Development of a Modified Medical Data Transmission over the Cellular Network System to Secure Health-Related Data from Changes in Environmental Parameters †

Krishnaveni Kommuri and Venkata Ratnam Kolluru *

Department of IoT, Koneru Lakshmaiah Education Foundation, Vaddeswaram 500502, AP, India; krishnavenikommuri2021@gmail.com
* Correspondence: kr20438148@wipro.com
† Presented at the International Conference on Recent Advances in Science and Engineering, Dubai, United Arab Emirates, 4–5 October 2023.

Abstract: Patients are generally sent to hospitals during emergencies and life-threatening conditions using ambulances. The health problems of patients become more serious when the treatment is delayed. If the vital signs of patients inside an ambulance or a treatment area sent to a hospital in real-time, the odds of saving lives will improve considerably. The patient’s medical needs can be arranged by paramedics with the doctors’ instructions until their arrival at the hospital. Information from past vital signs can also be archived their medical history. The Internet of Things (IoT) is a paradigm that visualizes practically everything connected to the Internet. This opens access to a lot of tiny medical needs and emergency relief tools. As a proof of concept, a test model prototype was implemented using an IoT-enabled ambulatory vital sign sensor board and a remote hospital framework. The objective of the implementation of such a prototype blends IoT technology with healthcare services to provide a more efficient and patient-centred approach to monitoring and controlling health issues, particularly in instances when continuous remote monitoring is advantageous. The working of the proposed device was validated and the results were monitored for the health-related data collected during the testing period. This strategy promotes health monitoring in emergencies with eHealth Signals for medical assistance.

Keywords: temperature; vital signs; health monitoring; cryptography; encryption; decryption; diagnosis; cipher text; internet of things; data privacy; patient monitoring

1. Introduction

Local hospitals should be willing to identify the most seriously wounded patients who need to be treated on time. In addition, additional medical staff and supplies and medical advice for patients in critical condition may be considerably delayed. Consequently, human lives are at risk in such cases. There is a need to bridge this gap and reduce the delay. Also, paramedics are not the decision-makers for the most important patients, and immediately after the outbreak of a mass accident, there is an absence of doctors on the triage site to evaluate the condition of patients who have been seriously wounded. It is therefore beneficial to explore a technique to collect the health-related data of patients and move them to the hospital while ambulances carrying several patients are in transit. The main objective of our work discussed in this paper was to strengthen previous work with real-time vital signs of patients being transferred to a remote hospital in a fast and secure way.

Our focus is to transfer to remote hospitals the real-time vital signs of patients securely. Their live transmission will enable the emergency room doctors in the hospital to be well-equipped in advance to treat patients on their way to hospitals. The state of the art in emergency health care management is considered a high priority. In Section 1, we discuss the literature review, which covers the vital sign data transmission techniques and diagnosis...
analysis. In Section 2, the proposed modified Medical Data Transmission over the Cellular Network (MEDTOC) system architecture, and the algorithm to allocate patients to hospitals based on the importance of the Revised Trauma Score (RTS) and other factors, are discussed. In Section 3, we cover the development of the ambulatory vital sign monitoring system functional platform board. In Section 4, the Modified Medical Data Transmission over the Cellular Network (MEDTOC) system is presented. Section 5 addresses the A-Data encryption algorithm for data security and simulation results. In Section 4, the results and a discussion of the work are provided, and in Section 5, the conclusion and future work are presented.

2. Literature Review

Medical emergency systems enabled by IoT have expanded tremendously as a result of technical improvements and the need for more efficient and rapid healthcare solutions. According to research, they have the potential to transform emergency treatment by offering prompt interventions, increasing patient outcomes, and improving the entire healthcare experience. However, security, data privacy, interoperability, and regulatory compliance remain concerns that academics and developers are actively addressing in their work.

