Secure Data Transfer for a Telemedicine System

Ashwini C*[1], Dr Arbind Kumar Gupta[2], Dr Venkatesan S[2], Numan Shaikh[1]

[1]*M.Tech, Computer Network and Engineering, Department of CSE, Dayananda Sagar College of Engg, Bangalore*

[2] *Professor, Department of CSE, Dayananda Sagar College of Engg, Bangalore*

ABSTRACT*-Ever* Since Telemedicine System has been put into effect, storage and transmitting the patients' health care information is an important issue. The view of storing and transmitting health care information from storage node/client to sink/server raises concerns about Health Care Information Security. This paperfocuses on preserving the Privacy of sensed healthcare Data, Integrity of healthcare data, avoiding impersonation, Prevention against Eavesdropping and Data Corruption. This paper, proposes the Json web Token authentication scheme, Advance Encryption Standard and Secure Hash Algorithm validation that protects the privacy of healthcaredata and the integrity of healthcare data. To preserve integrity of healthcare data and to avoid the storage node compromise with additional security while transferring data, we propose a data partition algorithm that partitions each data item into n number of files at the client side and merges all the n files at the server side to acquire the actual file containing the health care data.

KEYWORDS: *Telemedicine, Data security, Partioning.*

I. INTRODUCTION

People in rural areas cannot afford to go to hospitals in bigger cities, nor do doctors want to work in rural areas. But we can bring them close to each other by use of technology enabling a patient to have one-to-one talk to a doctor.Telemedicine is the use of information technology and telecommunication for the remote delivery of healthcare services, such as healthcare appraisal (accessing) or consultations ,over the telecommunications system which is put into action. It allows healthcare caregivers to consult and provide diagnosis of a patient's problem without the need for a patient to be present physically. Such solutions have already been developed and are in use in rural areas in a limited way. It has also been used to overcome distance barriers and to improve access to medical services that would often not be always available in distant and rural areas. It reduces the travelling time and also eliminates the distance barriers making the telemedicine system efficient. It is also used to save lives inemergency situations at rural places where there is no proper health care facilities. Although there are many implementations of telemedicine systems, they still have many limitation that inhibits its wide spread usage. Limitations can be listed as High cost of implementing telemedicine system, less human interaction which leads to error in providing clinical services, Level of trust is low between the patient and the healthcare service provider. Lack of privacy for health care data when it is transferred, Low internet speed which may lead to delayed telemedicine connectivity. Unauthorised people trying to send or access the health care data. Special training must be given to use the telemedicine system or to be flexible with User Interface of telemedicine system. We are working to propose a telemedicine system in order to overcome these challenges.

These telemedicine systems provide the communications between patient at rural areas and medical staff at urban hospitals with both ease and homage, as well as transmitting the health care information from client to server. The Overall objective of the telemedicine system should be: Collecting vital parameters of a patient that can be used for more informed diagnostic / therapeutic decisions. Monitoring and treatment of a patient by local care giver at rural areas. Transferring healthcare data over internet for consultation with specialists to take diagnostic / therapeutic decision at urban cities. One of the major concern of telemedicine system we are addressing in this paper, in our telemedicine solution that is securely transferring the health care data from client system to server system such that the health care data is not vulnerable to attacks in any form. The basic requirement of implementing secure telemedicine system are:

Problem statement

The problem to be addressed are:

- Privacy and integrity in two-tiered sensor networks that is the health care data must be transferred with proper privacy and integrity between the storage node and the sink.
- Protection against storage node compromise, where the health care data is stored must not be compromised.
- Protection against eavesdropping, data corruption, and telemedicine system must be secure enough to avoid eaves dropping and data corruption by third party/attackers.
- Telemedicine system must allow the sink /server to detect misbehaviour of storage nodes/client system and to detect whether the healthcare data is invalid.
- Avoiding Impersonation that is the telemedicine system must be capable of finding whether the healthcare data sent by client is from a valid and authorised user or not.
- The user interface must be simple that provides ease of use to care givers in rural area, thereby enabling wider acceptability.
- Verification of authenticity of users.

II RELATED WORK

[1]A survey has been made by the authors ofTelemedicine Security: A Systematic Review has started a systematic review, by analysing 58 journal ,which is related to understand the methodologies used, Among all the journals around 76% if the journals just define the security issues and 47% researched about security issues ,While 61% found a solution to these security issues. Authors summarize that the previous research and methodology related to security are insufficient and they used the outdated security techniques in their solutions.

