IJIRCCE

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

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 5, May 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005109|

Secure Searching of Medical IoT Data over Cloud Platform

Jaheda Parveen, Shendage Monika, Taware Priti, Shinde Dhanashree, Prof. S.K. Shinde

B.E Student, Department of Computer Engineering, K J College of Engineering & Management Research, Pune, Maharashtra, India

B.E Student, Department of Computer Engineering, K J College of Engineering & Management Research, Pune, Maharashtra, India

B.E Student, Department of Computer Engineering, K J College of Engineering & Management Research, Pune, Maharashtra, India

B.E Student, Department of Computer Engineering, K J College of Engineering & Management Research, Pune, Maharashtra, India

Department of Computer Engineering, K J College of Engineering & Management Research, Pune, Maharashtra, India

ABSTRACT: The use of modern IT solutions has accelerated the growth of the healthcare business. Conventional equipment is being phased out in favour of sophisticated technology in order to change healthcare institutions. Medical records, IoT devices, sensor systems, novel machinery, and smart gadgets are all being used to modernize healthcare providers. All of major changes in the healthcare industry create a massive amount of data. With the advent of IoT devices and the cloud platform, it has become imperative to achieve the securing of the data generated by the IoT sensors that is being stored on the cloud infrastructure. For this purpose, an effective approach has been devised for securing the IoT data being stored on the cloud platform through the use of Reverse Circle Cipher. This approach also provides an effective framework for searching the encrypted data on the public cloud through the use of Bucket creation and trapdoor generation. The approach has been evaluated extensively using certain performance metrics that have resulted in highly positive outcomes.

KEYWORDS: Internet of Things, Reverse Circle Cipher, Trap Door generation, Search over Encrypted Data

I.INTRODUCTION

The patient's medical history has turned into an important tool for clinicians. It is presently established of the healthcare environment in various countries and is subject to stringent governmental controls. It captivates people's interest further considering it involves extensive treatment procedures, neurological disorders, in-depth tests, and, in certain cases, surgical procedures. It is essential in hospitals because it is intended to provide experts who do not identify the patients with a representation of his personal state and also the ailments to that he's been predisposed. This saves time and avoids inappropriate treatments from being administered. The patient's medical history is a functional instrument for doctors that allows them to collect intelligence regarding their patients' conditions and then apply it to their counselling Every doctor does have his own approach, and because he would not have such a clear memory, he had to handwrite notes his visits. Nevertheless, if the client changes physicians, he would have to start over, and the practitioner would be impossible to resist collecting intelligence in order to assess the illness that the patient is suffering, especially if the patient has many diseases getting addressed by different specialists. In other words, the physician's observations were not regularly noted after every appointment, and that even if they had already been, they could not be revealed. Nevertheless, the fast growth of medical research has grown apprehensions about patients' and healthcare organizations' honesty, transparency, and accountability.

Accountability in consultation is now required, and this problem is now reflected in the keeping of a health record. A doctor's relationship with his patient has never been more frayed than what it is now. The doctor was concerned mainly with the illness and was disinterested in the patient's medical history. Then again, whenever a household is only ever visited by same physicians, interconnections build, allowing the doctor to identify the essence of his afflicted person and so remembering his multiple therapies, allowing him to avoid doing the same activities repetitively.

The information contained in the health record has become increasingly important, and all experts who care for a client have seamlessly integrated this into the health care system. As a consequence, data collection and transmission laws have to be established. The arrangement and substance of health data must be distinguished from the medium through which it has been supplied. Healthcare data is acquired from a variety of sources, comprising medical reports,

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005109|

consultations, and further critical assessment, such as a positron emission tomography report and pictures. The print is by far the most prevalent way to provide info. However, it has become less and less common, and it is progressively being superseded by cloud computing. Even though it is obvious that the physical documentation promotes participation health information and services responsibility for it, technological improvements and the fast spread of the Internet have made it possible to be autonomous of the physical repository without jeopardizing the content or records management. The trend toward digitization is developing, and the file format differs depending on the particular medical contact, such as admission, treatment, which result in generation of data that needs to be safeguarded. The medical data is critical and can be a source of a lot of leakage in this modern world. The proposed approachfor the purpose of achieving theeffective securing of the data is presented in this approach to provide a reliable and secure platform with accountability.

