A Reliable IoT-Based Embedded Health Care System for Diabetic Patients

Zeyad A. Al-Odat*, Sudarshan K. Srinivasan*, Eman M. Al-Qtiemat*, Sana Shuja†
*Electrical and Computer Engineering, North Dakota State University
Fargo, ND, USA
†Electrical Engineering, COMSATS Institute of Information Technology,
Islambad, Pakistan
Emails: *zeyad.alodat@ndsu.edu, *sudarshan.srinivasan@ndsu.edu, *eman.alqtiemat@ndsu.edu,
†SanaShuja@comsats.edu.pk

***Abstract*—This paper introduces a reliable health care system for diabetic patients based on the Internet of Things technology. A diabetic health care system with a hardware implementation is presented. The proposed work employs Alaris 8100 infusion pump, Keil LPC-1768 board, and IoT-cloud to monitor the diabetic patients. The security of diabetic data over the cloud and the communication channel between health care system components are considered as part of the main contributions of this work. Moreover, an easy way to control and monitor the diabetic insulin pump is implemented. The patient's records are stored in the cloud using the Keil board that is connected to the infusion pump. The reliability of the proposed scheme is accomplished by testing the system for five performance characteristics (availability, confidentiality, integrity, authentication, and authorization). The Kiel board is embedded with Ethernet port and Cortex-M3 micro-controller that controls the insulin infusion pump. The secure hash algorithm and secure socket shell are employed to achieve the reliability components of the proposed scheme. The results show that the proposed design is reliable, secure and authentic according to different test experiments and a case study of the Markov model. Moreover, a 99.3% availability probability has been achieved after analyzing the case study.**

***Index Terms*—IoT, security, embedded system, health care.**

I. Introduction

Cloud computing has been integrated with the Internet of Things (IoT) to enable the network devices to provide resilient services to all users and applications over the world. This integration helps to simplify the access of the IoT-enabled devices by all kind of users and applications, e.g., physical devices [1]. IoT is able to connect ubiquitous systems (including physical devices) using different network infrastructures to provide efficient services all the time [2].

The physical devices that are linked to the (IoT) are continuously increasing and emerging, which put a burden on the IoT service providers to provide secure and efficient services [3]. Physical devices are allowed to mimic human being's senses through various software and hardware that are connected together using the IoT. For example, the use of a smart home as an IoT-based application can turn on and off the air conditioning system when sensing the home residents leaving or coming their home [4]. Moreover, IoT-enabled devices can be controlled using a web page or smartphone applications, in the presence of Internet [5].

To utilize the IoT more efficiently, the industrial world has moved toward the use of IoT in small board and chips. For instance, manufacturers enable the internet connection on their small boards by adding the internet accessibility option to their products [6]. Moreover, different primitives can be connected together through IoT-based applications, and they can access a shared medium between them in the presence of IoT-cloud, e.g., the health care records that are shared between the patient, hospital, and eligible users can be accessed over the cloud through mobile applications [7].

The security and authenticity of the IoT-based applications become crucial, because many entities joined the world of IoT, and the possibilities of attacks and collisions have increased [8]. Therefore, the term of "Cyber-Physical System" (CPS) emerged to provide the integration between physical devices and cyber security [2]. Particularly, the integration of the IoT-base health care records where the health records are saved on the cloud and shared with different entities. Moreover, recent improvements in the IoT designs help with the support of health care systems, e.g., the tracking patient's records and bio-medical devices using the IoT applications [9][10].

Medical devices for diabetic care have also joined the world of IoT by supporting versatile design options [11]. However, security issues need to be addressed to ensure device security and the patient's privacy [12]. A system with an authentic security mechanism is required to guarantee the integrity and security of patient's records. One of the existing methods that can be easily implemented in hardware is the Secure Hash Algorithm (SHA) [13]. The SHA is an official hash algorithm standard that was standardized by the National Institute of Standards and Technology (NIST) [14].

SHA is compatible with hardware-level implementation, which makes it the most desirable methods for hardware designers to implement their reliable architectures [15]. The implementation of IoT technology in hardware has become crucial for high-performance applications [16]. The hardware allows a high-speed computation to manipulate and retrieve health records where health records are increasing day after the other. Therefore, medical-hardware designers have moved toward the use of IoT hardware-units in their designs to support high-speed computation power for IoT related functions [17].

This paper introduces an IoT-based embedded scheme for a diabetic insulin pump. The proposed design elaborates the mechanisms of data acquisition and monitoring between different parties (patient, cloud, hospital, and legitimate users). This design helps to share health data that are related to a patient's diabetes disease along with other health records on the cloud. All these data need to be secured and authenticated when they are retrieved from the cloud. We use the SHA algorithm to provide the security and authenticity terms for our proposal.

The rest of the paper is organized as follows. Section II provides preliminaries about the used components in this paper. Section III presents a literature review about the related work. The proposed methodology is presented in Section IV. Results and discussions are detailed in Section V. Section VI concludes the paper.

II. Preliminaries

Before going through the details of our proposal, brief descriptions about SHA-256, health care system components, and performance characteristics are presented in the subsequent text.

A. Brief Description of the SHA-256

SHA-256 is employed in our design to provide data integrity and authenticity. SHA-256 takes a message with an arbitrary size then, through message compression operations, produces a message hash of size 256-bit. Equation (1) shows how to get the hash (h) from a message (M) using compression function (H).

$$h = H(M), \tag{1}$$

where M is the input message and h is the digest generated using the hash algorithm H.

The secure hash algorithm is used to make sure that the data have not tampered during transmission. For instance, the message hash is computed at the sender side and appended with the transmitted message, then at the receiver side the received message hash is recomputed again and compared with the appended hash value. For the unchanged message, the hash values on both sides are equal, which means that the message has not tampered during the transmission.

Figure 1 depicts the general procedure that is used to compute the SHA-256 hash for any given message. The input message of size less than 2^{64} is padded first by adding 1 at the end of the message then add the least number of zeros to make it congruent to $448/512$. then the message size is appended to the end of the message as a 64-bit. At the end of the preprocessing phase, the final message size becomes multiple of 512-bit. Afterward, each message block is processed using the Initial Hash Value (IHV_0) and SHA-256 compression function (F). The output of each block is fed as IHV to the next block calculations.

At the end of the process, the hash value that is generated from the last block produces the final 256 bits hash. A detailed description of the secure hash algorithm can be found in [15].

Unlike the secure hash algorithm, the keyed-hash message authentication code (HMAC) involves a secure hash algorithm and a secret cryptography key. But, the *(*HMAC) algorithm is vulnerable against the length extension attack, which gives the attacker an opportunity to access the secret data [18]. Therefore, we avoid using the *HMAC* algorithm in our design. Though, data encryption functionality is the responsibility of the employed hardware and the encrypted *SSH* connection.

B. System Components

The proposed design consists of components that integrate together to form the overall architecture.

- Micro-controller unit. It is used to manage and control the medical devices according to a predefined procedure. This includes: delivers the control commands, daily patient's readings, and provide the secure connection layer. In our design, we use the Cortex-M LPC-1768 Keil board.
- Infusion Pump. It delivers the medical liquid (insulin) to the patient on a timely basis. In our design, Alaris-8100 infusion pump module is used.
- IoT-based cloud storage. In our proposal, we use the IoT-cloud as a medium between distributed medical institutions, patients and caregivers.
- Security components. They include a secure communication path using the secure socket layer (SSL/TLS), and cryptography mechanism to ensure the security of all system components.
- Legitimate users. The list of all authorized users to use the system according to predefined privileges.