Using the previously presented Medical Data Transmission over the Cellular Network (MEDTOC) [1] method, the delay in the first visit with doctors can be greatly reduced. Similarly, the vital signs of many patients in the MEDTOC system can be combined, optionally reduced, and sent over the cellular network to local hospitals for patient monitoring. The received data are decompressed and separated in the hospital to be shown to the doctors. MEDTOC features complex packet-header formats, guidelines for patient grouping, and a web portal to provide doctors with a stable and familiar interface. In a recent paper, ref. [2] outlined a revised MEDTOC-based system for controlling and accessing patient data until they appear for medication at the local hospitals using Smart algorithms. To adapt to the resources available, the previously specified framework was altered and improved.

A medicine reminder mechanism was used to integrate the patient data collected onsite using vital motes [3] and send it to hospitals using the cellular network. Vital motes are instruments that capture a patient’s vital signs and relay them for medication. Most of these systems, however, are limited to data for single patients. On the other hand, the aggregation of data for multiple patients assessed in [4–6] was limited to internal use either on-site or in hospital triage rooms. A web portal was designed to enable registered users to obtain vital statistics about the overall scenario of disaster management. Earlier, the concept of real-time wireless transmission of patient medical data was introduced, and several systems for this purpose have been developed. For multiple patients, Code Blue sensors [7] may be used to aggregate information on vital signs, including temperature, blood pressure, levels of SpO2 saturation, and pulse rate.

An approach that allows physicians to track health-related data like ECG, BPM, SpO2, and blood pressure obtained using a real-time event-based engine [8–10] has been proposed by Iancu Constantin et al. An e-Health framework for cardiac tele monitoring, which uses a Link It One development board, has been developed [11]. In [12], an eHealth Smart Networked Device was investigated. A framework for the automated collection of patient information using wireless sensor networks linked to medical equipment has been proposed by Rolim et al. In an emergency, IoT-based healthcare secure strategies were applied for further investigation [13]. The data collected were transferred to cloud healthcare provider centres to store, process, and analyse the data from patients. The role of the IoT has motivated researchers to investigate its use in the field of health care in a secure way over the last few years [14]. In the healthcare sector, however, the introduction of IoT is still in the early stages. In many cases, the healthcare domain mandates pervasive approaches [15] in distinct interventions. Various health advances in research and technical aspects were discussed [16–28] using adaptable setups.
3. Methodology for Modified Secure IoT Healthcare System

The patient’s health parameters can be monitored locally by various approaches. They can be sent to a remote location using Internet packet protocols. Taking this as motivation, with improvisation, a working prototype model was built. The Internet of Things (IoT) plays an important role in connecting devices by using messaging standards and networking protocols. One can easily transmit important health messages. The open-source IOT cloud is useful for storing sensor data. The advantage of digitally storing data is that data can be retrieved easily and quickly in the event of an emergency for safe healthcare. It has the ability to handle many patients with the vital attributes of patient care and well-being. Push notifications can be used when critical values are not met in the event. The vitals of the patients are being monitored with proposed Health care platform. Considering each physician’s smart device is getting vital signs, it is possible to ensure the safety of many patients in transit. Any change in a patient’s condition is recorded by the most recent data collected.

This model is divided into 3 functional level modules as listed below:
2. Modified Medical Data Transmission over the Cellular Network (MEDTOC) system.
3. Data Encryption algorithm for health-related data security and simulation results.


Health-related data monitoring applications are very useful in the field of health at the platform level. The block diagram is shown in Figure 1. This device connects individuals to the patients. All of the kits monitor various health data such as temperature, SPO2, ECG, EMG, GSR, Pulse, airflow, BP, glucose, etc. Individual vital signs are stored along with the patient’s name and ID.

![Figure 1. eHealth ambulatory vital sign monitoring embedded system.](image)

It defines the sampling frequencies for different physical parameters that automatically bring about asynchronous systems. Individual records are saved in the cloud from the local database server. From the cloud, hospital assistants and doctors can access to diagnose patients, as shown in Figure 2. The differences and modifications performed in the above algorithm are tracked for all of the patients at the same time. It was modified as a one-to-one track from each patient in real time.
The strategic method is improved and explained in the algorithm steps below:

1. Monitoring of Vital Signs (patient vital signs data, patient vital signs references, physician scheduled at a base)
2. Given: vital signs data for N patients, database for M physicians, capacity L patients per physician
3. For (i = 1 to N)
4. Receive vital signs data of patient I and display it in a graphical reference scale;
5. Connect it to the physician schedule database = D
6. For (j = 1 to M)
7. Search for an available physician by status (P, Q, NA)
8. If (i = 1, i = M, i++) i.e., physician found with status P, alert the physician before the arrival of the data with an audible beep. Start sending the vital signs data of patient “i” to the physician with status (P), or go to step 1.
9. If (i = 1, i = M, i++) i.e., physician found with status Q, stop accepting more patients capacity /// is reached. Record physician ID (T, Z) where T = title or “ID” of the physician and Z = MAC address of the physician’s smart device.
10. Or go to step 1.
11. if (j = 0, j = M, j++) i.e., physician found with status NA, patient is sent to step 8.

3.2. Modified Medical Data Transmission over the Cellular Network (MEDTOC) System

There are many mental images about what the term ‘Smart Hospital’ means. The reality, however, is that adding technology, devices, and sensors does not inherently make a building ‘smart’. In some situations, digital technologies are being pushed into hospitals without even worrying about the consequences. While hospitals are under increased pressure to achieve a real-time health system, they are hampered by the nature of their operating models or the interoperability problems that may exist. The approach helps to build the new eco system in the health domain to address the realtime problems. addresses consequences from all perspectives.

Smart Hospital digital technology can deliver a viable means to address these challenges. Figure 3 represents the patient ambulatory vital signs test setup arranged to monitor health-related data: (1) Identifying physical objects and their digital representation (basic requirement); (2) Creating an instance of physical objects and their environment, and connecting to existing data and systems (PLM and MES); (3) Selecting the connectivity protocols and using application needs; (4) Considering security; (5) Considering data science to be applied to achieve the requirements; and (6) Maintaining the records to clear and reuse the data.
The value of the modified MEDTOC system includes: (a) Improves overall quality and predicts quality (b) Provides services; (c) Records rotation and serialization; and (d) Grows revenue and opportunities. The developed hospital digital framework is shown in Figure 4. The vital sign values are taken from the in-patient outpatient services. These are coordinated at various stages, like patient health diagnostic services. Here, the vital signs are monitored and sent to the informatics lab. Any emergency services are linked by interconnected devices.

![Figure 3. Setup of the Ambulatory Vital Sign Monitoring Functional Platform Board.](image)

**Figure 4.** Information process of Ambulatory Vital Sign interconnected devices.

This is implemented by considering four key enabling factors: data, context, reasoning, and KPIs. Data from the Smart Hospital are used, such as data about people, processes, connected devices, operational building systems, Hospital/Clinical Information Systems, and external health systems, as discussed in the Client-Server Algorithm shown in Tables 1 and 2.

**Table 1.** Improved MEDTOC Client Side Procedure.

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create a Disaster Area (Location, Hospital, GPS)</td>
</tr>
<tr>
<td>2</td>
<td>Establish Secure Connection (Server(hi),Disaster Area Coordinates)</td>
</tr>
<tr>
<td>3</td>
<td>Form = 1………..n, 3.1 Retrieve (hospID, physID, Server(hi),DispatchpatID)</td>
</tr>
<tr>
<td>4</td>
<td>Establish Secure Connection (physID)</td>
</tr>
</tbody>
</table>
Table 2. Improved MEDTOC Server Side Procedure.

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Alert = Wait(H1); //Wait for the disaster management algorithm to start on server side</td>
</tr>
<tr>
<td>2</td>
<td>Retrieve info Disaster (disaster ID, GPS)</td>
</tr>
<tr>
<td>3</td>
<td>For each hospital “hi” in the list</td>
</tr>
<tr>
<td>4</td>
<td>Dmax = max distance (list)</td>
</tr>
<tr>
<td>5</td>
<td>Retrieve Info Patient (patID, RTS)</td>
</tr>
</tbody>
</table>

The modified MEDTOC calculates a hospital’s total treatment capacity (TTC) based on the individual critical care capacity (CCC) of each physician. The TTC of a hospital h is represented by the total number of patients. There are a limited number of physicians available to treat victims.