This research paper's Literature Review section portion looks at past work. Section 3 digs more into the methodology, whereas Section 4 emphasizes on the examination of the result. Section 5 concludes this study and offers some suggestions for further research.

II.LITERATURE REVIEW

H. Li et al. [1] suggested a multi-keyword prioritized search system for searching encrypted mobile cloud data that is accurate, efficient, and safe. Security research has shown that the suggested approach may successfully ensure document and index anonymity, trapdoor secrecy, trapdoor unlikability, and hiding the search user's access pattern. Extensive performance studies have revealed that the suggested system is more efficient than existing ones in terms of functionality and computing overhead. The authors conduct detailed security research to show that the EMRS can achieve a high degree of security, including document and index confidentiality, trapdoor privacy, trapdoor unlikability, and hiding the search user's access pattern.

C. Chen et al. looked at ciphertext search in the context of cloud storage. The authors investigate the difficulty of sustaining semantic relationships between various plain texts and related encrypted documents, as well as a design strategy for improving semantic search performance [2]. The MRSE-HCI architecture is also proposed to adapt to the needs of data explosion, online information retrieval, and semantic search. Simultaneously, a verifiable technique is presented to ensure the accuracy and thoroughness of search results. They also look at the search efficiency and security in the context of two prevalent threat models. The search efficiency, accuracy, and rank security are all evaluated using an experimental platform.

order-preserving symmetric encryption (MOPSE+) technique to meet the hierarchical authenticated query to make their model more feasible. Furthermore, they use rigorous security evidence to demonstrate the safety of the proposed systems.

J. Yao et al. offer a novel SSE approach for finding encrypted cloud data that hides the client's search pattern [4]. The authors use the chameleon hashing approach to generate safe search tokens in a randomized manner, such that search tokens for the same phrase vary across searches. For successful encrypted search on the cloud, they use the I O approach to safely translate the randomly generated search token to the deterministic one. They use rigorous security proofs to validate their scheme's security promises. They also undertake thorough experiments for evaluation to demonstrate the performance. The introduced scheme's performance is dependent on the underlying cryptographic technology I O.

In the multi-data-user and multi-data-owner situations, H. Wang et al. present a novel symmetric searchable encryption (SSE) technique [5]. Unlike Sun set alumite-client’s SSE technique presented at ESORICS 2016, the proposed approach not only enables multi-data-owner functionality, but also adds additional security features such as identity hiding, authentication, and confidentiality. The developed approach achieves about the same degree of efficiency as Sun et a scheme, 's according to the final findings.

O. Blaze et al. present an attribute-based security architecture that fulfills the limits of real IoT devices and deployment situations while enhancing security and privacy for topic-based pub/subsystems. The framework incorporates multiple current attribute-based cryptographic solutions in a consistent manner, as well as the ABKS-UR scheme, which authors improved to make it suited for distributed contexts while maintaining the required loose coupling between publishers and subscribers [6]. Therefore, all schemes employ the same set of properties, which is

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005109|

suitable and homogenous from both cryptography and a real-world deployment standpoint. Even when confronted with a realistic honest-but-curious broker model, the proposed architecture assures subscription secrecy, publication confidentiality, and payload confidentiality. It also provides for flawless publishing authentication and revocation of harmful subscribers.

