Enhancement of RK- Blowfish Algorithm for Data Encryption through Block Chain in Healthcare System

Dr. D. Kalpanadevi
Assistant Professor
Department of Computer Applictaions
Kalasalingam Academy of Research and Education
Krishnan koil, TamilNadu, India
kalpanapani@gmail.com, dkalpanadevi@klu.ac.in
Dr. M. Jansi Rani
Assistant Professor
Department of Computer Science and Engineering
Mepco Schlenk Engineering College
Sivakasi, Tamil Nadu, India
jansirani.m86@gmail.com
Dr. M. Karuppasamy
Assistant Professor
Department of Computer Applictaions
Kalasalingam Academy of Research and Education
Krishnan koil, TamilNadu, India
karuppasamy.m@klu.ac.in

Article Info
Page Number: 70-80
Publication Issue:
Vol 71 No. 3s2 (2022)

Abstract
In this research work, the sensors device to be connected with network/service from everywhere, will receive signal from the biological changes of patients and transfer to the IoT middleware. Such information received by the IoT middleware is uploaded into the internet cloud, where the information is saved for further analysis. The middleware is controlled by IPv6 addressing scheme using Runge-Kutta (RK) Blowfish algorithm by making the modification in Feistel cipher of blowfish through integration of Blowfish and the Runge-kutta method. By this enhancement of RK- Blowfish algorithm, reported as efficient when compared to Advanced Encryption Standard. The healthcare paradigm being the ultimate focus of IoT, it has lot of issues concerning the security, addressing scheme, objects identified and network efficiency. The versatile features of healthcare scheme can be invariably fixed by carefully studying the features.

Keywords— Runge kutta Method, Blowfish algorithm, block chain, Data Encryption, IOT, Monitoring in healthcare

Article History
Article Received: 28 April 2022
Revised: 15 May 2022
Accepted: 20 June 2022
Publication: 21 July 2022

I. INTRODUCTION

This research work aims to find an essential medical care for diabetics and finding new ways of product designed to appeal through automatic inject insulin pump in monitoring the blood glucose level. RK- Blowfish IPv6 encryption [1] based addressing scheme provides high security for data transaction. Patient Controlled Encryption has been developed and helps the user to store the medical health records [2]. Patient's medical records are encrypted and securely stored in cloud [5-

9, 11,12]. By use of Blockchain, the data can be authenticated on concurrent data processing was performed and processed in a MySQL database in reliable manner.

.

II. LITERATURE REVIEW

Vardhan et al., [23] reviewed the study of METABO model on Diabetes Management system. It is used in healthcare management of diabetic patients. Their aim is to provide virtual and physical areas of patients to handle health and empower the patients' health care ability. They represented preliminary results of lightweight based on PHP usage and performance outcomes.

Sarierao et al.,[24] conducted a study on Smart Healthcare Monitoring System Using MQTT Protocol. A smart healthcare device is pre-owned to measure the blood oxygen level, heart rate, body movement and the body temperature of the patient. The aim of their system is to gather the data using sensors and send this data to the doctor or nurse for the purpose of continuous monitoring of a patient. In their study, microcontroller acts as a network server for connecting to the Internet using Wi-Fi. By using MQTT protocol and cryptographic protocol, they showed that there is no ambiguous data is stored along with the needed data and maintained security.

Mishra et al.,[25] discussed Remote Web Based ECG Monitoring Using MQTT Protocol for IoT in healthcare which is able to control and analyze any non-living object from anywhere. In health care system, it is pre-owned to monitor the heartbeat rate. They implemented MQTT based remote ECG monitoring system that allows detecting the heart rate of a person using heartbeat sensing even if the person is at home. The sensor is interfaced to Raspberry pi3, allows to check heart rate and transmitting the heart rate over internet.

From this survey of the research work, the aim of the proposed work is to combine automatic insulin pump therapy based on Block chain model with Continuous Glucose Monitoring for better controlling. It sends alert to inject insulin through automatic insulin pump to serve diabetes patients at the right time by making decision to control the risk.

.