[2] Lambras , Makois, Nikolas authors of the paper, focused on confidentiality and integrity of health care data in telemedicine system, here end to end encryption scheme is used to prevent the data channel from any kind of modification and unauthorized access session key are exchanged using the public key cryptography. To ensure whether the message is complete and accurate there exist a protocol i.e. set of procedure. The messages carry user's id and password stored in identifiers, which is transmitted during communication in the communication channel. This paper address end to end encryption along with key management and distribution procedure for encryption.

[3]In the paper author is aiming to provide secure health care data delivery to rural/remote areas, using latency in tolerant network. Author also proposes a secure telemedicine system using a open network to exchange the health care data AES encryption is used to encrypt the date, But disadvantage lies in integrity and authenticity of data.

[4]AymanM author of the paper describes about the patients' healthcare centre, caregivers and patients. To improvise the quality of healthcare whenever it is required, Caregiver must access the healthcare data from anywhere when they require it. In this paper author presents interactive telemedicine solution (ITS) to implement automatic healthcare data transfer within a patient healthcare centre via voice over internet protocol, Wi-Fi, mobile phones.

[5]Preserving the privacy and integrity is one of the major challenge in telemedicine application, where the patients' health information and the patient's personal information is gathered and transferred over the telemedicine system. Author also discuss about the telemedicine network features and the security problems in the EPON which is responsible for conveying, traffic between the patient health care centres and patients. Accordingly, there are different types of security limitations which are classified and summary is presented. The main aim of this paper is to highlight security issues in telemedicine system and possible attacks during data transmission.

[6]In System for secure data exchange in telemedicine authors implements a system for secure data transfer in telemedicine system using public key cryptography/Asymmetric cryptography that is it uses two different keys public key and private key, public key given to everyone and private key known and given only to the owner, author has used RSA algorithm to encrypt the data before transmitting it to the remote server. The Limitations of the proposed system in this paper are: RSA Algorithm can be slow down in when there is large data to be encrypted. It requires third party to verify the reliability of public key. It can be tampered by a middleman who can compromise with the public key system. Attacks such as Searching message space and guessing d can be done on the proposed system.

III. EXISTING SYSTEM

Let us consider a two-tiered sensor network consisting of sensors and storage nodes. In context with telemedicine system the sensors are the Pulse rate sensors, ECG Sensors, Temperature sensors etc. and the storage node refers to the client system at primary health care system situated at rural areas. In this structure, sensors send their healthcare data to storage nodes and the sink issues requests only to storage nodes and receive the response from them, here the sink refers to the Remote server situated at urban areas where hospitals are situated, or it can be in cloud. The main concern about storage node is that it can be an easy target for attackers to attack due to their important role in telemedicine network. A compromised storage node may leak the data stored there to the attacker breaching the data privacy, integrity, and causes data corruption, impersonation and eavesdropping.Also, if the storage node is compromised then it may send wrong information as the response to a request sent by storage node breaking the data integrity.

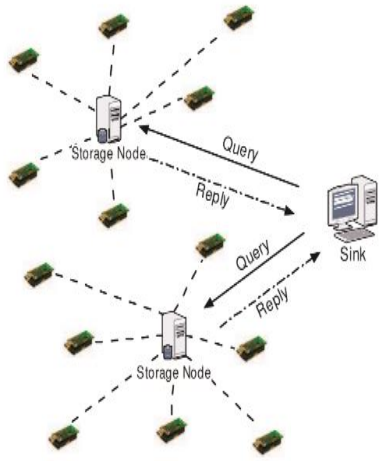

Figure 1: Existing System

Limitations of Existing System: Since the storage node plays an important role of storing collecting and transmitting health care data if the storage node is compromised it maylead to low level of trust between the patient and the healthcare service provider. Breach of privacy for health care data when it is transferred from patients at rural areas to the doctors at urban areas, will lead to patient confidentially being compromised. Unauthorised people trying to send or access the health care data will impact integrity of the system. Since the storage node is deployed in field with little or no physical or IT security, it becomes important to design the data security

of the system to protect it from such loss of integrity and breach of privacy.