J. Gao et al. provide a novel HPCPABKS-based system for finding and filtering encrypted cloud email. The ABKS architecture is applied creatively to the encrypted cloud email situation. The sender adds the recipient filtering server to an extra list of recipients for searching and filtering [7]. The encrypted keyword index's access control policy is based on the user's characteristics in this recipient list. Therefore, receivers can search for keywords depending on their qualities, and the recipient filtering server, in turn, can filter keywords depending on their properties. The solution providescomplete security through the use of dual system encryption and can withstand offline KGA. Users may find it just as easy to search and filter as they do with regular email.

l. xue et al. proposed a condition-hiding proxy re-encryption technique that allows keyword search and may be used to secure data exchange and delegation in e-healthcare systems. a doctor, alice can create a conditional authorization for another doctor bob, using a newly proposed technique by supplying a re-encryption key [8]. the cloud server can use the re-encryption key to perform ciphertext transformation, allowing bob to access the phrs that was originally encrypted using alice's public key, allowing for safe delegation. without knowing anything about the term or the underlying ailment, the cloud server may search encrypted phrs on behalf of the doctor. in the system, the authors acquired the attribute of proxy-invisibility.

on encrypted cloud data, l. tao et al. present a search approach that uses characteristics to identify joint keywords (fmjk). this approach recommends that each d keyword be chosen at random from the non-duplicated keywords retrieved from the data owner's documents to construct a joint keyword and that all joint keywords form a keyword dictionary, considerably reducing the size of the keywords dictionary [9]. because the dimension of constructing indexes and trapdoors is proportional to the dimension of the keyword dictionary, it minimizes the dimensions of the key, indexes, and trapdoors, improving search efficiency. the content characteristics and query keywords are precisely aligned with the joint keywords in the phrases dictionary during the creation of each dimension of the indexes and trapdoors, resulting in a weighted score that assures query accuracy.

l. guo et al. suggested a secure-channel free ciphertext policy decryptable attribute-based information retrieval system that is resistant to selected plaintext, chosen keyword, and inside off-line keyword guessing attacks [10]. the lsss access policy is linked to keywords and plaintext messages in the proposed system, ensuring that only individuals with specific qualities may access encrypted data on the cloud platform. to abolish the secure channel in the trapdoor transmission process, the authors introduce the public and private keys of the cloud server. their technique takes advantage of cloud servers' processing and storage capabilities to enable the cloud server to conduct various associated functions, such as keyword retrieval and partial ciphertext decryption. consequently, for trapdoor distribution, the developed technique does not require a secure channel. on ehealth cloud platforms, the proposed technique may be utilized to promote safe sharing and fine-grained searches on encrypted ehrs.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005109|