III. SCOPE OF THE RESEARCH

The scope of the research work is to develop Continuous glucose monitoring (CGM) Sensor based on IPv6 using Blockchain. The main scope of this research is follows:

- To diagnose the Blood glucose test by learning the level of fluctuation parameter as per the severity found early and injects automatic insulin pump can be integrated with CGM sensor device.
- The primary goal of the research is to set the CGM Sensor based on IPv6 addressing scheme with Blockchain in IoT. Self-addressable, self-routable queries and data can be available in IPv6 addressing scheme by data centric approach. This addressing space provides up to 2^{38}.
- For security process symmetric key algorithm of RK-Blowfish algorithm is implemented and this can be compared with Advanced Encryption Standard and identify which one is efficient for safety to share the data along block chain.

.

IV. RESEARCH METHODOLOGY

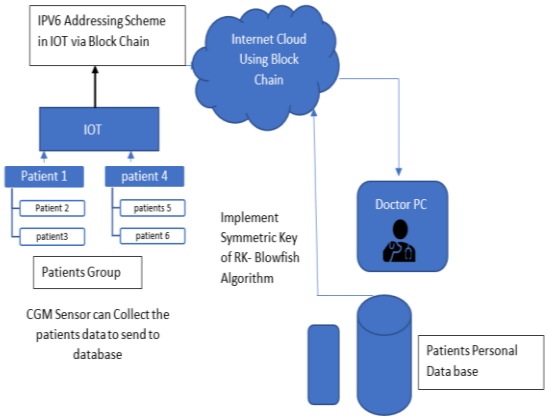

Figure 1. Architecture of Research Methodology

From figure 1 represents the research methodology can be summarized as given steps:

Step-1	Conduct the diabetic test for examining the risk factor of the diabetic patients. The Continuous Glucose Monitoring is integrated with IPv6 addressing scheme through Blockchain.
Step-2	By applying Blockchain, the patient data is collected in secure manner based on RK Blowfish algorithm.
Step-3	In order to compare Advanced Encryption Standard and RK Blowfish algorithm are applied for identifying which algorithm is efficient.
Step-4	Collecting the patient's data and storing in the database.

Primary goal of the research is to develop Continuous Glucose Monitoring Sensor based on IPv6 addressing scheme through Blockchain [3][4][5]. For security process it is used to compare cryptographic algorithms of symmetric key for identifying better performance of the encryption algorithm which stores the patients' data in database.

Blockchain is a smart intermediate function which can be used to store and retrieve the data that are connected to the blockchain network with IoT devices [16-22]. The Continuous Glucose Monitoring smart sensor can be worked when give treatment to patient, the data can be store on the blockchain network based on Ethereum platform. **Encryption Algorithm on IPv6 Addressing Scheme for Security Enhancement by comparing AES and RK-Blowfish Algorithm**

1. AES encryption algorithm

The AES encryption algorithm performs numerous transformations that an array of data is stored. The cipher text substitution of data process in first transformation; then the shifting of data in rows woks in second transformation and mixes columns in third.

Pseudocode

```
State =M
Add_Round_Key(State, &w[0])
For i=1 step 1 to 9
        SubBytes(State)
        ShiftRows(State)
        MixColumns(State)
        Add_Round_Key(State, &w[i*4])
End For
SubBytes(State)
ShiftRows(State)
Add_Round_Key(State, &w[40])
```

The last transformation is performed on each column using a different part of the encryption key. Longer keys need more rounds to complete. In this research, AES throughput time and encryption and decryption time taken are more to evolve in the work.

2. RK-Blowfish Algorithm

The symmetric cryptographic block cipher blowfish key has a key length is from 32 bits to 448 bits and 64-bit block size. In S- boxes, there is handle large key-dependent and 16- round Feistel cipher. Data encryption takes place at a rate of 26 clock cycles per byte on 32-bit microprocessor.

Key expansion renders the block of 64-bits into 4168 bytes in size, by transforming a 448-bit solution into several sub key arrays. It commended to be produced for encryption or decryption of data beforehand. The P-array contains 18, 32-bit sub keys such as $P1, P2 \ldots P18$ and S-Box of 4 thirty-two bits consist 256 entries each: S1:0. S1…. S3….255; S2:0, S2, 1……...S2……255; S3: 0, S3, 1……...S3….255;

Data encryption function iterates sixteen times of network. Every entity round contains a substitution of key-dependent alteration and data-dependent [10][13][14][15]. Then an operation completes XORs and the superfluities on 32-bits. The only complementary operation to the above regulating is indexing array of four data hunt portable for each encompassing.