\[
TTC_h = \sum_{i=1}^{p} CCC_i
\]  

When a patient is assigned to a physician, the capacity of the physician and the hospital is updated. MEDTOC updates the selected physician’s CCC by subtracting the difference between the patient’s RTS value and the maximum possible [2] RTS value of 7.8408. The equations for updating treatment capacities after assigning patient m to a physician n at hospital h are shown below:

\[
CCC_{n,new} = CCC_{n,old} - (7.8408 - RTS_m)
\]  

\[
CCC_{h,new} = TTC_{h,old} - (7.8408 - RTS_m)
\]

The distance to the hospital, the hospital trauma rank, and the TTC are used to assign a patient to a specific hospital, as shown in Equation (4):

\[
\text{Priority}(h) = \frac{TR_h}{TR_{max} \times RTS} + (1 - \frac{D_h}{D_{max}}) + TTC_{h,available}
\]

The assignment of a patient to a specific hospital is determined by the distance to the hospital, the hospital trauma rank, and the TTC as shown in Equation (4). Equation (4) determines a hospital’s priority inpatient assignment based on three factors. The first factor takes into account the hospital’s trauma ranking. This rank, which ranges from 1 to 5, is derived from the five parameters listed below. These parameters were validated in collaboration with a major hospital and trauma centre’s Head of Emergency. The method was designed to help a large number of victims in a disaster who could be accommodated in local hospitals.

Context includes real-time information about the actual hospital’s current condition, the people within it, and their interactions with each other. The key element here is capturing the current status of people, systems, and things and making them more visible. Reasoning is a method for applying reasoning to data that are needed to drive action. Most commonly, the reasoning is based on separately processed rules, artificial intelligence (AI) or machine learning (ML) models, or temporal reasoning for a varied frequency of events. Key performance indicators (KPIs) provide a meaningful business context and ensure alignment between the hospital objectives and the performance measurement. This saves time and is shown in Table 3. The dashboard data are accessible from the cloud by using secure APIs.
As a result, emergency room wait times can be reduced and patient flow can be improved, decreasing operational costs and enhancing the patient experience. One hospital measured a 90 per cent improvement in cost savings after implementing digital technology to remove bottlenecks in bed management and inpatient flow [3]. One of the familiar vital signs is tracked and monitored and listed in Table 3 with the improved RTS range.

Another vital sign of the patient is tracked and monitored for one hour. It was analysed and observed and is shown in Figure 5. This system allowed for achieving real-time access by analysing the whole picture in real time. Hospital management can examine the complete hospital environment from data to workflows to patients to clinicians. If a patient’s condition is abnormal or there is an emergency on a certain floor, the right action in real time is to respond. Tracking and improving, and context-rich semantic linking, provides a picture of the past, present, and future state of the hospital.

Figure 5. Cont.
3.3. **A Data Encryption Algorithm for Data Security and Simulation Results**

It is important to talk about the security aspects of using block cipher security algorithms. Ambulatory vital sign data protections, including cryptography keys, are used to guarantee the security of the user data and prevent any identity fraud (authentication). With the multiplication of devices used to become more sensitive to access paid services (cloud) or any other access-controlled resource, this subsequent asset becomes more sensitive. Finally, to prevent computer failure or malfunction, system functionality itself must be secured. A hash function is a type of computation that can map an indeterminate size of data within a set data size. More specifically, it gives some quantities that represent the data for input.

For many different problems, from integrity and authenticity, hash functions can be used, such as a block cipher hash function.

A cryptographic hash function can be improved in three criteria:

- Preimage resistance
- Second preimage resistance (weak collision resistance)
- Strong collision resistance

In Table 4, explains the hashing techniques to data, which resulted in decent efficiency, security, and original data recovery.

**Figure 5.** Ambulatory Vital Signs data uploads in the Thing Speak platform.
Table 4. Ambulatory vital sign attributes applied for cipher algorithm and data recovery to the real-time environmental parameters monitored data.