C. Performance Characteristics

Today, some medical liquids are delivered programmatically without human intervention, e.g., insulin [19]. With medical devices that include embedded systems, a number of conditions need to be met to consider them as reliable and secure systems.

- Availability. The property that gives the probability of the system being in the normal state for a period of time.
- Confidentiality. The property that ensures the patient's information and system data are unavailable to unauthorized third parties.
- Integrity. All system data that can affect the treatment of the patient must not be altered without the patient's knowledge.
- Authentication. It means, only authorized parties or components should be able to act as a trusted user of the system.
- Authorization. The property of providing the verification of certain actions before execution.

These characteristics will be discussed in Section V.

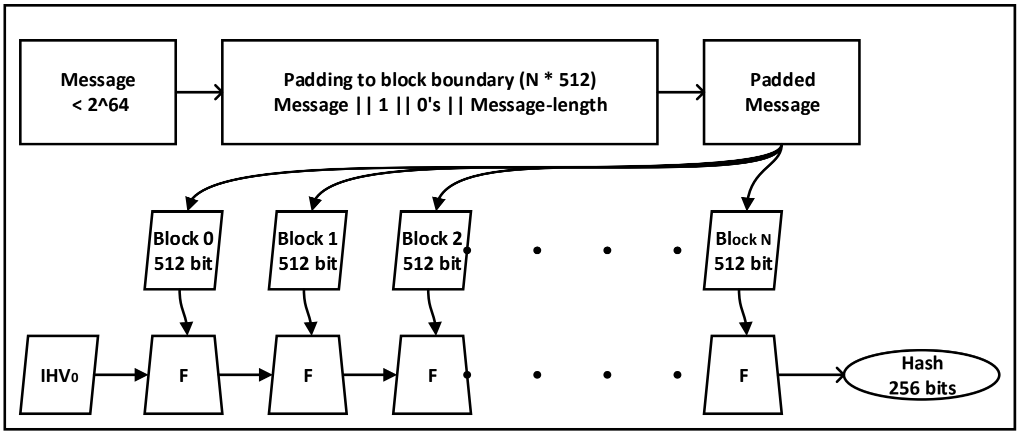


Fig. 1. General architecture to compute the SHA-256 hash function.

D. Contributions

The proposed design aims to provide the following contributions to the health care system, particularly diabetic patients. We use an external micro-controller (Kiel LPC1768) to program Alaris-8100 infusion pump. This design helps to solve current problems in the infusion pump.

- On-time medication, where a patient can get all his prescribed doses on time.
- Simplicity, affordability and the ease of use.
- Remote health record management through mobile applications or web browsers.
- Provide health service on the time of Off-Service physician.
- Provide secure and authentic health care service by employing cryptography and security approaches.

III. Related Work

Recently, the IoT-based applications have involved in all fields that influence Human life, especially, medical devices. The use of IoT in health monitoring and control is employed by different publications [9][13][20][21][22]. A novel IoT-aware smart architecture for automatic monitoring and tracking of the patient, personnel, and biomedical devices, was presented in [9]. The proposed work built a smart hospital system relying on three components: Radio Frequency Identification (RFID), Wireless Sensor Network (WSN), and smart mobile. The three hardware components were incorporated together through a local network to collect the surrounding environment and all related parameters to a patient's physiology. The collected data is sent to a control center in a real-time manner where all data are available for monitoring and management by the specialist through the Internet. The authors implemented a Graphical User Interface (GUI) to make the data access more flexible for the specialist.

To exploit the bridging point between the IoT and health care system, Rahmani *et al.* proposed a smart E-health care system for ubiquitous health monitoring [20]. The proposed work exploits ubiquitous health care gateways to provide a higher level of services. This work studied significant ever-growing demands that have an important influence on health care systems. The proposed work suggests an enhanced health care environment where control center burdens are transferred to the gateways by enabling these gateways to process part of the control center jobs. The security of this scheme was taken into consideration as the system deals with substantial health care data. The security scheme provides data authenticity and privacy characteristics.

A personalized health care scheme for the next generation wellness technology was proposed in [21]. The security of patient's records was addressed in case of data storage and retrieval over the cloud. The proposed work established a patient-based infrastructure allowing multiple service providers including the patient, service providers, specialists, and researchers to access the stored data. Their work was implemented on a cloud-based platform for testing and verification where a customized and timely messaging system for continuous feedback is tested. Moreover, multiple service providers are supported with an information infrastructure to provide unified views of patient's records and data. The use of special encryption schemes was also explored in [22], [23]. Liu *et al.* presented a scheme for secure sharing of personal health records in the cloud. The health records are ciphered before they are stored in the cloud. The proposed work uses Cipher-Text Attribute-Based Signcryption Scheme (CP-ABSC) as an access control mechanism. Using this scheme, they were able to get fine-grained data access over the cloud [22]. While Zhang *et al.* proposed a cloud storage scheme for electronic health records based on secret sharing. The proposed design consists of four phases, namely, the preprocessing phase, distribution phase, reconstruction outsourcing phase, and recovery and verification phase. In the preprocessing phase, each health record is uploaded to the cloud as a set of m blocks. Then in the distribution phase, the blocks are distributed over different storage locations in the cloud. In the reconstruction phase, the record's blocks are gathered from different storage locations. Lastly, in the verification phase, the gathered blocks are verified to determine whether if they belong to the accurate record or not [23].

With the emerge of IoT-enabled micro-chips, the researchers got benefited from this property by implementing embedded systems that provide IoT capabilities [24]. Different publications explored the use of embedded micro-controllers in medical devices. Particularly, the use of Keil LPC1768 micro-controller [13][17]. In [13], an online design for monitoring patient's data was presented. The proposed work employed an Advanced RISC Machine (ARM) architecture where Cortex M3 microprocessor is embedded in Keil LPC1768 board. In their work, the authors used pulse, temperature, and gas sensors to collect the patient's medical parameters. The LPC1768 board was used as a hardware layer between the Internet and the medical sensors. Each time the sensors' values change, the corresponding values on the Internet change immediately. However, their design was only used to monitor the surrounding environment without any interaction with the patient.

To have an embedded system with monitoring and control capabilities, Boppudi *et al.* proposed a data acquisition and control system using the ARM Cortex M3 microprocessor [17]. The proposed design send the monitored sensor data to the Internet using an Ethernet-controlled interface, which was built using Keil LPC1768 board. The proposed work employed two sensing devices temperature and accelerator-meter. Both sensors were used to collect data from the surrounding environment. The collected readings are sent to the Internet through the Ethernet interface. According to the uploaded readings, a specialist can change the behavior of the device through the Internet browser.

With the distributed components of the IoT-based health care systems, the need to verify and evaluate the integration of these components is crucial. The verification and evaluation of health care systems over the cloud is investigated by different researchers [25], [26]. Macedo *et al.* proposed a model to evaluate the IoT-based data redundancy. They employed a Markov model to test the probability of failure of one of the IoT components during the run time. They calculated the probability of failure of one of the cloud storage, then transfer the data store burden to less probability storage devices. The proposed design investigates the failure probability of the cloud storage components using the failure and recovery factor of each component. They were able to build a Markov model that describes the transition between the redundant storage locations at any given time [25]. However, Anastasiia *et al.* extended their work to build a model for IoT health care system [26]. The proposed work establishes a Markov model considering the failure of components for the IoT health care system. In their work, they gave the case study of Markov model to test the availability of health care components if any failure has happened at any time or location.