III.PROPOSED SYSTEM

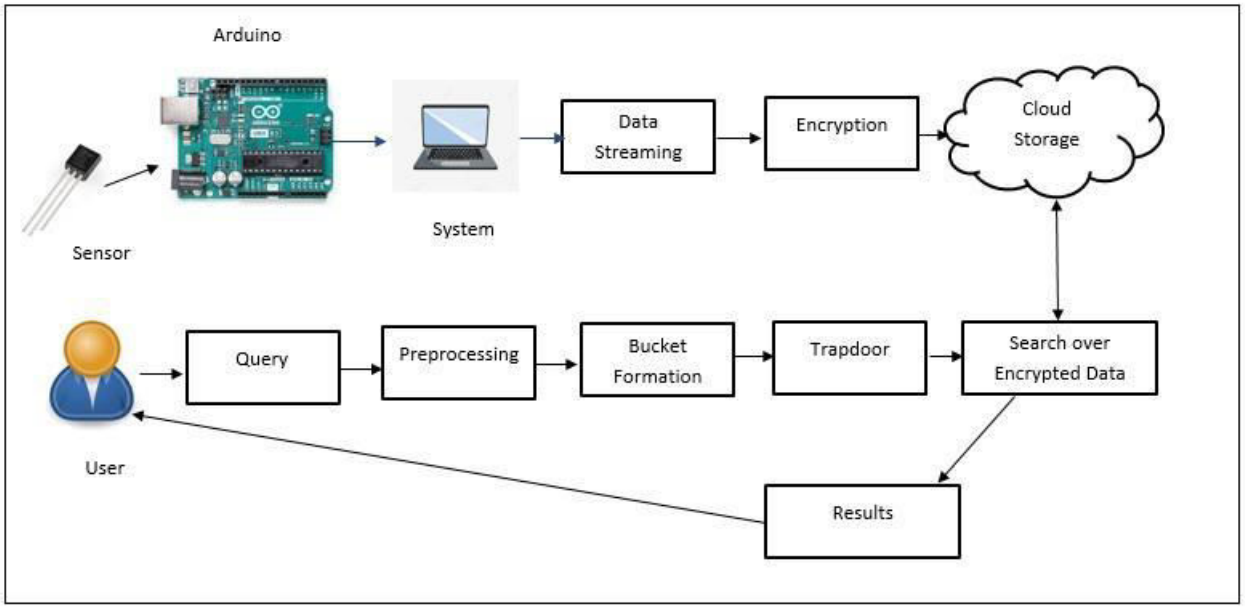

Fig 1 Proposed System

Figure 1 depicts the suggested solution for securing Internet of Things Medical Data on the public cloud, and the processes used to achieve it are discussed below.

Step 1: *User Registration and System Initialization* – The proposed system is designed using the Swings framework through the Java Programming language. The Interactive Interface is used by the user to register by providing valid details such as name, sex, email id, mobile number, user ID, and password. After successful validation and registration, the user can log into the system by providing the user ID and password used at the time of registration.

Once the user logs into the system it is greeted by an operation frame that contains several options in the form of a menu. These options include, edit, data storage, settings and logout. The user can edit the parameters of their profile entered during registration, through the edit option. The data storage option has 2 sub menus such as data streaming and view history, the data streaming option allows for the initialization of the data streaming from the sensors and the view history shows the data collected for a certain date. Once the streaming is initiated by the user the sensor data is collected as shown in the next step of the procedure.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005109|

Step 2: *Sensor Data Collection* – The Arduino UNO microcontroller is connected to the development machine to commence the methodology. The Arduino UNO controller is being employed to integrate the sensors and gather their information. This configuration makes use of a variety of sensors, including ultrasonic, skin temperature, heart rate, and ambient temperature sensors. Those very same sensors are linked to a microcontroller board and then a code that collects and streams sensor information to a laptop. The circuit connections for the sensor with the Arduino UNO microcontroller is given in the figure 2 below.