IV PROPOSED METHODOLOGY

The telemedicine system has the following design requirement, as given in the figure 2**.**

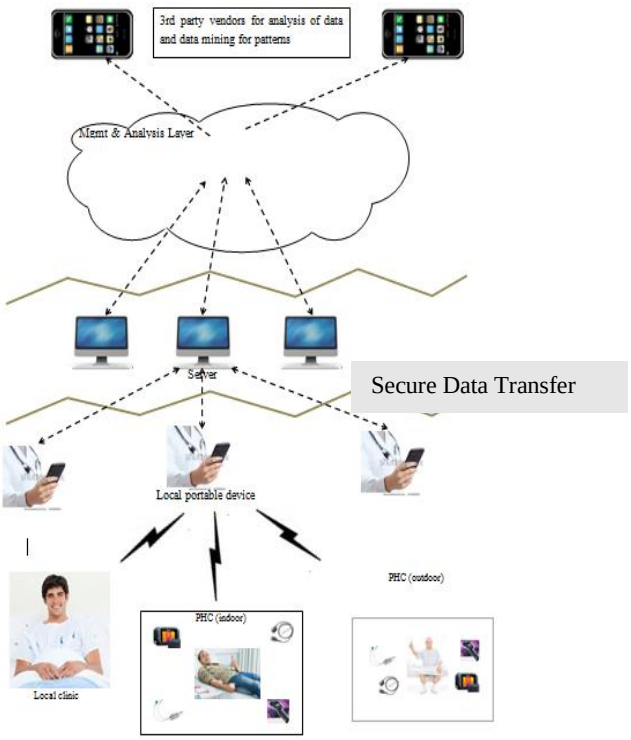

Figure 2:Design requirement of the system

- The network deployment on the Client side consist of 4 sensors placed in an 30x30 feet Room ,Each sensor is connected to local hand held device/Laptop via Aurdino board using Wi-Fi module to read the sensor value from ECG sensor ,Pulse rate sensor ,Temperature sensor respectively.
- In the system all the sensors must be connected to a local hand held device/Laptop using a Wi-Fi module (Wireless).
- The network deployment on the Server side is a server, currently for prototype we are using a Personal Computer/Laptop as server.
- More than one sensor can be connected to a local hand held device/Laptop at a time.
- Each sensor connected to the local hand held device sends the received reading to the server in a .txt file format.
- The local hand held device/laptop before receiving the file verifies the sender of file using jwt token authentication.
- The Client and Server Uses File Transfer Protocol.
- The file to be transferred will be encrypted by AES encryption and SHA algorithm for integrity and file will be sent to the server with time stamp and data partition information attached to it.
- The system should be capable of detection of storage node compromise.
- On the server side the file will be decrypted and validated with SHA and verification of its jwt token will be done along with the data merging.
- The system should be capable of securely communicating between the storage node and sink/server.

In the above system, designing for secure data transfer requires the following-

- Establishing connectivity and transfer of data from laptop/LHD to a remote computer using internet.
- Data encryption for information security.
- Data Validation for information integrity.
- Authentication for privacy.
- Data Partioning for additional security.
- Transfer of data to remote server / consulting doctor for long term storage / retrieval and use of data.

Our goal is to design scheme where the sensors will collect the patients' health care data such as ECG (Electro cardio graph), Pulse rate, Heartbeat, Temperature using the aurdino and sensors and it transfer the collected patients detail to the storage node/client via Wi-Fi module .Once the Storage node/client receives the patient data it has to securely transfer it to the server located at the hospital (urban location). The security of patient's data is ensured by preserving the Privacy of Sensed Data, Integrity of data, avoiding Impersonation, Prevention against Eaves Dropping and Data Corruption. The Json web Token authentication scheme, Advance Encryption Standard and Secure Hash Algorithm Validation are used to protect the privacy of sensor data. To enhance data integrity, we propose a data partition algorithm that partition each data item into n number of files at the client side and merges all the n files at the server side to acquire the actual file containing the health care data.

