International Journal of
Sensor Networks and Data Communications

Shirisha Reddy et al., Int J Sens Netw Data Commun 2019, 8:2
DOI: 10.4172/2090-4886.1000165

Research Article Open Access

E - Health Monitoring Using a Centralized - Decentralized System

Shirisha Reddy K*, Balaraju M, Hetal Shah and Jyothi Agarwal

JNTUH, Hyderabad, Telangana State, India

Abstract

Contemporary development of Wireless Sensor Networks (WSNs) has enabled ubiquitous sensing and actuating for the creation of communication- actuation architecture known as the Internet of Things. The IOT infrastructure has an indispensable role in the E-health care environment and allows connections between different entities such as human beings (patients, medical staff, etc.), medical devices, wireless sensors etc. Cloud computing which provides rapid delivery of IT services in which resources can be retrieved from the Internet with minimal management effort thereby relying on sharing of resources to achieve coherence. Most of the modern and rapidly increasing trends deal with IOT and cloud together. E - Health smart system supports monitoring of a huge number of patients using WSNs and Cloud. Yet this paradigm doesn't provide absolute security to the data transmission. There are several threats to data like denial of service attacks and modification or theft of the data. This might lead to sharing of data or passwords with unauthorized or fallacious recipients and diminution of user privacy. Thus in this paper, we propose an unwavering solution using a centralized - decentralized mechanism for the transmission of sensor data using WSNs, Cloud, Hardware Security Module, Block chain technology, and a central server to the doctor. The paramount idea is the distribution of public and private keys generated using RSA algorithm (embedded in Raspberry Pi) and DES algorithm (applied by the central server on a public key generated using RSA) between four parties providing the clients (doctor) to retrieve data (patient information) securely.

Keywords: E-Healthcare; WSN; RSA; Cloud (Firebase); HSM (AWS Cloud HSM); Block chain technology; Central Server; Centralized; Decentralized

Introduction

Sensor networks are being extensively used in the healthcare environment. Sensor devices can be used to monitor human activities like temperature, heart rate, blood pressure and etc. Applications of wireless sensor networks focused on monitoring the health status of patients have been in demand and various projects are in the development and implementation stages [1]. Due to the direct involvement of human beings the information can be termed as highly sensitive. Low security of a large amount of data due to poor design of sensors is a major drawback. Adversaries with malicious intentions may use private data to harm the person. The author in [2] broadly classifies security into two levels - system security and information security. Security to the information can be provided using cryptography or cryptology in order to avoid the adversaries from reading the data. Cryptography can be categorized into two types - Symmetric cryptography and Asymmetric cryptography. The symmetric cryptography uses single key i.e. a public key for both encryption and decryption whereas asymmetric cryptography uses two keys i.e. a public key for encryption and a private key which is kept secret for decryption. According to [2,3], WSN is facing many challenges such as limited computing power, memory capacity and data transmission capabilities and therefore using cloud computing would be an appropriate solution to improve sensors efficiency. The author of [4] defines cloud computing as pooling computing resources from clusters of servers dynamically assigning virtual resources to applications on demand with virtualization as its foundation. But the data in the cloud faces severe security threats. Firebase [5-9] is a platform that provides users with tools to develop high quality apps, firebase hosting and firebase authentication, real time database and etc. The real time database provides an application data to be synchronized across clients and stored on firebase's cloud. Contemporary cloud servers like Microsoft Azure, Amazon Web services etc. provide Hardware Security Module (HSM) services, which is a physical computing device that safeguards and manages digital keys for strong authentication and provides crypto processing. They are generally found in the form of a plug - in card or external device that is directly attached to a network server. AWS Cloud HSM [8] provides isolation to the module by creating dedicated Virtual Private Network and enables easy generation and usage of desired encryption keys on the AWS cloud. Keys can be managed using FIPS 140-2 Level 3 validated HSMs. It enables control of encryption keys using a secure channel to create users and set HSM policies. AWS manages the HSM appliance but it does not have access to the data stored in it i.e., keys and also provides role-based access to the HSM. In this way, it proves to be secure key storage. A block chain or initially known as block chain is a growing list of records, called blocks which are linked using highly secure cryptographic algorithms. Each block consists of a cryptographic hash of previous block, a timestamp and the transaction data. It is a network of computing nodes and is managed by this peer to peer network collectively cohered with protocol to validate the new blocks. The recorded data cannot be altered or tampered without alteration of all the subsequent blocks which requires unanimity of majority of network. It is a distributed ledger that verifies and stores transactions occurring in peer - to - peer network. Ethereum is widely used block chain that supports a Turing - complete scripting language like solidity for semiautonomous programs running on block chain known as smart contracts. Remix is a powerful, open source tool that helps in writing the solidity contracts straight from the browser. Healthcare sector is one of the largest sectors in the world. This sector comprises of humongous amount of data, which requires extortionate security. But the current system and design reins in providing effective security to the health care data. As a consequence, the sensitive data is either lost or modified or sharing of passwords to malicious adversaries