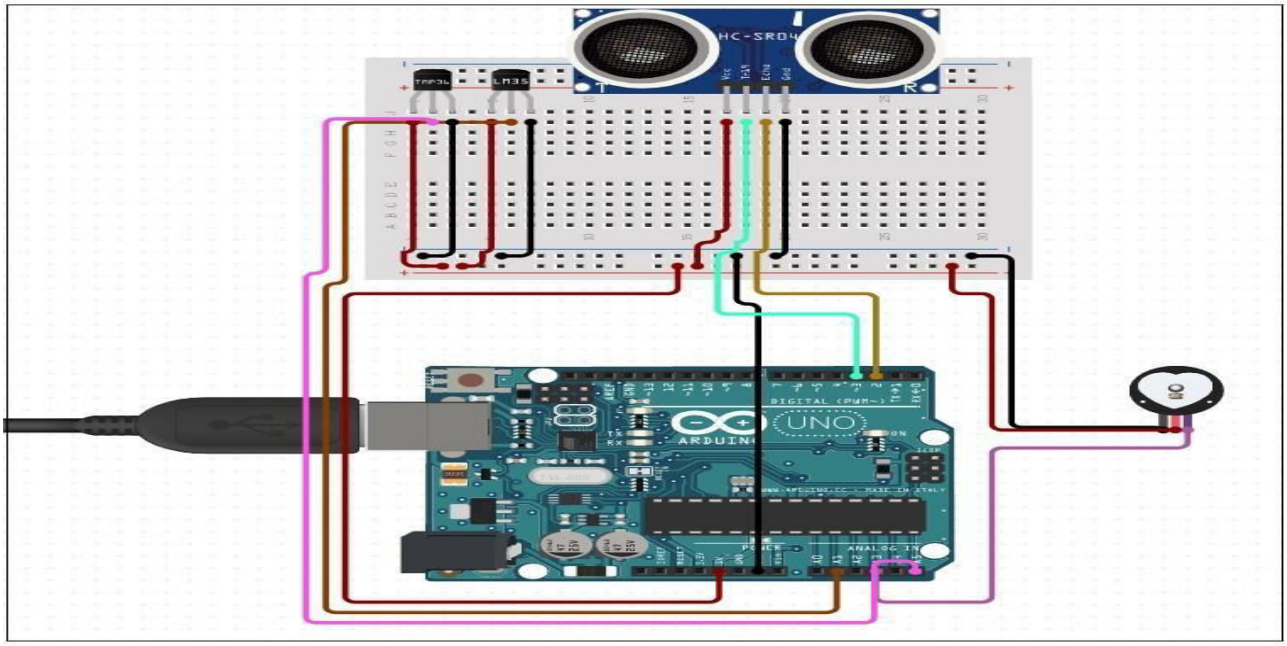

Figure 2: Circuit Diagram

The java code is commenced to gather sensor readings from the microcontroller. An intuitive user interface has already been designed for this objective in order to activate the sensor data gathering engine. When enabled, a thread is started that monitors on the COM27 port for sensor readings to be transmitted. The thread collects sensor values from the ultrasonic, skin temperature sensor, heart rate sensor, and ambient temperature sensor and stores them in the database together with the current date and time. As long as the thread is active, this will keep on going perpetually. The user interface allows you to pause the gathering of sensor readings by pressing the stop button, which instantaneously stops the thread from processing.

Step 3: *Sensor Data Encryption and Cloud Storage* – The sensor data transmitted in the preceding phase is used as an input in this stage, including the time and date to be encrypted. For this reason, the RCC (Reverse circle Cipher) Encryption protocol is used, and the encryption keys are created.

A hardcoded symmetric key is provided for the purpose of encryption. This key is sent into the RCC technique, which creates the keys that are then used to anonymize the sensor information.

Reverse Circle Cipher – The Reverse Circle Cipher is among the examples of highly efficient cryptographic techniques that can be used on a cloud infrastructure. The RCC approach works by rotating the input characters in precisely an anti-clockwise or clockwise direction, followed by character substitution. This is accomplished in the provided approach by dividing sensor data into groups and executing rotations on the pieces to encode information. The Reverse Circle Cipher properly performs the cryptography, and the cryptographic information is subsequently transmitted to the cloud. The Reverse Circle Cipher is amongst the most significant and economical encryption algorithms for protecting data confidentiality. The entire process for Reverse Circle Cipher Encryption is given in the Algorithm 1 below.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005109|

ALGORITHM 1: Reverse Circle Cipher

// Input: Sensor Data S_D

// Output: Sensor Cipher Data S_{CD}

Function reverseCircleCipher (S_D, KEY)

1: Start

2: Initialize list Block LST_{BLK} =∅, DIV_{STR}="", addupval=0

3: ***for*** i = 0 to size of KEY

4: addupval= addupval+ASCII ($KEY_{[i]}$)

5: ***end for***

6: addupval= addupval MOD 20

7: ***for*** i = 0 to size of S_D

8: char ch= $S_{D\,[i]}$

9: D_{STR} = D_{STR} +ch

10: ***if***(D_{STR} size =10), ***then***

11: LST_{BLK} = LST_{BLK} + D_{STR}

12: D_{STR} =""

13: ***end if***

14: ***end for***

15: LST_{BLK} = LST_{BLK} + D_{STR}

16:

17: **For** i = 0 to size of LST_{BLK}

18: STR= $LST_{BLK\,[i]}$

19: STR=rotate (STR, i)

20: **For** j = 0 to size of STR

21: char ch= $STR_{[j]}$

22: newchar=ASCII(ch) + addupval

23: S_{CD} = S_{CD} +newchar

24: ***end for***

25: ***end for***

26: ***return*** S_{CD}

27: **STOP**

Once the Data has been encrypted, it is then uploaded on to the Amazon public cloud through the AWS or Amazon Web Services integration. This is achieved by the user selecting the create table in cloud option which creates a table in the MySQL database instance on the amazon cloud. This table is then populated with the encrypted sensor

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005109|

values which can be seen through the view history option of the data storage menu. The data can be viewed for a particular date which is decrypted and shown to the user through the steps given below.