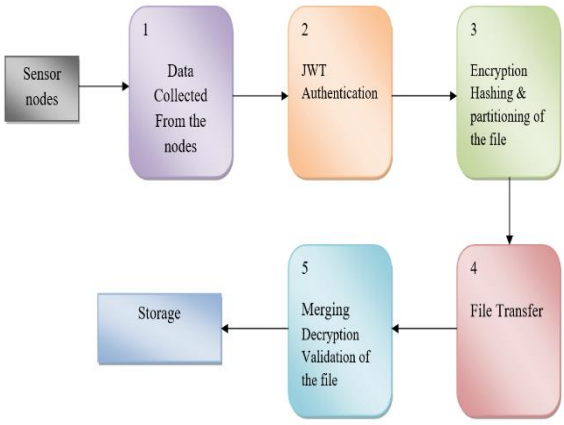

Figure 3: Architecture for a Secure Telemedicine system.

The Fig 2 shows the Architecture for a secure telemedicine system, it contains six top level models. The proposed framework signifies the implementation of secure file transfer in a telemedicine system.

A. Data Collected from the sensor nodes

Figure 3: Data Collected from the sensor nodes

In the Data Collection Phase the Client/patient is connected to different sensors as shown in the figure 3

The sensed data are collected and sent to the storage node in a .txt file format.

B. JWT Token Authentication

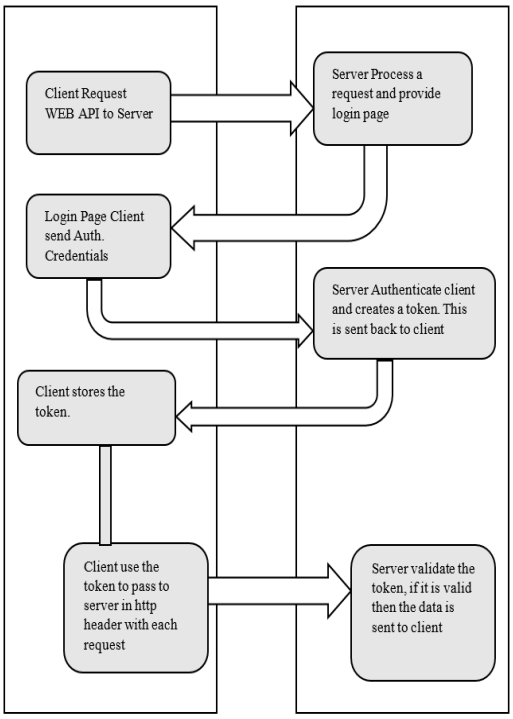

Figure 4: JWT Token Authentication.

- In the jwt Authentication Phase as shown in the figure 4 the client application sends a request to the server application.
- Server processes the request from the client and provides a login page.
- Client application provides the valid authentication Credentials that is the Registered Care Givers Login Id and Password.
- Server Authenticates client and creates a JWT token.
- The format of jwt token is as followsheader, payload and signature.
- Header: The header component of the JWT contains information about how the JWT signature should be computed.
- Payload: The payload component of the JWT is the data that's stored inside the JWT (this data is also referred to as the "claims" of the JWT).
- Signature: The signature is computed by encoding the header and the payload created in the first 2 steps.
- Then the algorithm will join the resulting encoded strings together with a period (.) in between them. In our algorithm, this joined string is assigned to data.To get the JWT signature, the obtained data string is hashed with a randomly generated secret key using the hashing algorithm specified in the JWT header.Client stores the token.
- Client uses the token to pass to the server in http header with each request.
- Server validates the token if it is valid then the data is received from the client or sent to the client.

C. Encryption and partitioning of file

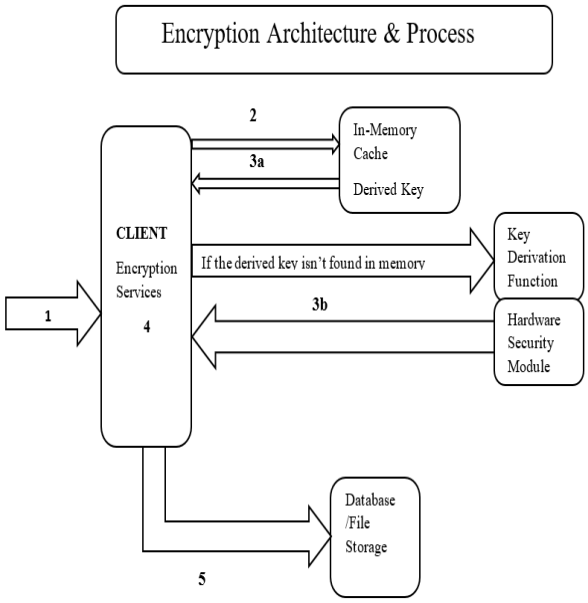

Figure 5: Design of Encryption Model.