In the subsequent section, the integration between different components of the IoT health care system and the conjunction between the diabetic insulin pump (Alaris 8100) and Keil LPC-1768 board will be discussed in details.

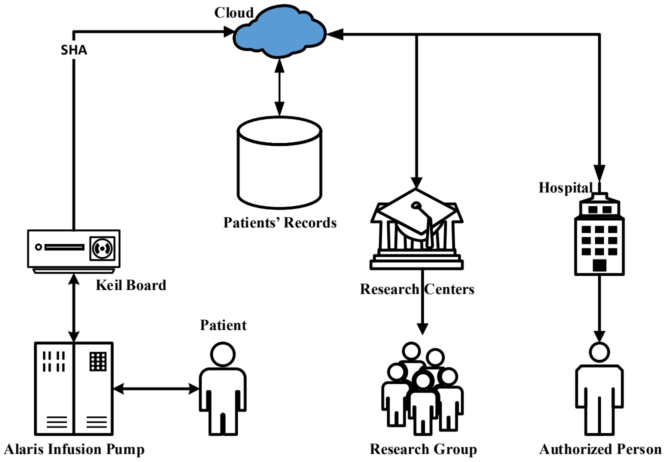


Fig. 2. General architecture of the proposed scheme.

IV. Proposed Methodology

In the proposed methodology, all system components that were mentioned in Section II will be integrated together to form the general architecture of the embedded IoT health care system. The proposed design comprises three main operations: monitoring, storing, and control, which are connected together to form the overall system. In this section, a case study of Markov model will be presented to test the availability of the proposed design.

For secure communication, the Secure Socket Shell protocol is employed. The SSH is the worldwide highest quality level for remote framework organization and secure document exchange. SSH is utilized in each datum focus and in each real endeavor. One of the highlights behind the enormous prevalence of the SSH is the solid verification utilizing SSH keys [27].

A. General Architecture of the Proposed Scheme

The proposed design employs the Alaris 8100 infusion pump to deliver insulin to the patient. The infusion pump is controlled using LPC-1768 board that contains the Cortex-M3 micro-processor. Figure 2 shows the general architecture of the proposed design.

The diabetic patient is attached to the infusion pump to get prescribed insulin doses. The Infusion pump is connected to the micro-controller unit (Keil LPC-1768 board) through a serial connection. A secure connection between the micro-controller and the cloud is established using the Secure Socket Shell (SSH) protocol and supported by the SHA-256 mechanism to authenticate the data exchange between cloud and micro-controller. Cloud computing provides the required infrastructure to handle all communications between the local and remote entities and reserves the desired amount of storage to store all health records and patient's data. The proposed architecture allows the authorized remote entities (e.g., medical and research institutions) to access the stored health records and monitor the patient's vital signs. Moreover, the proposed architecture provides the ability to control the infusion pump, remotely, through privileges that are given to an authorized physician.

Figure 3 shows the hardware setup of the proposed architecture. The Alaris-8100 infusion pump was disassembled to reach out the infusion components inside the pump. Then we built the interface between the Keil LPC-1768 board and the pump. Afterward, we used Keil μ-Vision Software Development Kit (SDK) to program the micro-controller.

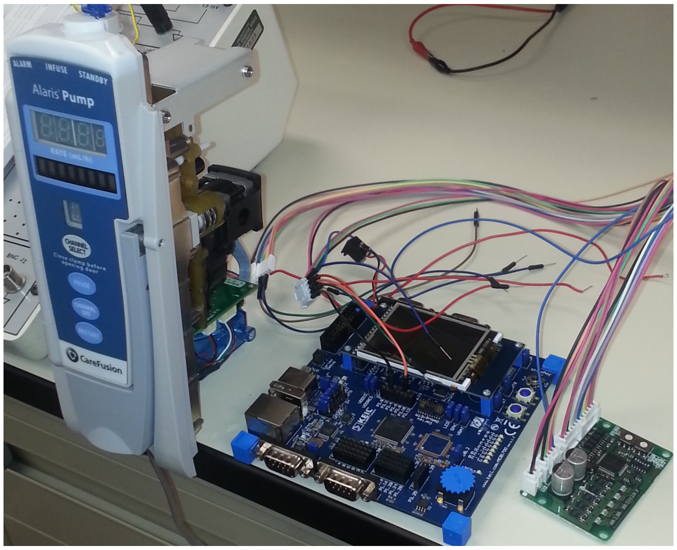


Fig. 3. Connection of Alaris Infusion Pump 8100 with Keil 1768 PCB board.

The hardware setup operations and system deployment were integrated together at the North Dakota State University (NDSU)-Electrical and Computer Engineering laboratories.

B. Monitoring, storing and controlling IoT health care system

The proposed design categorizes the IoT-health care system into three operations, which are the monitor, store, and control operations. The monitor operation involves the process of monitoring the status of the patient at any time and broadcasts the recorded data to the legitimate parties. The monitoring operation is accomplished by the micro-controller and insulin pump sensors. The store operation responsible for storing the collected data in local and remote databases, which is accomplished by the micro-controller. The control operation, which is accomplished by the micro-controller, changes the insulin pump schedule according to predefined or modified schedules. The schedule of the insulin pump is only generated by an authorized physician. Each operation is a complement to the other where the micro-controller operates as a common part between them.

1) Monitor health records: The process of health record monitor is accomplished according to Algorithm 1. The Secure Socket Shell (S) connection is initialized between the legitimate user and the cloud. Then the legitimate user receives the desired patient record appended with its SHA-256 hash value (H_p). The hash value (H_q) of the received record (P_q) is computed at the user side then, compared with the appended hash value (H_p). If both hash values are equal then the received health record is valid and contains the last updated health data.

Algorithm 1: Monitor patient's records

```
Input: Query ($Q$)
Output: $Q$ + Hash($c$)
for $q \leftarrow 0$ to $n$ do
    $S = Init(SSH)$
    $Receive(P_q + H_p)$
    $H_q = Hash(P_q)$
    $Compare(H_q, H_p)$
        $Case(equal) \leftarrow$ Valid
```

2) Store health records: Each health record has a designated SHA-256 value that is appended to the health record at the time of generation. Algorithm 2 shows the general procedure that is carried out to store the newly generated or updated health record. The hash value (H_p) of health record (P) that is related to the patient (i) is computed using the SHA-256 hash function. The computed hash (H_p) is appended to the patient record (P_i). An SSH connection between the micro-controller and the cloud is initialized to send the combination of hash and record (A_p) to the cloud for storage. Moreover, the new health record is stored in a Local Storage (LS) unit for quick data access.

Algorithm 2: Store health records

```
Input: Health record ($P$)
Output: $P$+Hash($P$)
for $i \leftarrow 0$ to $n$ do
    $H_p = Hash(P_i)$
    $A_p = Append(P_i, H_p)$
    $S = Init(SSH)$
    $LS(A_p)$
    $Send(A_p, S)$
```

As health records are sensitive information, the *SSH* uses a symmetric encryption mechanism to ensure the data privacy between different parties. This is accomplished after initialization of the *SSH* connection between client and server. The client initializes the connection by contacting the server, then the server responds to the client by sending the server's public key. Figure 4 shows the construction of data record (P_i). The data record is signed using the *SHA* algorithm, then the produced hash value (H_p) is appended to the end of the data record. Afterward, The *SSH* connection is used to transfer data record to the cloud.