Encryption

In Runge kutta method, forth order form can be followed in this work to reduce the storage requirements by this implementation. In fourth order method there is four approximations to the slope. Below given approximation of slope can be represents to estimate the slope at time t_0.

$l_1=f(x*(t_0), t_0)$

$l_2=f(x*(t_0) +l_1h_2, t_0+h_2)$

$l_3=f(x*(t_0) +l_2h_2, t_0+h_2)$

$l_4=f(x*(t_0) +l_3h, t_0+h)$

Each of these slope estimates by given below,

- l_1 is the beginning of the time step on the slope.

- If the slope l_1 time step on halfway, then l_2 is indicates slope at the midpoint estimation. From the second order midpoint method is indicates the slope as l_2. By making approximations for x(t), it comes more accurate than l_1
- If the slope l_2 time step on halfway, then l_3 is indicates slope at the midpoint estimation.
- Finally, the slope, l_3, the time step (to t_0+h) can use to step all the way across and the slope at the endpoint l_4 can be estimated.

Then to use a weighted sum of these slopes to get our final estimate of $y^*(t_0+h)$

$dx(t)/dt=f(x(t), t)$

To proceed by one time step h from a point at $t=t_0$, $x^*(t_0)$, and follow the given steps (repetitively).

$l_1=f(x*(t_0), t_0)$ approximate derivative at $t=t_0$

$x_1(t_0+h2) = x*(t_0) +k1h2$ intermediate estimate of function at t=t0+h/2(usingk1)

$l_2=f(y1(t_0+h2), t_0+h2)$ slope at t can estimate by

$t_0+h/2$

$x_2(t_0+h_2) =y*(t_0) + l_2h_2$ t can estimate by another intermediate function on $t_0+h/2$ (using l_2)

$l_3=f(x_2(t_0+h2), t_0+h2)$ another slope at t can estimate by

t0+h/2

$x_3(t_0+h) =y*(t_0) +l_3h$, here the function can estimate at

t=t0+h (using l_3)

$l_4=f(x_3(t_0+h), t_0+h)$ estimate of slope at $t=t_0+hy*(t_0+h)$ =

$y*(t_0) +l_1+2l_2+2l_3+x4/6$ estimate of $x(t_0+h)$.

In RK-Blowfish, incorporating the Runge kutta method with Blow Feistel network 64-bit data element as an input which consists of 16 rounds. Here

Divide K into 2 thirty-two- bit halves: lA, lB

For j=1 to 16:

F(YL)= (lA_1, a XOR lB_2, b) XOR (lA_3, c XOR lB_4, d)

XOR (<<<lB_2, b XOR<<< lA_3, c)

Here lA_1 represent as S1 , lB_2 represent as S2, lA_3 represent as S3, lB_4 represent two XOR operations (lA_1, a XOR lB_2, b) and (lA_3, c XOR lB_4, d) as parallelly evaluate under threads and two shift operations. This operation can be reduced to the time consumed for one XOR operation.

RK-Blowfish can ensure security with safety and maintains less memory usage when compared with other algorithms. Thus, encryption algorithm mainly rests on the key length the wit the supreme strength under Key Aggregation. It is helping the user to share their data partially over cloud storage. In Patient Controlled Encryption framework, the sensor can be implemented for store the patients' medical records over cloud and share their data.

In initialization of P-array and S-boxes, Blowfish's key plan can start with derived values from the hexadecimal of pi. In order the P entries are evolved with XOR for obtained secret key. All-zero blocks of 64 bits have encrypted. The outputs result can be calculated by adding with modulo of 232 and inverted by XOR of P on ciphertext block, then P-entries for reverse order [14].

EXPERIMENT ANALYSIS

Table 1 Comparison of different features in

Algorithm	**Key size**	**Blocks**	**Round**	**Structure**	**Features**	**Flexible**
Advanced Encryption Standard	128,192,256 bits	128 bits	Depend upon the Key size 10,12,14	Substitution Permutation	Excellent Security	Yes
RK-Blowfish Proposed Method based on Runge Kutta Method	32 to 448 bits	64 bits	16	Fesital	Excellent Security	Yes

Table 1 represents the comparison of features analyzed from the two algorithms. Here the key-size, Blocks, Round represent depend upon the key size how many times it can be rounded on the box, structure, features and flexibility can be analyzed.