<table>
<thead>
<tr>
<th>Monitored Day and Time</th>
<th>Entry Id</th>
<th>Humidity (g/m³) in %</th>
<th>Temperature in Degrees Celsius</th>
<th>Encrypted Data</th>
<th>Data Recovered</th>
</tr>
</thead>
<tbody>
<tr>
<td>2021-05-13 05:40:11 UTC</td>
<td>1</td>
<td>73</td>
<td>28</td>
<td>Okfh</td>
<td>jpfh</td>
</tr>
<tr>
<td>2021-05-13 05:40:38 UTC</td>
<td>2</td>
<td>73</td>
<td>28</td>
<td>Okfh</td>
<td>jpfh</td>
</tr>
<tr>
<td>2021-05-13 05:41:04 UTC</td>
<td>3</td>
<td>84</td>
<td>29</td>
<td>Plfh</td>
<td>jqfh</td>
</tr>
<tr>
<td>2021-05-13 05:41:31 UTC</td>
<td>4</td>
<td>86</td>
<td>29</td>
<td>Pnfh</td>
<td>jqfh</td>
</tr>
<tr>
<td>2021-05-13 05:42:00 UTC</td>
<td>5</td>
<td>78</td>
<td>29</td>
<td>Qpfh</td>
<td>Qpfh</td>
</tr>
<tr>
<td>2021-05-13 05:42:25 UTC</td>
<td>6</td>
<td>84</td>
<td>30</td>
<td>Plfh</td>
<td>plfh</td>
</tr>
<tr>
<td>2021-05-13 05:42:52 UTC</td>
<td>7</td>
<td>84</td>
<td>29</td>
<td>Plfh</td>
<td>plfh</td>
</tr>
<tr>
<td>2021-05-13 05:43:45 UTC</td>
<td>8</td>
<td>80</td>
<td>29</td>
<td>Pqfh</td>
<td>Pqfh</td>
</tr>
<tr>
<td>2021-05-13 05:44:10 UTC</td>
<td>9</td>
<td>77</td>
<td>28</td>
<td>Oofh</td>
<td>jpfh</td>
</tr>
<tr>
<td>2021-05-13 05:44:37 UTC</td>
<td>10</td>
<td>77</td>
<td>28</td>
<td>Oofh</td>
<td>jpfh</td>
</tr>
<tr>
<td>2021-05-13 05:45:04 UTC</td>
<td>11</td>
<td>76</td>
<td>28</td>
<td>Ofnfh</td>
<td>jofh</td>
</tr>
<tr>
<td>2021-05-13 05:45:31 UTC</td>
<td>12</td>
<td>77</td>
<td>28</td>
<td>Oofh</td>
<td>jpfh</td>
</tr>
<tr>
<td>2021-05-13 05:45:56 UTC</td>
<td>13</td>
<td>77</td>
<td>28</td>
<td>Oofh</td>
<td>jpfh</td>
</tr>
<tr>
<td>2021-05-13 05:46:06 UTC</td>
<td>14</td>
<td>76</td>
<td>27</td>
<td>Ofnfh</td>
<td>jofh</td>
</tr>
<tr>
<td>2021-05-13 05:46:36 UTC</td>
<td>15</td>
<td>76</td>
<td>28</td>
<td>Ofnfh</td>
<td>jofh</td>
</tr>
</tbody>
</table>

Here, the hash function used mathematical one-way functions and calculated them to create an input hash value. Using block ciphers, cryptographic hashes were created. The encryption was represented using modular arithmetic by first transforming the letters into numbers, according to the scheme:

\[ A = 0, B = 1, \ldots, Z = 25. \]

Encryption by a shift ‘n’ is described mathematically as:

\[
\text{En}(x) = (x + n) \mod 26 \quad (\text{encryption phase with shift } n) \tag{5}
\]

\[
\text{Dn}(x) = (x - n) \mod 26 \quad (\text{decryption phase with shift } n) \tag{6}
\]

To this, sensor values were observed as shown in Table 5 and fed to the program to generate cipher data as follows:

1. Assumed lowercase letters in string format.
2. A shifted integer between 0–25
3. Traversed one character at a time throughout the specified text.
4. Transformed the given character as per the rule for each character, depending on whether we are encrypting or decrypting the document. Return the newly produced string.
5. At the end, received the value (integer) for the text (string) and shift, and returns the encrypted text.