3) Prescription control command: The prescription control command is generated by a remote caregiver. Algorithm 3

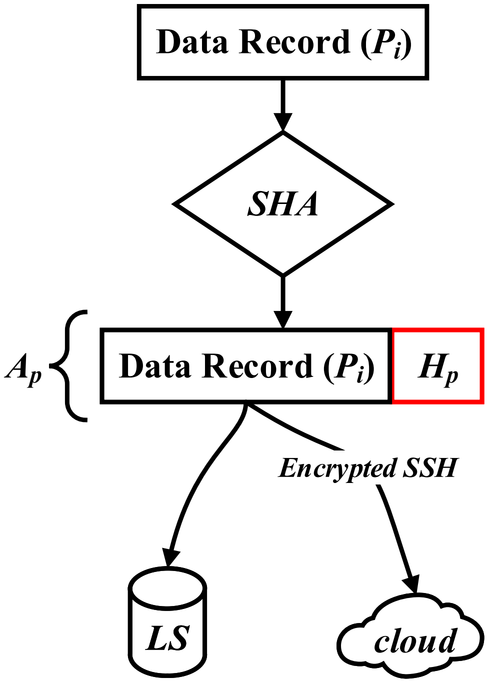


Fig. 4. Construction of data record.

shows the general procedure to send a new control command to the insulin pump. The prescription control command (C) is generated and appended with its corresponded SHA-256 hash value (H_c) to form the appended control command (A_c). A secure Socket Shell (S) is initialized between the remote caregiver and the micro-controller through the cloud. Then the new control command is sent through the SSH Chanel. At the receiving side, the micro-controller verify the received control command by following steps $3-6$ of Algorithm 1 where the received message is $C+H_c$. If the received prescription control command is valid, then the micro-controller will forward it to the insulin pump to start the new schedule.

```
Algorithm 3: Send prescription control command
  Input: Prescription control command ($C$)
  Output: $C$ + Hash($c$)
  for $i \leftarrow 0$ to $n$ do
      $H_c = Hash(C_i)$
      $A_c = Append(C_i, H_c)$
      $S = Init(SSH)$
      $Send(A_c, S)$
```

Figure 5 shows the connection between different components of IoT health care system. The embedded micro-controller controls the insulin device and collects the required health information. This is accomplished using a serial connection (6.25Mbps) between the micro-controller and the infusion pump. The Cortex-M3 micro-controller, which is embedded in the LPC1768 board, uses a universal asynchronous receiver-transmitter (UART) that supports 8 bits communication without parity and is fixed at one stop bit per configuration. The Keil LPC1768 board is programmed using micro-vision-5 software development kit (SDK) under windows 10 and implemented under *C* software stack.

The micro-controller collects data and stores them on local storage (LS) and remote storage (Remote DB) through the SSH connection. The IoT-cloud takes the responsibly to provide a replica for the stored data, it is considered as one of the great benefits of using the IoT-cloud. The data between the IoT-cloud and local storage are synchronized all the time to provide quick local access for the patient's health records.

The insulin device receives the doses schedule and delivers insulin to the diabetic patient. A local caregiver (CG) is responsible for a group of patients in emergency situations. A patient using the Alaris 8100 infusion pump will take preset insulin doses regularly [28]. The Alaris infusion pump is controlled and monitored by the Keil Cortex M3 board through a serial connection. All dosages related records are sent to the cloud through the Keil board using the Ethernet connection. To ensure the security and authenticity, the recorded data are digitally signed using the *SHA-256* compression function and encrypted using a symmetric key encryption mechanism. Moreover, the The signature and patient's records are stored together in the cloud.

In the cloud, a Secure Socket Shell (SSH) is provided to authorized entities to access the health records. For instance, a physician can follow up with a patient's case using a mobile application or a web browser. Furthermore, research institutions are given the authorization to access health records upon agreements made between patient, medical centers, and research institutions.

The integrity of the health care records is verified using the SHA-256 signature. While the authenticity is ensured by the encryption mechanism and *SSH* connection. The SHA-256 value is computed after the health records or prescription commands are generated. Then the generated SHA-256 is appended to the corresponding data (health record or preset control command). The health record and its signature remain correlated in all places (cloud, hospital, and patient's side). For instance, the physician in the hospital confirms that the record is received without altering using the SHA-256 signature. When the health record is received at the hospital, SHA-256 computation will be carried out. The resultant SHA-256 value will be compared with the appended SHA-256 value. Once both values are equal, the record will be confirmed to their corresponding patient. Otherwise, the health record will be discarded as it does not belong to the patient. Bearing in mind that all connections and data transfer are carried out using an encrypted *SSH* connection.

In the case of the preset control command, this command is generated from the hospital and appended with its corresponding hash value. The preset control command and the SHA signature are sent through the cloud to the infusion pump. At the patient's side, the hardware takes the responsibility to check

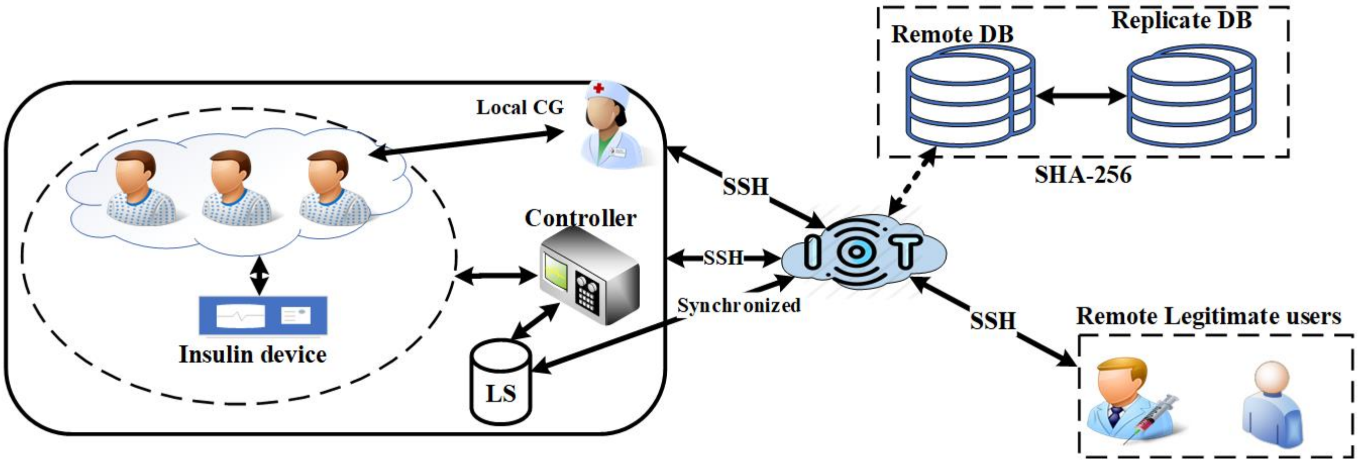


Fig. 5. General architecture of the proposed scheme.

the genuineness of the received control command by SHA-256 computation and comparison. The Keil micro-controller computes the SHA-256 value for the received preset control command and then compares the result with the appended SHA-256 value. Once authorized, the preset control command is passed to the infusion pump for a new schedule.