***Corresponding author:** Shirisha Reddy K, Research Scholar, JNTUH, Hyderabad, Telangana State, India, Tel: +91 9550042010; E-mail: shirishakasireddy20@gmail.com

Received March 02, 2019; **Accepted** May 16, 2019; **Published** May 24, 2019

Citation: Shirisha Reddy K, Balaraju M, Shah H, Agarwal J (2019) E - Health Monitoring Using a Centralized - Decentralized System. Int J Sens Netw Data Commun 8: 165. doi: 10.4172/2090-4886.1000165

might take place. Every hospital either has its own server or uses a third party server and the breach of security might be caused in both. Therefore, we propose a solution to provide the medical information absolute security. In this paper, we propose a solution to provide the security to the medical information using a Centralized - Decentralized mechanism. The prime scheme is to distribute the keys generated using randomized algorithms between four parties. Initially, the medical information is collected from the sensors and passed to a series of single board computer i.e. Raspberry pi 2 [5,6], which has the RSA algorithm embedded in it. The information is encrypted using the RSA algorithm and a cipher file along with public and private keys are generated. The cipher text file and the public key are stored onto the firebase (cloud) [9] using a secure channel and the private key is stored onto the HSM (AWS Cloud HSM), thus making the system centralized. To perform the computational activities and to store the relational data we establish a third party server known as Central Server. The key aim of the central server is to keep the frequently accessed data intact for a fraction of time. The cipher file is then downloaded from the cloud (firebase) and a symmetric key is generated by employing the DES algorithm onto the cipher file. The Data Encryption Standard is a symmetric - key algorithm used for encryption of data. The public key generated is short in length i.e. 56 bits. This key is then deployed onto the blockchain [7] to ensure absolute security to the medical data.

To the end, the rest of the paper is organized as follows. The work motivation is mentioned in section 2.0; the section 3.0 illustrates related works. The section 4.0 covers proposed solution and section 5.0 illustrates stimulation and implementation results. Section 6.0 demonstrates the existing and proposed solution.

Related Work

Mohammed S. Jassas and Abdullah A. Qasem [1] extend a novel solution aiming to prevent delays in arrival of patient's data to medical healthcare providers specifically during emergency situations. The architecture is based on medical sensors which are used to measure the physical parameters using WSNs. The transfer of data from the sensors to the healthcare providers (doctors) take place over cloud environment. It also circumvents the users to manually enter the medical data and helps in increasing the bed capacity to overcome the emergency situations particularly during public gatherings thereby increasing the quality of E - health services. However, this system does not take provide absolute security to the medical data. The authors in [10-13] centralize the data integrity in information security. They propose a various integrity verification methods for digital verses of the Holy Quran. The advanced algorithms like SHA256 and RIPEMD160 are used to generate the hash function and store it in the hash table.