The development board came up with the AES architecture and presented here is the modification and improvisation that happened with the BCHASH algorithm padding procedure. Almost 20 years ago, the National Institute of Standards and Technology (NIST) developed AES as an encryption standard to replace the Data Encryption Standard (DES). AES encryption keys can go up to 256 bits, after all, while DES stopped at just 56 bits. A cipher that provided greater protection may have been chosen, but the trade-off would have required greater overhead, which would not be realistic.
Table 5. Real-time ambulatory vital sign data and encrypted data.

<table>
<thead>
<tr>
<th>Health-Related Data Monitoring Parameters</th>
<th>Encrypted Outputs for the Monitored Health-Related Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temperature</td>
<td>Glucose</td>
</tr>
<tr>
<td>--------------</td>
<td>---------</td>
</tr>
<tr>
<td>100.1</td>
<td>70</td>
</tr>
<tr>
<td>98</td>
<td>71</td>
</tr>
<tr>
<td>99.3</td>
<td>83</td>
</tr>
<tr>
<td>98.2</td>
<td>84</td>
</tr>
<tr>
<td>100</td>
<td>85</td>
</tr>
<tr>
<td>102</td>
<td>86</td>
</tr>
<tr>
<td>98.2</td>
<td>87</td>
</tr>
<tr>
<td>98.6</td>
<td>88</td>
</tr>
<tr>
<td>98.6</td>
<td>89</td>
</tr>
<tr>
<td>98.3</td>
<td>80</td>
</tr>
<tr>
<td>99</td>
<td>81</td>
</tr>
<tr>
<td>100</td>
<td>82</td>
</tr>
<tr>
<td>98.3</td>
<td>73</td>
</tr>
<tr>
<td>98.1</td>
<td>74</td>
</tr>
</tbody>
</table>

4. Results and Discussions

The proposed work helped the hospital framework, which helps to monitor vital signs such as BP, ECG, SpO2, and HR, which are converted to digital format. The system exhibits the patients’ physiological vital signs monitored on a local level. Once the data have been collected, they can be transmitted to a remote location using Internet packet protocols over a cellular network. In this study, a working prototype model was created based on a physiological monitoring platform. For testing purposes, we wrote code in the open-source Arduino integrated development environment (IDE) software to read the patient’s test temperature data and upload it to the Arduino board connected to the My Signals hardware. This code reads the health parameters and writes them to the serial port of the Arduino. The ESP8286 is an SoC with Wi-Fi connectivity. The ESP8266 has an embedded TCP/IP protocol stack that allows every microcontroller to connect to a Wi-Fi network. In the test model of our proposed device, we interfaced the ESP8266 computer with the Arduino module to read data from the Arduino’s serial port and transfer them to the remote hospital server. The Arduino board reads patient data and transfers them to the serial port of the Arduino. The ESP8286 module then reads the data from the serial port and sends them to a defined Thing Speak platform. Multiple real-time ambulatory vital signs are observed. Because each smart device is receiving the vital signs, it is possible to ensure that any change in the real values prompts an evaluation of the condition of the patient and is captured for analysis.

A host machine used to store the data is shown in Figure 2. The Arduino board sends medical sensor data to the serial port of the host machine, which displays the obtained vital signs in graphical form on the monitor attached to it. This helps the paramedics inside the ambulance, who will check the patient’s health status at any time. Figure 5 displays a single patient’s vital signs on Thing Speak.

Assuming N patients, M physicians, and K hospitals. The modified MEDTOC determines the available hospital nearby and the patient’s current state as determined by the paramedics and vital signs by solving Equation (4).