In the case of a fault exception, all Cortex-M processors (including Keil LPC-1768) have a fault exception mechanism embedded inside the processor. If any fault is detected, the corresponding exception handler will be executed [29].

C. Case Study: A Markov Model of proposed scheme

In IoT health care system, the failure of one or more components may lead to system failure. In our design, we have four main components: 1) Insulin Pump. It is represented by the Alaris 8100 infusion pump. 2) Micro-controller. It is represented by the LPC-1768 Keil board. 3) IoT-cloud. It provides infrastructure and medium. 4) Authority failure that represents the loss of security. Figure 6 shows the Markov model that connects the main components during system failure. The failure rate is represented by the symbol λ and the recovery rate is represented by the symbol μ.

The case study depicts 12 states that represent the transition from one state to another with the corresponding failure rate and recovery rate. However, some states are represented by the failure rate only because they are unable to recover. Thereby, the states are defined as follows: 1) Normal operation where all components work as required. 2) Insulin pump failure due to hardware defects. 3) IoT-cloud failure due to connection failure. 4) Failure due to data delivery between Insulin Pump and micro-controller. 5) Failure due to the power supply. 6) IoT-cloud software failure. 7) IoT-cloud hardware failure. 8) Insulin pump software failure. 9) insulin pump hardware failure. 10) IoT-cloud failure due to the failure of cloud components. 11) Insulin pump failure due to the failure of insulin pump components. 12) Failure of the system.

The Markov model depicted in Figure 6 can be represented as a system of Kolmogrov differential equations, as shown by equations (2)-(13). The probability ($P_i(t)$) represents the probability to find the system in state i. In our design, we chosen the initial conditions as follows: $P_1(t) = 1$, $P_i(t) = 0$ for i = 2, .., 12.

To collect the failure components and build our case study, we analyzed references [19][30][31][32][33][34][35]. All kind of failures are caused by software or hardware failures that might affect the main system components and cause the system failure. To further help other researchers, We list the values of failure and recovery rates in Table III.

$$\begin{aligned} dP_1/dt = -(\lambda_{1,2}+\lambda_{1,3}+\lambda_{1,4}+\lambda_{1,5})P_1(t)+ \\ \mu_{2,1}P_2(t)+\mu_{3,1}P_3(t)+\mu_{4,1}P_4(t)+\mu_{5,1}P_5(t) \\ +\mu_{11,1}P_{11}(t)+\mu_{12,1}P_{12}(t) \end{aligned} \tag{2}$$

$$\begin{aligned} dP_2/dt = -(\mu_{2,1}+\lambda_{2,9}+\lambda_{2,8})P_2(t)+ \\ \lambda_{1,2}P_1(t)+\mu_{9,2}P_9(t)+\mu_{8,2}P_8(t) \end{aligned} \tag{3}$$

$$\begin{aligned} dP_3/dt = -(\mu_{3,1}+\lambda_{3,6}+\lambda_{3,7})P_3(t)+ \\ \lambda_{1,3}P_1(t)+\mu_{6,3}P_6(t)+\mu_{7,3}P_7(t) \end{aligned} \tag{4}$$

$$dP_4/dt = -\mu_{4,1}P_4(t)+\lambda_{1,4}P_1(t) \tag{5}$$

$$dP_5/dt = -(\mu_{5,1}+\lambda_{5,11})P_5(t)+\lambda_{1,5}P_1(t) \tag{6}$$

$$dP_6/dt = -(\mu_{6,3}+\lambda_{6,10})P_6(t)+\lambda_{3,6}P_3(t) \tag{7}$$

$$dP_7/dt = -(\mu_{7,3}+\lambda_{7,10})P_7(t)+\lambda_{3,7}P_3(t) \tag{8}$$

$$dP_8/dt = -(\lambda_{8,11}+\mu_{8,2})P_8(t)+\lambda_{2,8}P_2(t) \tag{9}$$

$$dP_9/dt = -(\mu_{9,2}+\lambda_{9,11})P_9(t)+\lambda_{2,9}P_2(t) \tag{10}$$

$$dP_{10}/dt = -\lambda_{10,12}P_{10}(t)+\lambda_{6,10}P_6(t)+\lambda_{7,10}P_7(t) \tag{11}$$

$$\begin{aligned} dP_{11}/dt = -(\mu 11,1+\lambda_{11,12})P_{11}(t)+\lambda_{9,11}P_9(t)+ \\ \lambda_{8,11}P_8(t)+\lambda_{5,11}P_5(t) \end{aligned} \tag{12}$$

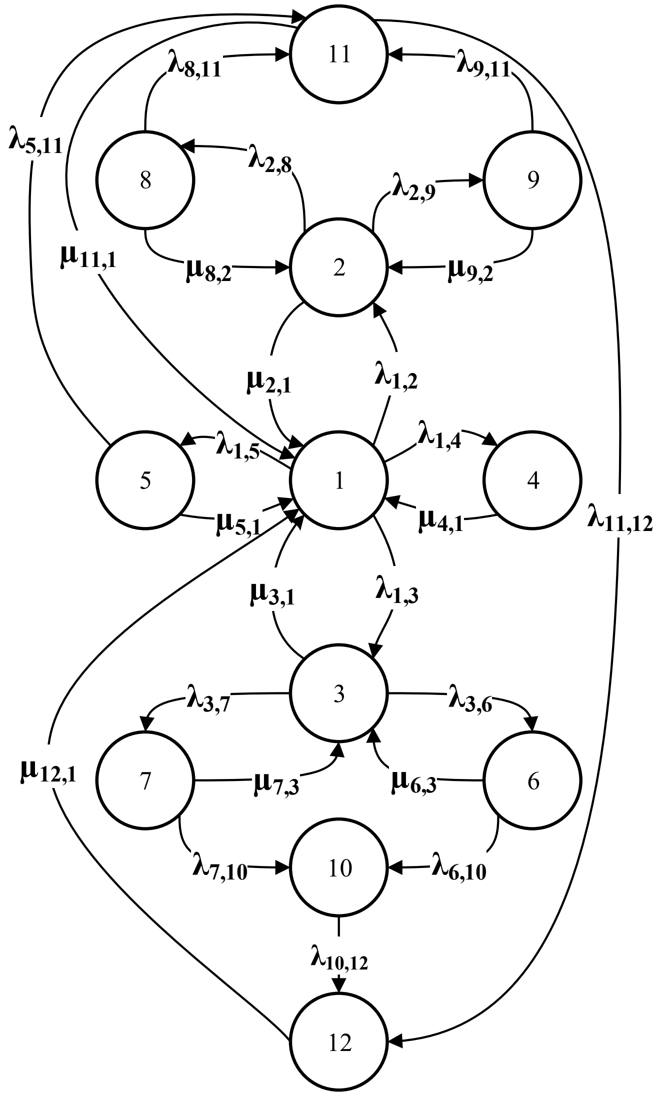


Fig. 6. Markov model graph for the IoT health care failure.

$$
\begin{aligned}
dP_{12}/dt = -\mu_{12,1}P_{12}(t) + \lambda_{10,12}P_{10}(t) \\
+\lambda_{11,12}P_{11}(t)
\end{aligned}
\tag{13}
$$

In the subsequent section, we show the performance characteristics and their applicability to our proposal.

V. Results and Discussion

Our proposal has been tested toward the five performance characteristics that are mentioned in Section II.