Khandakar Entenam Unayes Ahmed, Mark A Gregory extended a solution to integrate the cloud computing model with WSN where the users request will be served through three service layers (Iaas, Paas, Saas) either from the archive which is made by collecting data periodically from WSN to Data Centres. The authors in [14] propose a scheme to provide security to the original data by slicing it into different slices and applying various encryption algorithms and store it into the cloud storage [12]. proposed an efficient approach to utilize the aggregation of data in WSN and assure end to end encryption of data between sink and leaves. It also aimed to minimize the bit transfer between the sensor nodes and to find an encryption algorithm which is simple to implement and would help in increasing the life of batteries. The authors in [13] propose a solution to automate the manual collection of patient's data which is error prone and slow by using sensors attached to the medical equipment that are connected to each other forming a wireless sensor network. The information is then made available on the cloud which can be accessed by the healthcare providers to process and analyse the patient's data. This solution helps in making real - time data collecting and eliminating manual collection work and errors [15]. Proposed a solution in which AES, blowfish, RC6 and BRA algorithms are employed to provide block wise security to the data on the cloud. Each and every block in the file is encrypted using different algorithms simultaneously using multithreading technique. The key size is 128 bits which is inserted into cover image using LSB technique. In [16], the authors propounded cloud based architecture for medical wireless sensor networks to manage huge amount of sensitive medical data and to provide useful and real information about the patient's health to the medical health providers and to improve the rescue process of patient during emergency. This mechanism is dependent on the Cipher text Policy Attribute - based Encryption (CP - ABE) to provide effective and flexible security mechanism guaranteeing confidentiality and integrity of the data. In [17], the authors proposed architecture of collecting and managing the huge amount of data generated by the medical sensor networks. This solution addresses the problem of lack of data management. Furthermore, effective and flexible security mechanism is proposed. This architecture is composed of three common architectures that are Body Area Networks (BAN), gateways and remote monitoring system. The authors in [18] propounded an efficient centralized secure architecture for end to end integration of IoT based healthcare system deployed in cloud environment. It uses Fog computing environment to run the framework. The authors mainly focused to secure authorization and authentication of all the devices, identifying and tracking the devices deployed in the system. Communication among the devices and data transfer between the remote healthcare systems is established using asynchronous mode of transfer. In [19], the authors proposed a feasible solution which benefits from the concept of Fog computing. They show effectiveness of fog computing in IoT based healthcare systems in terms of bandwidth utilization, QoS assurance and emergency notification. They particularly chose Electrocardiogram (ECG) feature extraction as the case study as it plays a major role in diagnosing cardiac diseases. These signals are analysed in the smart gateways with heart rates, P wave and T wave extracted via flexible template based on lightweight wavelet transform mechanism. The authors in [20] propounded a comprehensive survey on IoT and blockchain Integration with an objective to analyse current research trends on the usage of blockchain and IoT context.

Proposed Solution

The architecture of the proposed solution as shown in Figure 1 is mainly based on the integration of WSNs and cloud and blockchain along with the distribution of the keys generated using RSA algorithm (embedded in Raspberry Pi) and DES algorithm (applied at the central server to the cipher file). We propose a two-channel key distribution protocol where the keys are distributed among four parties i.e. the cloud, HSM vault, central server, and block chain.

Initially, the sensors detect the medical information such as temperature, blood pressure etc. and the pi applies RSA algorithm [5] embedded in it. The algorithm operates on the fact that factor of large composite numbers is difficult. The patient's physical parameters (heartbeat, blood pressure etc.) are detected using sensors and transferred to the pi. RSA algorithm is applied onto the data file and public key, private key and cipherfile are generated which is latter stored onto the cloud database. Rivest - Shamir - Adleman (RSA) algorithm is widely used for providing security to the data. It generates one public key which is used for encryption and a private key which is kept secret

for decryption of the cipher text. It provides confidentiality, integrity, authenticity and non – repudiation of electronic communication and data. The algorithm is as shown below Figure 2.