A considerable number of users are drawn to untrusted servers by the ease of maintenance and motivation. A cloud server (CS) can disclose confidential information to third parties. As a result, all data must be distributed in ciphertext mode to guarantee data confi-
dentiality and integrity in the face of untrustworthy cloud service providers (CSPs) [11,12]. The transmitted data are encrypted such that only approved parties can decipher them. The primary security methods used are presented. Symmetric encryption, also known as “private key cryptography”, is a simple and reliable means of securing online transmission. A private key saves arbitrarily generated words or combinations of letters linked to a hidden key to modify the message specifically. This encryption technique used is “block cipher”, with the amount of data encrypted or decrypted strictly proportional to the amount of time and processed for a fixed amount of data. The data are being monitored and applied to the block cipher algorithm to implement security aspects. Here, it was executed for 8 vital signs of the patient and performed encryption and decryption using the proposed block cipher hash values. Compared with various literature algorithms as listed in Table 6, the secure algorithm exhibited less time (0.6 ms) for encryption vice versa for decryption than the other algorithms. Finally, the objective of the proposed research method on a Secure IoT Healthcare Data Transfer System based on Environmental Parameters Monitoring was implemented.

Table 6. Comparative Analysis of Symmetric Encryption Algorithms.

<table>
<thead>
<tr>
<th>Factors</th>
<th>DES</th>
<th>3DES</th>
<th>AES</th>
<th>EDES</th>
<th>BCHASH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Length (bits)</td>
<td>56</td>
<td>112, 168</td>
<td>128, 192 or 256</td>
<td>1024</td>
<td>56</td>
</tr>
<tr>
<td>Cipher Type</td>
<td>Symmetric</td>
<td>Symmetric</td>
<td>Symmetric</td>
<td>Symmetric</td>
<td>Symmetric</td>
</tr>
<tr>
<td>Block Bits</td>
<td>64</td>
<td>64</td>
<td>128</td>
<td>128</td>
<td>64</td>
</tr>
<tr>
<td>Possible Key</td>
<td>$2^{56}$</td>
<td>$2^{112}$</td>
<td>$2^{128}$</td>
<td>$2^{1024}$</td>
<td>$2^{56}$</td>
</tr>
<tr>
<td>Time to Encrypt</td>
<td>7 s</td>
<td>21 s</td>
<td>13 s</td>
<td>2 s</td>
<td>0.6 ms</td>
</tr>
<tr>
<td>real-time data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td>Passing</td>
<td>Passing</td>
<td>Secure</td>
<td>Secure</td>
<td>Secure</td>
</tr>
</tbody>
</table>

5. Conclusions

The remote location is at a large distance from health centres. The sudden occurrence of a health emergency requires medication and treatment. This paper proposes a digital architecture Healthcare system for patients to a doctor at the nearest facility in normal situations and emergencies. A cloud-connected hospital framework is built. The framework includes patient ID, hospital ID, nearest accessible distance, and physician status in an interactive way using smart IoT platforms. The work represents a smooth function of the patients allocated to a doctor at the nearest hospital. In the communication of the inter-device patient data, the health messaging standards use the IoT (Internet of Things), and security aspects that were built play a vital role in effectively being able to store ambulatory vital sign data securely by improved hash algorithm techniques. As to future scope, we recommend extending the project reach by linking patient data obtained from essential motes and automatically transferring decisions using edge MQTT lightweight protocols. Starting with the first phases of system design and architecture, scalability and dependability were considered. Continuous monitoring and testing have been observed to maintain a high level of performance and availability as the system expands to accommodate more hospitals and patients.


Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.
Informed Consent Statement: Not applicable.

Data Availability Statement: All the data used are available in the present work.

Acknowledgments: I would also like to show my gratitude to Supervisor and KLEF, for guidance and assistance, which improved the quality of the research work and manuscript.

Conflicts of Interest: The authors acknowledged that there are no conflicting interests in the research work.

References


2. Zubairi, J.A.; Idwan, S. Smart algorithms for patient assignment in disasters. ICT Express 2018, 4, 107–111. [CrossRef]


15. Haghhi, M. A Flexible and Pervasive IoT-Based Healthcare Platform for Physiological and Environmental Parameters Monitoring. IEEE Internet Things J. 2020, 7, 5628–5647. [CrossRef]


Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.