In this module the data is sent from the sensor node to the local hand held device or laptop where the following process takes place. (modify / delete)

The main functions of this module are:

1. Send the data from the sensor node to local hand held device or laptop.

2. On reception of the data encryption process is initiated. The key for encryption is derived from in memory cache and is sent to the encryption service.

3. If the derived key isn't found in memory the key derivation function (or) from a hardware security module key is obtained and sent to the encryption service.

4. In the encryption service the file or data is encrypted using the key and stored in the Database for further data transfer.

D. Data Partitioning

In this module the data file is partitioned into distinct files and the partitioning information contains the number of files it should be divided into. Data Partitioning is divided into two phases

Partitioning Phase

In our partition algorithm the first Phase is as follows. Suppose the file to be partitioned consists of S = {d1,d2,⋯,dn} where d1,d2,dn….. Is the data to be stored in the file partitioned respectively. The partitioned file will be partioned and stored as a .temporary file they are generally deleted after their purpose is completed.

After the partioning phase the data is securely transferred to the server system.

Merging Phase

In the merging phase, the temporary files will be merged based on the name given to the files partioned.Once the partioned files are merged data can be obtained in a single file. And the file reception successful message is sent to the storage node.

V. RESULTS AND ANALYSIS

First the patient is connected to the different sensors such as Temperature Sensor (DS18B20), ECG Module (AD8232), EMGModule (ZX-SEMG), PulseSensor (HBT-O) respectively then the sensors collects the data, while the program for each sensors are stored in the buffer and while the code is running the data is collected. We use Raspberry pi Micro-Controller connected to sensor and the data transfer is done by the Wi-Fi module to storage node. Care giver is given a unique user-id and password through which he can login and send the sensed data to the server/sink. The below figure 6 represents the collected health care data.After the login successful phase, when the care giver provides valid login credentials, caregiver gets logged in and a Java Web Token (JWT) will be generated which is further used to transfer file.

Figure 6: Patient Health Care Data.

Figure 7 shows the file upload, on successful login a JWT token is generated by the server this token in turn goes and gets store in the header of client the ,caregiver browses file from its directory and uploads the file that he wants to send once the file is uploaded the file can be sent.

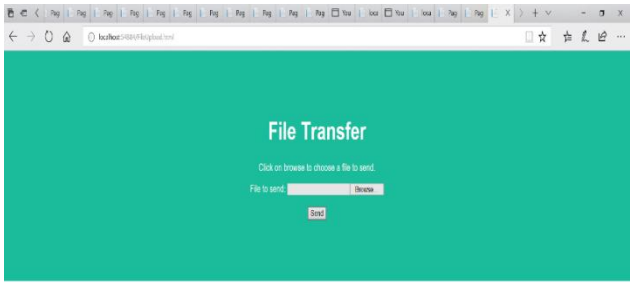

Figure 7: File Upload.

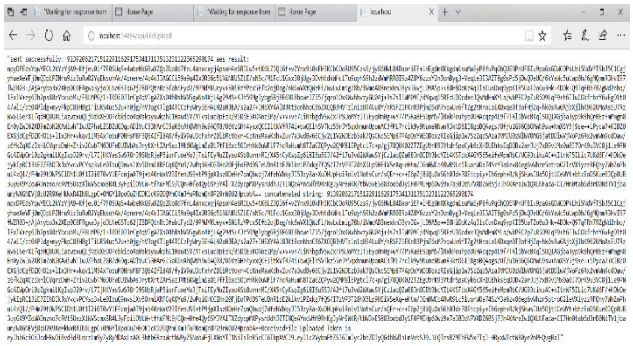

Figure 8: File Encryption and Hash.

The above figure 8 shows file encryption and Hashing, the encryption of the file takes place using Advanced Encryption Standard (AES) and Hashing of plain text is done using SHA1.