We use this service in the proposed solution to ensure unmitigated security to the private key generated using RSA algorithm (Embedded in the pi). As shown in Figure 3, the tiny computer (Raspberry Pi) has the encryption algorithm embedded in it. On applying the RSA encryption:

i. A public key is generated which is stored in cloud (Firebase) along with the cipher file and sensor id.

ii. A private key is generated which is stored in Cloud HSM (AWS) along with Pi id Figure 4.

Initially, a cluster is created and a Virtual Private Cloud (VPC) is specified along with one or more subnets. The cluster is given role based access i.e. administrator and user. An EC2 instance is created and launched on that VPC and a HSM is created. The HSM runs in the VPC created and enables to use HSM with applications running on EC2 instance. Standard VPC protocols cab be used to manage the security controls to access the HSM. The applications are connected to the HSM using mutually authenticated SSL channels established by the HSM client software. Once the cluster is initialized and activated, the private keys are stored in it. The central server's role is to perform

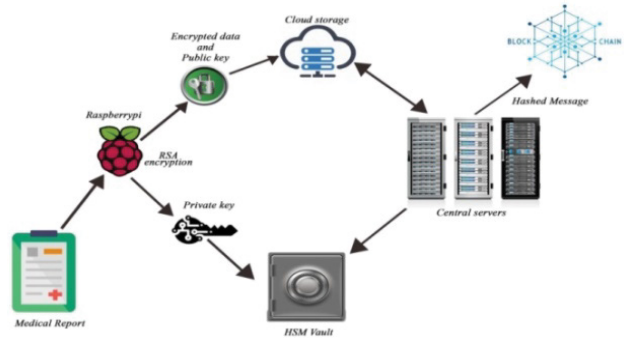

Figure 1: Architecture of Proposed Solution.

Step 1: Key Generation

Generate two large prime numbers, p and q.

Let n = p.q

$\varphi(n) = (p-1)(q-1)$

Choose e (co prime to $\varphi(n)$) such that $\gcd(e, \varphi(n))=1$

Find d, such that

$e.d \bmod \varphi(n) = 1$

Key:

Public key = (e,n)

Private key = (d,n)

Figure 2: Rivest - Shamir - Adleman (RSA) algorithm.

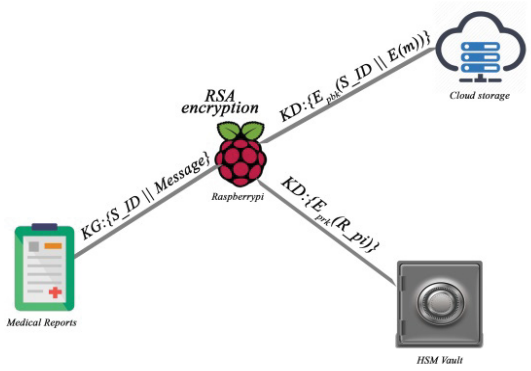

Figure 3: Distribution of public and private keys obtained on applying RSA algorithm.

Key distribution in proposed solution

During Encryption:

1. Sensor reads the information and passes it to Raspberry pi and RSA encryption algorithm is applied to it.

   Sensor → *KG: RSA(SID || E(M))*

2. Once RSA algorithm is applied, private and public keys are generated.

   Pi → $KD: E_{pbk}(SID \,||\, E(M)))$ *[Stored in cloud.]*
   Pi → $KD: E_{pvk} \,||\, Pid$ *[Stored in HSM.]*

3. Once the encrypted file and public key is stored on cloud, Central server accesses the public key and applies RC4 encryption.

   Cloud → Central server: KG: E_{DES} (E_{pbk}(SID || E (M)))

4. Central server then stores the symmetric key generated along with the file ID on a block and deploys it on blockchain.

   Central server $\xrightarrow{\text{Blockchain}}$ SKG || FID

Figure 4: Key distribution in proposed solution.

the computational activities. It stores the frequently accessed data. For example, if the doctor requests for a document stored in central server for a particular amount of time, the computational activities will not be necessary to repeatedly performed. The server accesses the cipher file from the cloud and applies the Data Encryption Standard (DES) algorithm generating a symmetric key Figure 5.