Step 5: *Searching* – The initial step that is performed for the purpose of enabling the search is the utilization of the trap door. A Trap Door is a set of encrypted Queries are used to search the encryptedentities such as the sensor dataunloaded on the cloud database, this is referred to as the Trapdoor. The trapdoor in this approach is the date of the sensor value collection.This date is stored in an encrypted form on the cloud database. The desired date for sensor data viewing by the user is first encrypted, this is act as the trap door for searching and then compared with the encrypted values on the cloud database. When the encrypted trapdoor matches the database records for the date, the data related with that date is retrieved and decrypted for presentation to the user.

This trap door is built for cloud platform search operations since the date given in encrypted format is comparable to the date used to store sensor data on the cloud database. This increases the searching module's accuracy and gives effective and comprehensive search results for the specific query.

IV.RESULT AND DISCUSSIONS

The presented technique for enabling search over the encrypted sensor data on public cloud is developed using java programming language through the use of the NetBeans Integrated Development Environment. A laptop for the purpose of development of this approach runs on the Windows operating system and has a configuration which consists of the Intel Core i5 Processor paired with 8 GB of RAM and 1 TB of hard drive space. The Arduino UNO microcontroller is being used to interface the various sensors and their readings. The Amazon Web Services is being used to store the sensor values on the cloud database.

The proposed technique's practicality has been carefully evaluated over a wide range of factors. The experimental investigation's outcomes are described below.

Encryption and Decryption Time performance

To provide adequate confidentiality of the sensor values getting transferred onto the cloud database, the suggested approach employs encryption and decryption algorithms. The functionality of this strategy must be evaluated, which accomplished using the methodology is outlined below. Table 1 shows the time required for the encryption and decryption procedures dependent on the amount of characters used.

Number of Characters	Encryption Time in Milliseconds	Decryption Time in Milliseconds
15	3	3
1808	15	17
2808	33	32
3012	46	54
5003	52	56
5789	64	62
6342	67	64
8426	77	78
9210	82	81
9991	96	99

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005109|

Table 1: Encryption and Decryption time performance

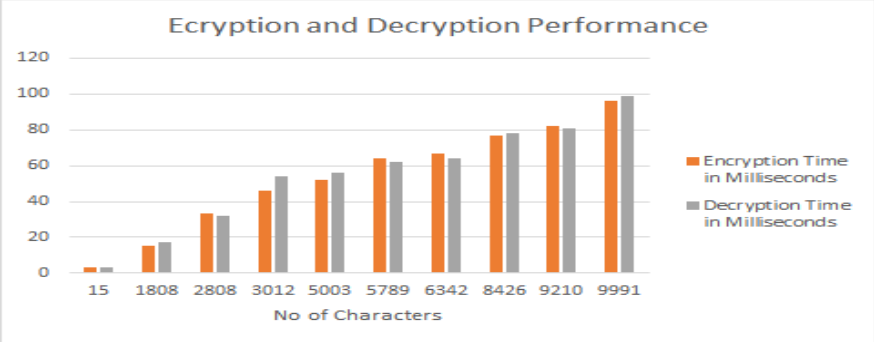

Figure 3: Encryption and Decryption Time

The listed results were appropriately retrieved for visual analysis in the bar graph shown in figure 3 above. As can be seen, the time needed for encrypting and decrypting is not exactly related to the number of input digits. This is because the cryptographic mechanism used for this strategy, the reverse circle cypher, has been carefully studied and deployed. This is why, as evidenced by the performance metrics, the execution of this strategy is incredibly effective.