A. Availability

As mentioned earlier, the availability property ensures that the system is available all the time. Our design is tested for availability by solving the system of Kolmogorov differential equations and compute the probabilities of system states. The values of system sates probabilities, after calculations, are as follows:

$$
\begin{array}{ll}
P_1 = 0.9925712 & P_2 = 0.0002091 \\
P_3 = 0.0005966 & P_4 = 0.002998966 \\
P_5 = 0.00009805 & P_6 = 1.09E{-}06 \\
P_7 = 2.99E{-}05 & P_8 = 0.0019989 \\
P_9 = 0.00049866 & P_{10} = 4.24E{-}07 \\
P_{11} = 0.0009958 & P_{12} = 3.00E{-}07
\end{array}
$$

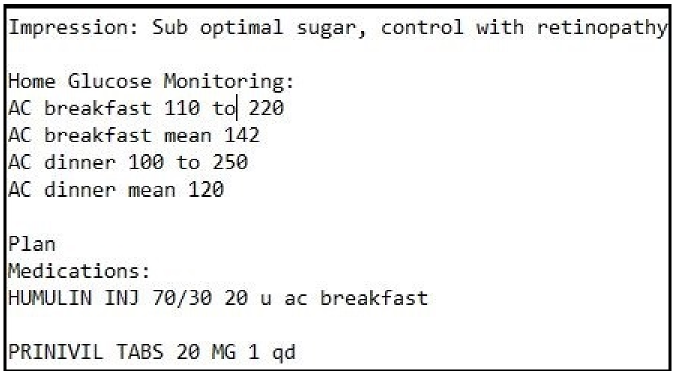
The availability function is represented by the probability value of $P_1(t)$, which means that the system has a probability of $\approx$ 99.26% to stay at the normal state. The calculated probability proves the availability property of the IoT health care embedded scheme. Through this value, the proposed design ensures a high level of availability.

B. Confidentiality

To provide a confident system for data on transit, our design uses the *SSH* tunnel that is only given to the authorized entities. The *SSH* connection is initialized only by a legitimate user and supported by "private-public key pair authentication" scheme that ensures the connection is established between the designated two parties.

C. Integrity

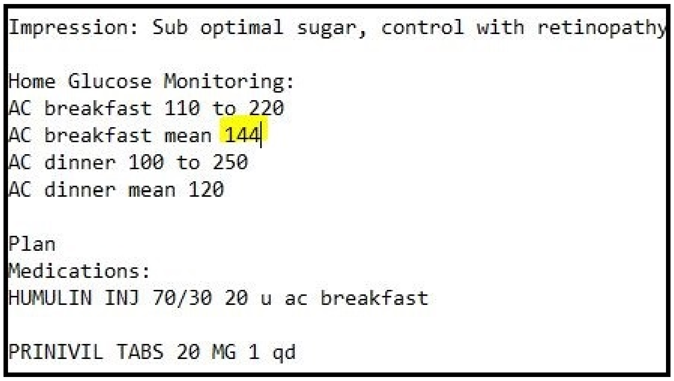
The proposed design has been tested and verified for integrity using sample data from [36]. The sample data contains glucose levels in the patient's body during a 24 hour period, a patient's profile information, and the patient's medical information. A snipped portion of the sample data is shown in Figure 7, the figure shows the glucose levels in the patient's body after two meals (breakfast and dinner). To test the integrity property, the sample data is modified as shown in Figure 8. When both figures are compared, the only difference between them is the "AC breakfast Mean", it is equal to 142 in the original sample and 144 in the modified one.



```
Impression: Sub optimal sugar, control with retinopathy

Home Glucose Monitoring:
AC breakfast 110 to 220
AC breakfast mean 142
AC dinner 100 to 250
AC dinner mean 120

Plan
Medications:
HUMULIN INJ 70/30 20 u ac breakfast

PRINIVIL TABS 20 MG 1 qd
```

Fig. 7. Snipped health record from the original sample.

The proposed design considers that the SHA-256 value is computed every time a health record is requested. The sample data is stored in the cloud and appended with the



```
Impression: Sub optimal sugar, control with retinopathy

Home Glucose Monitoring:
AC breakfast 110 to 220
AC breakfast mean 144
AC dinner 100 to 250
AC dinner mean 120

Plan
Medications:
HUMULIN INJ 70/30 20 u ac breakfast

PRINIVIL TABS 20 MG 1 qd
```

Fig. 8. Snipped health record from the modified sample.

corresponding SHA-256 value. If the patient's side requests the same health record, the micro-controller will compute the SHA-256 value of the record and compares it with the appended SHA-256 value. If both hash values (cloud and patient) are equal then the received record is valid and never been tampered during the transmission. Table I shows the SHA-256 value of the sample record on both sides where the sample record has not tampered.

However, any tiny modification to the health record will produce a totally different SHA-256 hash value. Table II shows two different hash values for the original sample that is requested from the cloud side and the modified sample at the patient's side. Both SHA-256 values are different because the received record on the patient's side has been altered during transmission. Then, the micro-controller at the receiver side will detect the alteration after comparing both hash values.

TABLE I. SHA-256 HASH VALUES OF THE SAMPLE DATA ON BOTH SIDES.

Cloud side:	14b93acf-ccdcbe40-ea3795be-c1073498-51a96c90-6cedfc9c-49d8e2cf-a141befb
Patient side:	14b93acf-ccdcbe40-ea3795be-c1073498-51a96c90-6cedfc9c-49d8e2cf-a141befb

TABLE II. SHA-256 HASH VALUES OF THE ORIGINAL AND MODIFIED SAMPLE DATA ON BOTH SIDES.

Cloud side:	14b93acf-ccdcbe40-ea3795be-c1073498-51a96c90-6cedfc9c-49d8e2cf-a141befb
Patient side:	358c4f29-f0e2bb60-8efa35d4-a88a6b3b-58939ffd-deebf824-8065c195-b834b8cd

On another hand, to ensure the integrity of prescription control command, the same procedure is carried out between the sender (corresponding physician) and receiver (micro-controller). At the patient's side, the micro-controller detects the alteration and discard the tampered control commands.

D. Authentication

To provide an authentic system, the SSH protocol is employed to ensure that only legitimate users are eligible to access the health records. Moreover, in the case of the prescription control command, special users are given a special SSH tunnel and a public-private key pair to ensure the security and authenticity of the communication medium between the Caregiver (CG) and micro-controller.

E. Authorization

The authorization and verification of certain actions before execution are accomplished by the encrypted *SSH* connection and the *SHA*, respectively. The encryption of health records ensures that only the authorized entities can decrypt and read the data contents. Moreover, if any certain action is tampered or modified before reaching the destination, then the corresponding hash value will determine whether the action is authorized. Moreover, the patient is given some privileges to change the schedule according to a predefined prescription from the corresponding physician.

F. Speed

The processing speed of the proposed design is tested using 70 samples of diabetic's records [37]. Figure 9 shows the time elapsed (in second), mean and standard deviation of the 70 samples. The elapsed time to process the samples depends on different factors, including, sample size, connection speed, and system utilization. The figure shows how the processing speed changes according to the aforesaid factors. The average time to process these samples is equal to $5.8e-04$-second, while the standard deviation value shows the amount of variation of the elapsed time for all samples.

G. Final Remarks

Our design provides a set of benefits to the health care systems, particularly, diabetic patients. We list these benefits as follows:

- Patients can access their health records easily and communicate with their caregiver instantly.
- Caregivers and physicians can control the insulin infusion pump remotely according to reliable information delivered through the proposed design.
- The security and integrity of patient's records are guaranteed by the encrypted *SSH* and the SHA.