The cipher file is also stored onto the central server's database along with the file id. The symmetric key obtained on applying DES algorithm on the cipher file is then deployed onto the block chain along with the file id as shown in Figure 6. There are three types of transactions in ethereum: financial, message calls and contract creation. We use the Ropsten test network [7] to deploy are smart contact (programmed using solidity) and by setting up the gas limit value. In this way, the

Data Encryption Standard Algorithm:

function DES(M,K) where M=(L,R)
M=IP (M)
for round=1 to 16 do
Ki=SK (K, round)
L=L xor F (R, Ki)
Swap (L,R)
End
Swap (L, R)
M=IP-1(M)
Return M
End

Figure 5: Algorithm for DES encryption technique.

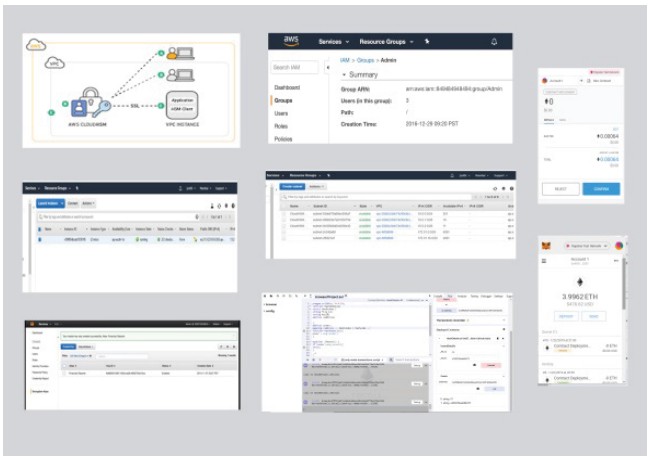

Figure 6: HSM and Block chain.

During decryption process:

1. After authentication, the doctor can access the file id and the hashed symmetric key and provides it to the central server.

$$Doctor \xrightarrow{Checks\ on\ FID} Blockchain$$
$$Blockchain^{SKG} \longrightarrow Central\ Server$$

2. The decryption process is performed at central server where the public key is obtained by applying DES decryption.

$$\text{Central server: } E_{DES}\,(\,E_{pbk}(SID) \,||\, E(M)) \xrightarrow[Decryption]{} E_{pbk}(SID) \,||\, E(M))$$

3. Using the public key and private key are accessed using SID and PID and the reverse RSA process is performed.

$$E_{pbk}^{SID} \longrightarrow \text{Firebase (Public key)}$$
$$E_{pvk}^{PID} \longrightarrow \text{Vault (Private key)}$$

Figure 7: Decryption process.

Sensor	Sensor ID (SID)	Date	Sensor Data
TEMP	01	1st January, 2019	37
TEMP	02	1st January, 2019	31
TEMP	03	1st January, 2019	26
TEMP	02	2nd January, 2019	29
TEMP	01	2nd January, 2019	24

Table 1: Showing the various temperatures recorded at different time.

S.No.	Message	Cipher text(RSA)	Public key	Private key
1.	37	46	91	29
2.	31	58	901	555
3.	26	146	415	219
4.	29	486	2173	1837
5.	24	9	201	53

Note: While transferring the data, the public key will be transferred along with the sensor id, the private key with the Pi id and the cipher text will be transferred with the patient id.

Table 2: Showing the public and private keys generated on applying RSA.

S.No.	Cipher text (RSA)	Cipher text (DES)	Symmetric key
1.	46	ec54fd8f5e76c8a1	e329232ea6d0d73
2.	58	f1c36709ae4e6b915	e329232ea6d0d73
3.	146	6cc81b23279d240	e329232ea6d0d73
4.	486	3c473a92147d644	e329232ea6d0d73
5.	9	52cc44e58d1f27d0	e329232ea6d0d73

Table 3: Showing the generation of symmetric key using DES algorithm.

medical information is provided complete security making the data immutable and accessible at any point of time. Trust in the execution of the code emerges from the trust in the integrity of block chain. Thus the access to the data is achieved using a centralized and decentralized mechanism Figure 7.