Table 2 Comparison Time Efficiency during
Encryption and Decryption

FOR 60 KB FILE SIZE	**Time Taken**	
	AES	**RK-Blowfish**
Encryption Time per second	50.05	31.09
Throughput Time MB Per Second	0.0214	0.0102
Decryption Time per second	49.5	32.45
Throughput Time MB Per Second	0.028	0.0107

Table 2 represents the time taken per second. The performance of different algorithm is analyzed with respect to application of the training data of file size 60KB as denoted in figure 2. Encryption

through put time and Decryption through put time is taken by 60 KB file size of training data. By comparing AES algorithm with RK- Blowfish algorithm, it gives better security than AES algorithm for storing data in database.

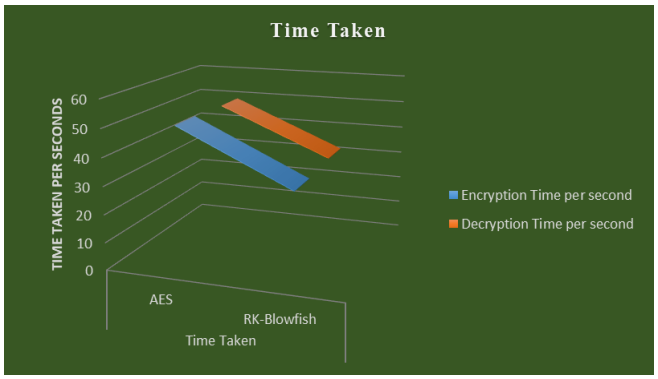

Figure 2 Time Taken for Different Algorithms during Encryption and Decryption

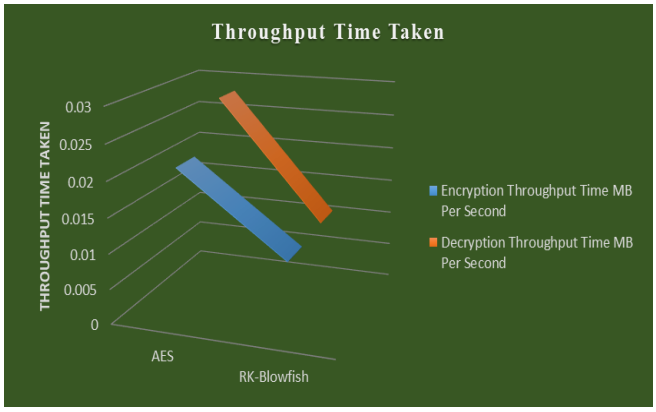

Figure 3 Throughput Time Comparison of Encryption and Decryption

Figure 3 illustrates, to comparison of throughput time of encryption and throughput time of decryption which can be analyzed in graphical method. Here Blue color represents an encryption throughput time of different algorithms and red color represents the decryption throughput time of different algorithms. The time taken by the file size is measured in Mega Bytes (MB) per seconds. Hence, RK-Blowfish algorithm takes less time on encrypt and decrypt the file efficiently as shown in figure 1.

Table 3 Comparison of Encryption Throughput Time for Different File Size

FILE SIZE	**Encryption Throughput time per seconds**	
	AES	**RK-Blowfish**
10 KB	51.8	38.98
25 KB	48.95	32.05
50 KB	43.77	30.21
1 MB	43.56	27.01

1.5 MB	45.23	23.91
2 MB	52.58	29.50
2.5MB	52.25	29.05
Average Throughput Time MB per Seconds	0.0204	0.0131

Tables 3 and 4 represent encryption and throughput time taken for decryption in different file sizes. For experiment, 10 KB to 2.5 MB of data can be applied. Here also, the table shows that RK-Blowfish algorithm records the data faster during encryption time and takes less time taken in comparison to other algorithms. Additionally, RK-blowfish algorithm is compared as a highlight for securing of data, faster in decryption and takes less time to achieve the security alert.