However, the limitation of this approach can be seen in the case of a successful attack on the used security components. Until now, there is no successful collision attack for the *SHA-256* that is used in this design. The collision attack allows an adversary to tamper the data contents and produce the same hash (signature) of data before and after modification. Moreover, the length extension attack is a kind of attacks that targets the keyed hash algorithms (HMAC). Therefore, we avoid using the (HMAC) in our design and keep the authenticity requirements to the symmetric encryption mechanism of the *SSH* connection.

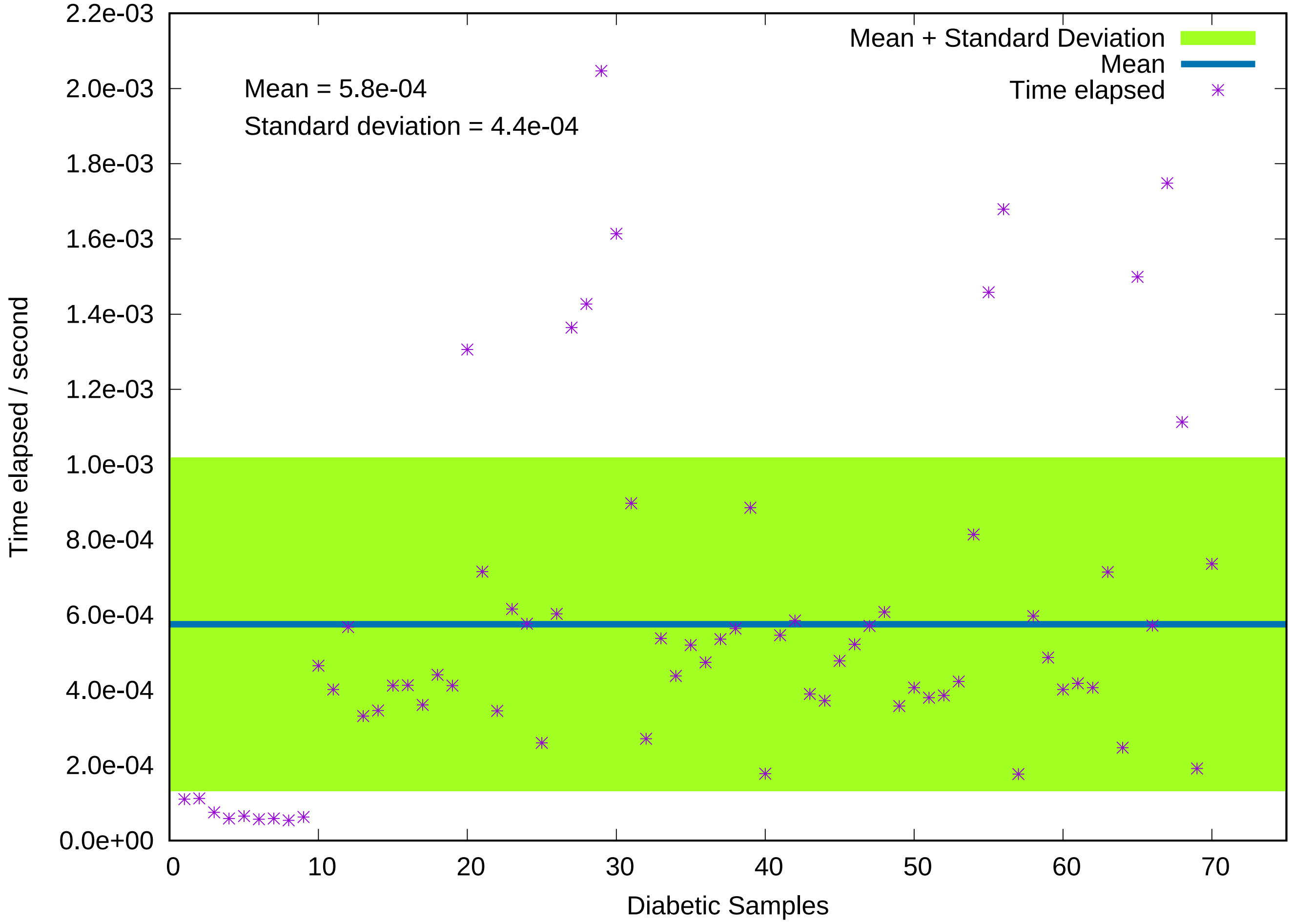


Fig. 9. Time elapsed to process 70 diabetic samples.

VI. Conclusion and Future work

In this paper, a reliable embedded health care system based on the Internet of Thing is presented. The proposed design employs secure hash algorithm SHA-256, Secure Socket Shell (SSH), Keil LPC-1768 board, Alaris 8100 infusion pump, and IoT-cloud to build the health care system. The proposed design showed that the reliability characteristics of availability, confidentiality, integrity, authentication, and authorization are accomplished. Moreover, the results showed that the proposed design has a 99.3% probability to stay in the normal operation stage and an average speed of 5.8×10^{-04} seconds to process the health records.

The scope of reliable IoT-based health care system is open. In the future, further analysis of the health care system to develop a generalized reliability model of the health care system including handheld medical devices.

Acknowledgments

This publication was funded by a grant from the United States Government and the generous support of the American people through the United States Department of State and the United States Agency for International Development (USAID) under the Pakistan - U.S. Science & Technology Cooperation Program. The contents do not necessarily reflect the views of the United States Government.

Computing services, financial and administrative support from the North Dakota State University Center for Computationally Assisted Science and Technology (CCAST) and the Department of Energy through Grant No. DE-SC0001717 are gratefully acknowledged.

Appendix

The values of failure and recovery rates, which were used in the case study, are listed in Table III.

References

[1] Z. A. Al-Odat, S. K. Srinivasan, E. Al-qtiemat, L. D. Mohana Asha, and S. Shuja, “Iot-based secure embedded scheme for insulin pump data acquisition and monitoring,” in *The Third International Conference on Cyber-Technologies and Cyber-Systems*. IARIA, 2018, pp. 90–93.

[2] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, “A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications,” *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, 2017.

TABLE III. FAILURE AND RECOVERY RATES PARAMETERS

Failure (λ)	Value	Recovery (μ)	Value
$\lambda_{1,2}$	1.857E-09	$\mu_{2,1}$	99.57E-2
$\lambda_{1,3}$	2.499E-07	$\mu_{3,1}$	95.08E-2
$\lambda_{1,4}$	3.331E-07	$\mu_{4,1}$	98.76E-2
$\lambda_{1,5}$	4.985E-07	$\mu_{5,1}$	92.37E-2
$\lambda_{2,8}$	2.50E-07	$\mu_{6,3}$	2.12E-3
$\lambda_{2,9}$	2.50E-07	$\mu_{7,3}$	4.07E-3
$\lambda_{3,6}$	7.50E-3	$\mu_{8,2}$	4.20E-4
$\lambda_{3,7}$	3.56E-05	$\mu_{9,2}$	2.93E-4
$\lambda_{6,10}$	1.28E-2	$\mu_{11,1}$	1.23E-6
$\lambda_{7,10}$	1.63E-2	$\mu_{12,1}$	1.857E-8
$\lambda_{8,11}$	2.00E-4		
$\lambda_{9,11}$	3.11E-5		
$\lambda_{10,12}$	2.70E-3		
$\lambda_{11,12}$	25.87E-3		

[3] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[4] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[5] R. Kazi and G. Tiwari, "Iot based interactive industrial home wireless system, energy management system and embedded data acquisition system to display on web page using gprs, sms & e-mail alert," in *Energy Systems and Applications, 2015 International Conference on*. IEEE, 2015, pp. 290–295.