We have tested our prototype using body temperature sensor considering the cost constraints of the experiment. We have collected hypothetical patient's data for the test sample and we have observed the various patients body temperatures in the terms of degree Celsius. As shown in the Table 1, we have various temperatures recorded using various sensors.

The result of applying RSA algorithm to the data collected from the pi is as shown in the Table 2.

The results of DES algorithm applied on the cipher text obtained from RSA algorithm is as shown the Table 3.

Existing Verses Proposed Solution

Scenario 1: In our proposed solution, we establish a centralized - decentralized mechanism to ensure complete security and integrity while transferring the data. An unmitigated distribution of keys helps to restrict unauthorized access to the data and allows secure data transfer at any moment of time. The load on the cloud server is balanced with the introduction of central server and block chain.

Scenario 2: The establishment of the cloud server helped in transfer and access of the data at any moment of time but there is uncertainty of good security to the data. But cloud suffers from data breaches and severe attacks which can't be avoided. Additionally upon multiple requests at a time might not be balanced by the cloud server, delaying

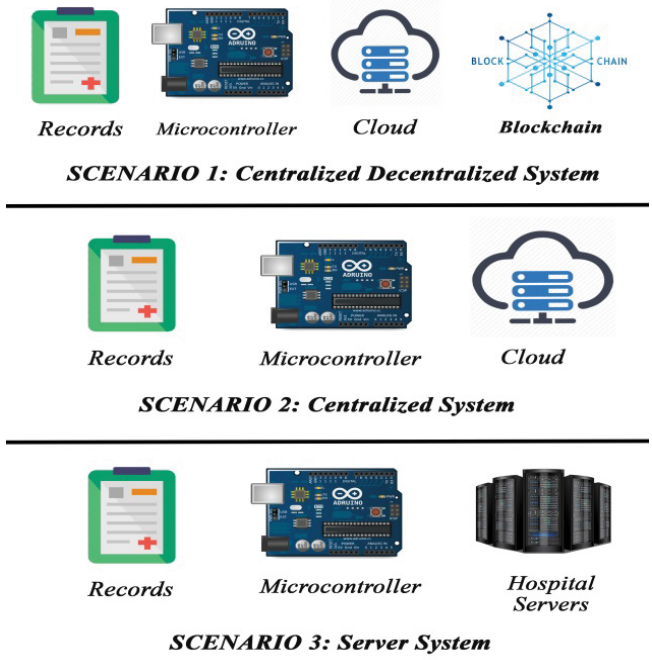

Figure 8: Various scenarios of the healthcare environment.

the access to the data during emergency. Sometimes, complete crash of the cloud might lead to data loses.

Scenario 3: Initially, the hospital data was stored in its own server which made the portability of the data manual. The data was prone to severe attacks and data breaches and loses would occur Figure 8 [21-24].

Conclusion

The integration of wireless sensor networks and cloud along with block chain technology will help in developing a new-fangled generation of technology in various aspects of health monitoring. The proposed system provides integrity and complete security to the medical data following a centralized - decentralized mechanism. During the times of heavy traffic at the server, the load is balanced by introducing block chain technology which is distributed, hence providing indistinguishable availability of information every time and at one's convenience. The double encryption performed on the medical information and the distribution of the keys generated provides high security to the data. Considering the fact of involvement of high monetary values with large data during block chain transactions, we deploy only small string on the block chain making the cost minimal.

In the future work, we will enhance the performance of the algorithm by using some meta-heuristic and hybrid algorithm. We are planning to enhance the security of the system using various cryptographic algorithms which provide higher security and to provide greater data integrity using hashing algorithms. The functionality of the system will be escalated by adding more sensors and collecting larger patient data.

Acknowledgement

The author would thank to higher authorities of JNTUH to use the research laboratories. The author would thank for the facilities provided by FIST for research in VBIT.