FILE FORMAT	**Decryption Throughput time per seconds**	
	AES	**RK-Blowfish**
1 0 KB	49.87	36.5
25 KB	48	30.45
50 KB	42.62	28.96
1 MB	44.4	28.35
1.5 MB	45.1	28.91
2 MB	52.4	29.04
2.5MB	52.2	25.01
Average Throughput Time MB per Seconds	0.0221	0.0111

Table 4 Comparison of Decryption Throughput Time for Different File Size

Table 5 Comparison of Memory Usage

ALGORITHM	**MEMORY USAGE**
Advanced Encryption Standard	30 KB
RK-Blowfish Proposed Method based on Runge Kutta Method	10.45 KB

Table 5 illustrates that RK-Blowfish algorithm consumes less memory storage space when compare with Advanced Encryption Standard.

CONCLUSION

In this research work, it can be concluded that RK-Blowfish IPv6 based addressing scheme and data encryption can be provide high data security. PCE has been developed and helps the user to store the medical health records. Patient's medical records are encrypted and securely stored in cloud.
By use of Blockchain, the data can be authenticated on concurrent data processing was performed and processed in a MySQL database in reliable manner.
The IPv6 addressing scheme used here allocates and connects all types of sensors and actuators and the sensor data connected to the cloud determines their emergency to counselling. The sensor can be embedded to their body for monitored to the patients in efficient manner.
In an embedded system, this security algorithm can be worked in proper way to analyzed the performance of throughput time of encryption and decryption and memory usage taken. When compared Advanced Encryption Standard, the RK-blowfish algorithm has made better results, also it is secure and faster process.

REFERENCES

1. Jara, A. J., Ladid, L., & Gómez-Skarmeta, A. F. (2013). The Internet of Everything through IPv6: An Analysis of Challenges, Solutions and Opportunities. J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl., 4(3), 97-118.
2. Bequette, B. W. (2010). Continuous glucose monitoring: real-time algorithms for calibration, filtering, and alarms. Journal of diabetes science and technology, 4(2), 404-418.
3. Xiao, C., Wang, L., Jie, Z., & Chen, T., Multi-level intelligent selective encryption control model for multimedia big data security in sensing system with resource constraints. In 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud) 148-153.

4. Mehedi, S.K.T.; Shamim, A.A.M.; Miah, M.B.A. Blockchain-based security management of IoT infrastructure with Ethereum transactions. Iran J. Comput. Sci. 2019, 2, 189–195.
5. Firouzi, F., Farahani, B., Ibrahim, M., & Chakrabarty, K. (2018). Keynote paper: from EDA to IoT eHealth: promises, challenges, and solutions. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 37(12), 2965-2978.
6. Kumar, G., & Tomar, P. (2018). A survey of IPv6 addressing schemes for internet of things. International Journal of Hyperconnectivity and the Internet of Things (IJHIoT), 2(2), 43-57.
7. Huang, J., Meng, Y., Gong, X., Liu, Y., & Duan, Q. (2014). A novel deployment scheme for green internet of things. IEEE Internet of Things Journal, 1(2), 196-205.
8. Kumarage, H., Khalil, I., Alabdulatif, A., Tari, Z., & Yi, X. (2016). Secure data analytics for cloud-integrated internet of things applications. IEEE Cloud Computing, 3(2), 46-56.
9. Ali, I., Sabir, S., & Ullah, Z. (2019). Internet of things security, device authentication and access control: a review. arXiv preprint arXiv:1901.07309.
10. Jeeva, A. L., Palanisamy, D. V., & Kanagaram, K. (2012). Comparative analysis of performance efficiency and security measures of some encryption algorithms. International Journal of Engineering Research and Applications (IJERA), 2(3), 3033-3037.
11. Judmayer, A., Ullrich, J., Merzdovnik, G., Voyiatzis, A. G., & Weippl, E. (2017). Lightweight address hopping for defending the IPv6 IoT. In Proceedings of the 12th International Conference on Availability, Reliability and Security, 1-10.
12. Talal, M., Zaidan, A. A., Zaidan, B. B., Albahri, A. S., Alamoodi, A. H., Albahri, O. S., ... & Mohammed, K. I. (2019). Smart home-based IoT for Realtime and secure remote health monitoring of triage and priority system using body sensors: multi-driven systematic review. Journal of medical systems, 43(3), 42-45.
13. Singhal, N., & Raina, J. P. S. (2011). Comparative analysis of AES and RC4 algorithms for better utilization. International Journal of Computer Trends and Technology, 2(6), 177-181.
14. Mr. Mehari Mesfin Abay, "Performance Analysis of Blowfish, Idea and AES Encryption Algorithms", International Journal of Research and Analytical Reviews, 7 (1), 668-678.
15. Akshaya, R., N. Niroshma Raj, and S. Gowri. "Smart Mirror-Digital Magazine for University Implemented Using Raspberry Pi." In 2018 International Conference on Emerging Trends and Innovations In Engineering And Technological Research (ICETIETR), pp. 1-4. IEEE, 2018.
16. R. Yetis and O. K. Sahingoz, "Blockchain Based Secure Communication for IoT Devices in Smart Cities," 2019 7th International Istanbul Smart Grids and Cities Congress and Fair (ICSG), Istanbul, Turkey, 2019, pp. 134-138.
17. G. G. Dagher, J. Mohler, M. Milojkovic, P. B. Marella, Ancile:Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology, Sustainable cities and society 39 (2018) 283–297.
18. L. Mearian, IBM Watson, FDA to explore blockchain for secure patient data exchange, https://www.computerworld.com/article/3156504/ibm-watson-fda-to-explore-blockchain-for-secure-patient-data-exchange.html, [Online; accessed 28-May2020] (2020).
19. G. G. Dagher, J. Mohler, M. Milojkovic, P. B. Marella, Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology, Sustainable cities and society 39 (2018) 283–297.
20. J. Xu, K. Xue, S. Li, H. Tian, J. Hong, P. Hong, N. Yu, Health chain: A blockchain-based privacy preserving scheme for large-scale health data, IEEE Internet of Things Journal 6 (5) (2019) 8770–8781.