[6] I. Ungurean, N.-C. Gaitan, and V. G. Gaitan, "An iot architecture for things from industrial environment," in *Communications (COMM), 2014 10th International Conference on*. IEEE, 2014, pp. 1–4.

[7] D. Hinge and S. Sawarkar, "Mobile to mobile data transfer through human area network," *IJRCCT*, vol. 2, no. 11, pp. 1181–1184, 2013.

[8] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of things security and forensics: Challenges and opportunities," *Future Generation Computer Systems*, vol. 78, pp. 544–546, 2018.

[9] L. Catarinucci *et al.*, "An iot-aware architecture for smart healthcare systems," *IEEE Internet of Things Journal*, vol. 2, no. 6, pp. 515–526, 2015.

[10] J. Yu, K. Ren, and C. Wang, "Enabling cloud storage auditing with verifiable outsourcing of key updates," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 6, pp. 1362–1375, 2016.

[11] K. Gai, M. Qiu, L.-C. Chen, and M. Liu, "Electronic health record error prevention approach using ontology in big data," in *High Performance Computing and Communications (HPCC), 2015 IEEE 7th International Symposium on Cyberspace Safety and Security (CSS), 2015 IEEE 12th International Conferen on Embedded Software and Systems (ICESS), 2015 IEEE 17th International Conference on*. IEEE, 2015, pp. 752–757.

[12] X. Chen, X. Huang, J. Li, J. Ma, W. Lou, and D. S. Wong, "New algorithms for secure outsourcing of large-scale systems of linear equations," *IEEE transactions on information forensics and security*, vol. 10, no. 1, pp. 69–78, 2015.

[13] G. Harsha, "Design and implementation of online patient monitoring system," *International Journal of Advances in Engineering & Technology*, vol. 7, no. 3, p. 1075, 2014.

[14] Q. Dang, "Changes in federal information processing standard (fips) 180-4, secure hash standard," *Cryptologia*, vol. 37, no. 1, pp. 69–73, 2013.

[15] F. PUB, "Secure hash standard (shs)," *FIPS PUB 180*, vol. 4, pp. 1–27, 2012.

[16] S. Salinas, C. Luo, X. Chen, W. Liao, and P. Li, "Efficient secure outsourcing of large-scale sparse linear systems of equations," *IEEE Transactions on Big Data*, vol. 4, no. 1, pp. 26–39, 2018.

[17] L. P. Boppudi and R. Krishnaiah, "Data acquisition and controlling system using cortex m3 core," *International Journal of Innovative Research and Development*, vol. 3, no. 1, pp. 29–33, 2014.

[18] "HashPump - A Tool To Exploit The Hash Length Extension Attack In Various Hashing Algorithms," Sep 2018, [accessed 04. May 2019]. [Online]. Available: https://www.prodefence.org/hashpump

[19] N. Paul, T. Kohno, and D. C. Klonoff, "A review of the security of insulin pump infusion systems," *Journal of diabetes science and technology*, vol. 5, no. 6, pp. 1557–1562, 2011.

[20] A.-M. Rahmani *et al.*, "Smart e-health gateway: Bringing intelligence to internet-of-things based ubiquitous healthcare systems," in *Consumer Communications and Networking Conference (CCNC), 2015 12th Annual IEEE*. IEEE, 2015, pp. 826–834.

[21] P.-Y. S. Hsueh, H. Chang, and S. Ramakrishnan, "Next generation wellness: A technology model for personalizing healthcare," in *Healthcare Information Management Systems*. Springer, 2016, pp. 355–374.

[22] J. Liu, X. Huang, and J. K. Liu, "Secure sharing of personal health records in cloud computing: ciphertext-policy attribute-based signcryption," *Future Generation Computer Systems*, vol. 52, pp. 67–76, 2015.

[23] H. Zhang, J. Yu, C. Tian, P. Zhao, G. Xu, and J. Lin, "Cloud storage for electronic health records based on secret sharing with verifiable reconstruction outsourcing," *IEEE Access*, vol. 6, pp. 40 713–40 722, 2018.

[24] G. J. Joyia, R. M. Liaqat, A. Farooq, and S. Rehman, "Internet of medical things (iomt): applications, benefits and future challenges in healthcare domain," *J Commun*, pp. 240–247, 2017.

[25] D. Macedo, L. A. Guedes, and I. Silva, "A dependability evaluation for internet of things incorporating redundancy aspects," in *Networking, Sensing and Control (ICNSC), 2014 IEEE 11th International Conference on*. IEEE, 2014, pp. 417–422.

[26] S. Anastasiia, K. Vyacheslav, and U. Dmytro, "A markov model of healthcare internet of things system considering failures of components," in *4th International Workshop on Theory of Reliability and Markov Modelling for Information Technologies*. CEUR-WS, 2018, pp. 530–543.

[27] S. C. Williams, "Analysis of the ssh key exchange protocol," in *IMA International Conference on Cryptography and Coding*. Springer, 2011, pp. 356–374.

[28] K. L. Grant and B. D. Tracey, "Infusion pump assembly," Sep. 16 2014, uS Patent 8,834,429.

[29] E. Alkim, P. Jakubeit, and P. Schwabe, "Newhope on arm cortex-m," in *International Conference on Security, Privacy, and Applied Cryptography Engineering*. Springer, 2016, pp. 332–349.

[30] M. U. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A critical analysis on the security concerns of internet of things (iot)," *International Journal of Computer Applications*, vol. 111, no. 7, 2015.

[31] P. A. Kodeswaran, R. Kokku, S. Sen, and M. Srivatsa, "Idea: A system for efficient failure management in smart iot environments," in *Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services*. ACM, 2016, pp. 43–56.

[32] E. Solaiman, R. Ranjan, P. P. Jayaraman, and K. Mitra, "Monitoring internet of things application ecosystems for failure," *IT Professional*, vol. 18, no. 5, pp. 8–11, 2016.

[33] M. Hassanalieragh *et al.*, "Health monitoring and management using internet-of-things (iot) sensing with cloud-based processing: Opportunities and challenges," in *2015 IEEE International Conference on Services Computing*. IEEE, 2015, pp. 285–292.

[34] J. H. Abawajy and M. M. Hassan, "Federated internet of things and cloud computing pervasive patient health monitoring system," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 48–53, 2017.

[35] A. Guenego *et al.*, "Insulin pump failures: has there been an improvement? update of a prospective observational study," *Diabetes technology & therapeutics*, vol. 18, no. 12, pp. 820–824, 2016.

[36] "Sample Medical Record: Monica Latte | Agency for Healthcare Research & Quality," Oct 2018, [accessed 1. Oct. 2018]. [Online]. Available: https://www.ahrq.gov/professionals/prevention-chronic-care/improve/system/pfhandbook/mod8appbmonicalatte.html

[37] "UCI Machine Learning Repository: Diabetes Data Set," Feb 2019, [accessed 3. Feb. 2019]. [Online]. Available: https://archive.ics.uci.edu/ml/datasets/diabetes