEE Internet of Things Journal,Vol.1,no.3,pp.265-275,June2014,doi:10.1109/JOIT.2014.2323395.

[22] Rounak Sinha, Hemant Kumar srivatsava, Sumita Gupta,‖Performance based comparison Study of RSA and Elliptic Curve of Cryptography‖, IJSER, Vol: 4, Issues 5 May 2013.

[23] Hindawi, Journal of Sensors ―Influence of Encryption Algorithms on Power Consumption in Energy Harvesting Systems‖ Volume 2019, Article ID 8520562.

[24] Generation Methods of Elliptic Curves by Harald Baier and Johannes Buchmann August 27, 2002.

[25] Manan Mehta, ―ESP8266: A Breakthrough in wireless sensor networks and internet of things‖, IJECET, Vol: 6, Issue:8, August 2015.

[26] Makarenko, S. Semushin, S. Suhai, S. M. Ahsan Kazmi, A. Oracevic and R. Hussain, "A Comparative Analysis of Cryptographic. Algorithms in the Internet of Things," 2020 International Scientific and Technical Conference ModernComputer Network Technologies (MoNeTeC), Moscow, Russia, 2020, pp. 1-8, doi:10.1109/MoNeTeC49726.2020.9258156.

[27] Kanakaris, Venetis & Papakostas, George & Bandekas, D.V.. (2019). Power consumption analysis on an IoT

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7399
***Article Received**: 04 May 2023 **Revised:** 26 June 2023 **Accepted:** 19 July 2023*

network based on wemos: a case study. TELKOMNIKA (Telecommunication Computing Electronics and Control). 17. 2505.10.12928/telkomnika.v17i5.11317.

[28] Ooko, Samson. (2019). A Comparison of Arduino, Raspberry Pi and ESP8266 Boards.

[29] V.A. Thakor, M.A. Razzaque, M.R.A. KhandakerLightweightcryptographyalgorithms for resource-constrained IoT devices: A review, comparison and research opportunities IEEE Access, 9 (2021), pp. 28177-28193.

[30] Al_Barazanchi I, Murthy A, Al Rababah AA, Khader G, Abdulshaheed HR, Rauf HT, Daghighi E, Niu Y (2022) Blockchain technology-based solutions for IOT security. Iraqi J Comput Sci Math 3(1):53–63

[31] Lata N, Kumar R (2022) Security in internet of things (IoT): challenges and models. Math Stat Eng Appl 71(2):75–81

[32] Alfandi O, Khanji S, Ahmad L, Khattak A (2021) A survey on boosting IoT security and privacy through block chain. Clust Comput 24:1–19

[33] S. Singh, A.S.M.S. Hosen, B. Yoon Blockchain security attacks, challenges, and solutions for the future distributed IoT network IEEE Access, 9 (2021), pp. 13938-13959

[34] IoT devices are more vulnerable thaneverHomepage. https://www.itpro.com/network-internet/internet-of-things-iot/360850/iot-devices-are-more-vulnerable-than-ever. Last accessed 23 Mar 2022

[35] M. Hasan, ―IoT in healthcare: 20 examples That'll make you feel better,‖ April 2, 2020. [Online]. Available: https://www.ubuntupit.com/iot-in-healthcare-20-examples-thatll-make-you-feel-better.

[36] H. HaddadPajouh, A. Dehghantanha, R. Parizi, M. Aledhari, H. KarimipourAsurvey on internet of things security: requirements, challenges and solutions Elsevier: Internet of Things, 14 (2021).

[37] Naidu, Purushotam, P. Krishna Subba Rao, and MHM Krishna Prasad. "Smart-farming: IoT Based Crop Prediction System using Machine Learning Techniques." Solid State Technology 64, no. 1 (2021): 4085-4096

[38]]Kaspersky(2022)AttacksonIoTdevicesdoubleinayearHome page. https://iottechnews.com/news/2021/sep/07/kaspersky-attacks-on-iot-devices-double-inayear/.Lastaccessed 21 Mar 2022.