21. RM Gomathi, JML Manickam, A Sivasangari, P Ajitha,"Energy efficient dynamic clustering routing protocol in underwater wireless sensor networks", International Journal of Networking and Virtual Organisations, Vol.22,4 pp. 415-432
22. M. Du, Q. Chen, J. Chen, X. Ma, An optimized consortium blockchain for medical information sharing, IEEE Transactions on Engineering Management (2020).
23. J. Xu, K. Xue, S. Li, H. Tian, J. Hong, P. Hong, N. Yu, Health chain: A blockchain-based privacy preserving scheme for large-scale health data, IEEE Internet of Things Journal 6 (5) (2019) 8770–8781.
24. Vardhan, B. S., Yeshwanth, C., Harsha, A. P., Reddy, E. R., & Narayan, K. R. (2019). Study on Diabetes Management using METABO on ICT, 1-5.
25. Sarierao, B. S., & Prakasarao, A. (2018). Smart healthcare monitoring system using mqtt protocol. In 2018 3rd International Conference for Convergence in Technology (I2CT), 1-5.
26. Mishra, A., Kumari, A., Sajit, P., & Pandey, P. (2018). Remote web-based ECG Monitoring using MQTT Protocol for IoT in Healthcare. Development, 5(4), 1096-1101.
27. Subhashini R , Milani V, "IMPLEMENTING GEOGRAPHICAL INFORMATION SYSTEM TO PROVIDE EVIDENT SUPPORRT FOR CRIME ANALYSIS", Procedia Computer Science, 2015, 48(C), pp. 537–540
28. Harish P, Subhashini R, Priya K, "Intruder detection by extracting semantic content from surveillance videos", Proceeding of the IEEE International Conference on Green Computing, Communication and Electrical Engineering, ICGCCEE 2014, 2014, 6922469
29. Sivasangari A, Ajitha P, Rajkumar and Poonguzhali," Emotion recognition system for autism disordered people", Journal of Ambient Intelligence and Humanized Computing (2019).
30. Ajitha, P.Sivasangari, A.Gomathi, R.M.Indira, K."Prediction of customer plan using churn analysis for telecom industry",Recent Advances in Computer Science and Communications,Volume 13, Issue 5, 2020, Pages 926-929.
31. Kanyadara Saakshara, Kandula Pranathi, R.M. Gomathi, A. Sivasangari, P. Ajitha, T. Anandhi, "Speaker Recognition System using Gaussian Mixture Model", 2020 International Conference on Communication and Signal Processing (ICCSP), pp.1041-1044, July 28 - 30, 2020.