References

1. Jassas MS, Qasem AA, Mahmoud QH (2015) A smart system connecting e-health sensors and the cloud. Canadian Conference on Electrical and Computer Engineering 28: 712-713.
2. Ameen MA, Liu J, Kwak KS (2012) Security and privacy issues in wireless sensor networks for healthcare applications. J Med Syst 36: 93-101.
3. Ahmed KEU, Gregory MA (2011) Integration of wireless sensor networks with cloud computing. Seventh International Conference on Mobile Ad-hoc and sensor networks.
4. Zhang Q, Cheng L, Boutaba R (2010) Cloud computing: state-of-the art and research challenges. J Inte Servic Applic 1: 8-12.
5. Soheila Omer AL, Koko FM, Babikar A (2015) Comparison of various encryption algorithms and techniques for improving secured data communication. J Comp Eng 17: 65-66.
6. www.raspberrypi.org
7. www.metamask.io
8. www.aws.amazon.com/cloudhsm
9. https://firebase.google.com/
10. Almazrooie M, Samsudin A, Gutub AA, Salleh MS, Omar MA, et al. (2018) Integrity verification of digital holy quran verses using cryptographic hashing function and compression. Journal of King Saud University-Computer and Information Sciences. Pp: 6-9.
11. Artur ROT (2018) Data and services security issues and challenges in cloud computing environments. The 22nd World Multi - Conference on Systemics, Cybernetics and Informatics. Pp: 101-104.
12. Sharifnia S (2018) Encryption Data in Wireless Sensor Network. Int J Comp Sci Cloud Comp 7: 43-45.
13. Rolin CO, Koch FL, Becker C, Werner J, Fracalossi A, et al. (2017) A cloud computing solution for patient's data collection in health care institutions. IEEE Conference Publication Pp: 1-5.
14. Bobde RR, Khaparde A, Raghuwanshi MM (2015) An approach for securing data on cloud using data slicing and cryptography. IEEE 9th International Conference on Intelligent Systems and Control (ISCO).
15. Maitri PV, Verma A (2016) Secure file storage in cloud computing using hybrid cryptography algorithm. International Conference on Wireless Communications, Signal Processing and Networking.
16. Lounis A, Hadjidj AK, Bouabdallah A, Challal Y (2015) Healing on the cloud: secure cloud architecture for medical wireless sensor networks.
17. Lounis A, Hadjidj A, Bouabdallah A, Challal Y (2012) Secure and scalable cloud - based architecture for e - health wireless sensor networks. 21st International Conference on Computer Communications and Networks (ICCCN). Pp: 1-4.
18. Thota C, Sundarasekar R, Manogaran G, Varatharajan R, Priyan MK (2018) Centralized fog computing security platform for iot and cloud in healthcare system. Fog computing: break throughs in research and practice. p: 14.
19. Gia TN, Jiang M, Rahmani AM, Westerland T, Liljeberg P, et al. (2015) Fog computing in healthcare internet - of - things: a case study on ecg feature extraction. IEEE conference on computer and information technology, Pp: 356-360.
20. Panarello A, Tapas N, Merlino G, Longo F, Puliafito A (2018) Block chain and IoT integration: a systematic survey. Sensors 18: 3-15.
21. Garg H (2019) A hybrid GSA-GA algorithm for constrained optimization problems, Inform Sci 478: 499-523.
22. Patwal R, Narang N, Garg H (2018) A novel TVAC-PSO based mutation strategies algorithm for generation scheduling of pumped storage hydrothermal system incorporating solar units. Energy 142: 822-837.
23. Garg H (2016) A hybrid PSO-GA algorithm for constrained optimization problems, Appl Math Comput 274: 292-305.
24. Garg H (2015) A hybrid GA-GSA algorithm for optimizing the performance of an industrial system by utilizing uncertain data. Handbook of Research on Artificial Intelligence Techniques and Algorithms, IGI Global, Pp: 620-654.