V.CONCLUSION & FUTURE SCOPE

The proposed approach for the purpose of achieving an effective framework for enabling search over encrypted IoT data stored on a public cloud has been effectively outlined in this research article. The presented approach initiates with the user registering on the proposed standalone application by providing the relevant and valid details. Once the user is registered, they can log into the system by providing the relevant login credentials. After the authentication of the user, they are greeted with an operation frame where the system can be activated to start streaming the sensor values. The sensor array is fitted with 3 different sensors interfaced with an Arduino UNO microcontroller board. The sensor values are collected and then effectively encrypted using the Reverse Circle Cipher cryptographic technique. The encrypted data is then uploaded on to a cloud database using the Amazon Web Services. The uploaded encrypted data also contains an encrypted date which will be used for the purpose of trap door creation. The user can search the database for the sensor values based on a particular date which is encrypted and matched with the database values. Once the respective database value is matched, the related sensor values for the date are extracted and provided to the user after decryption. The approach has been effectively experimented to reveal that our approach has been implemented effectively.

The future directions to this research can be provided with the realization of the IoT data collection and encryption from multiple devices in multiple locations such as hospitals and clinics etc.

REFERENCES

[1] H. Li, D. Liu, Y. Dai, T. H. Luan, and X. S. Shen, "Enabling Efficient Multi-Keyword Ranked Search Over Encrypted Mobile Cloud Data Through Blind Storage," in IEEE Transactions on Emerging Topics in Computing, vol. 3, no. 1, pp. 127-138, March 2015, DOI: 10.1109/TETC.2014.2371239.
[2] C. Chen et al., "An Efficient Privacy-Preserving Ranked Keyword Search Method," in IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 4, pp. 951-963, 1 April 2016, DOI: 10.1109/TPDS.2015.2425407.
[3] X. Yao, Y. Lin, Q. Liu, and J. Zhang, "Privacy-Preserving Search Over Encrypted Personal Health Record In Multi-Source Cloud," in IEEE Access, vol. 6, pp. 3809-3823, 2018, DOI: 10.1109/ACCESS.2018.2793304.
[4] J. Yao, Y. Zheng, C. Wang, and X. Gui, "Enabling Search Over Encrypted Cloud Data With Concealed Search Pattern," in IEEE Access, vol. 6, pp. 11112-11122, 2018, DOI: 10.1109/ACCESS.2018.2810297.

[5] H. Wang, G. Sui, Y. Zhao, and K. Chen, "Efficient SSE With forwarding ID-Privacy and Authentication in the Multi-Data-Owner Settings," in IEEE Access, vol. 9, pp. 10443-10459, 2021, DOI: 10.1109/ACCESS.2020.3039040.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005109|

[6] O. Blazy, E. Conchon, M. Klingler and D. Sauveron, "An IoT Attribute-Based Security Framework for Topic-Based Publish/Subscribe Systems," in IEEE Access, vol. 9, pp. 19066-19077, 2021, DOI: 10.1109/ACCESS.2021.3051469.

[7] J. Gao and F. Zhou, "An Encrypted Cloud Email Searching and Filtering Scheme Based on Hidden Policy Ciphertext-Policy Attribute-Based Encryption With Keyword Search," in IEEE Access, vol. 10, pp. 8184-8193, 2022, DOI: 10.1109/ACCESS.2021.3136331.

[8] L. Xue, "DSAS: A Secure Data Sharing and Authorized Searchable Framework for e-Healthcare System," in IEEE Access, vol. 10, pp. 30779-30791, 2022, DOI: 10.1109/ACCESS.2022.3153120.

[9] L. Tao, H. Xu, Y. Shu, and Z. Tie, "An Efficient Search Method Using Features to Match Joint Keywords on Encrypted Cloud Data," in IEEE Access, vol. 10, pp. 42836-42843, 2022, DOI: 10.1109/ACCESS.2022.3168730.

[10] L. Guo, Z. Li, W. Yau, and S. Tan, "A Decryptable Attribute-Based Keyword Search Scheme on eHealth Cloud in the Internet of Things Platforms," in IEEE Access, vol. 8, pp. 26107-26118, 2020, DOI: 10.1109/ACCESS.2020.2971088.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details