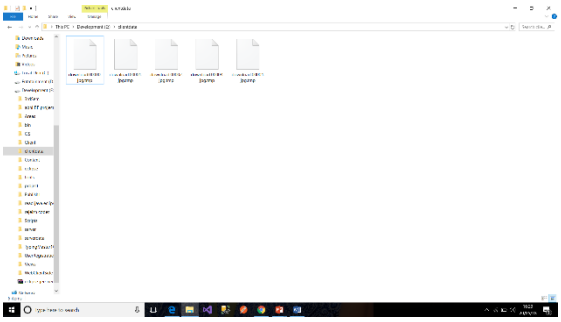

Figure 9: File Partioning.

The above figure 9 represents the data partioned and stored as a temporary files at the storage node after which it is transferred to the server which ensures that even if the storage node is attacked the health care data cannot be compromised and during transmission since it is transferred as partitions it cannot be merged by intruder to get the information stored in the file.

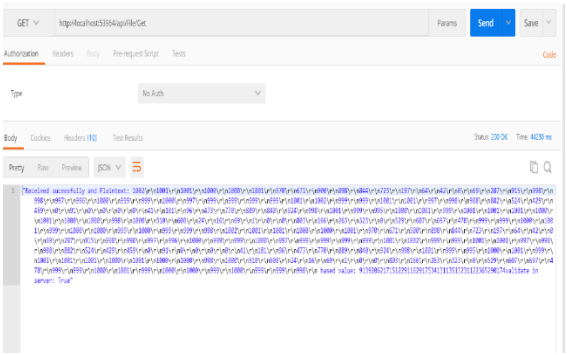

Figure 10: File Decryption and Validation.

Above figure 10 shows the file Decryption and Validation, at the server side the file is decrypted using AES algorithm and the hash of plaintext is computed if the hash is getting validated with the hash of client then the integrity of file is preserved and it is from intended sender.

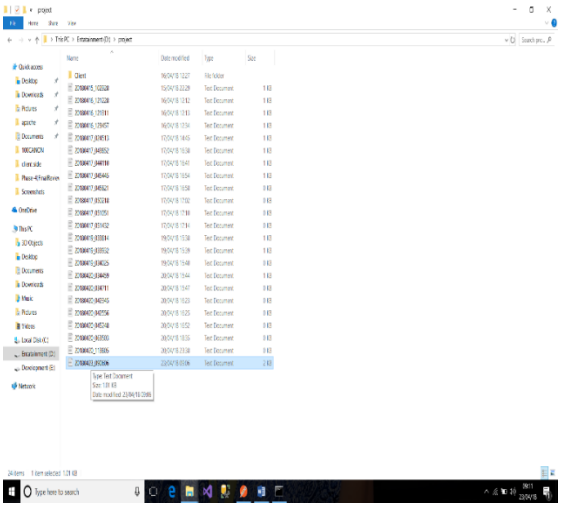

Figure 11: File Stored in Server Side.

Figure 11 shows the received file getting stored at server side when the server receives the file, the file gets stored on the server system in specified folder.

VI CONCLUSION AND FUTURE WORK

In this paper we have implemented a secure telemedicine system that focuses on preserving the Privacy of Sensed healthcare Data, Integrity of data, avoiding Impersonation, Prevention against Eaves Dropping and Data Corruption and securely transmitting it to the server system. This paper, proposes the Json web Token authentication scheme, Advance Encryption Standard and Secure Hash Algorithm Validation that protects the privacy of sensor data and the integrity of data. To preserve integrity, this thesis propose a data partition algorithm that partition data item into a separate files at the client system transmits and merges it at the server system.

The future work will include optimization and in memory encryption techniques. Client system can be replaced with a Local hand held device such as tablet or mobile phones for low computing power limited resource, and low cost. Furthermore, the application of secure telemedicine data can work on video transfer using the video compression techniques reducing the space and the response time.

REFERENCES

[1] Vaibhav Garg, M.S and Jeffrey Brewer, M.S,***"Telemedicine Security: A SystematicReview".***

[2] Lambros Makris, Nikolaos Argiriou and Michael G.Strintzis. Information Processing Laboratory, Electrical and Computer Engineering Department Aristotle University of Thessalonik ***"Network Access and Data Security Design for Telemedicine Applications"***.

[3] Ahmad Zainudin, Amang Sudarsono, Bagas Mardiasyah Prakoso Department of Electrical Engineering Politeknik Elektronika Negeri Surabaya ***"An Implementation of Secure Medical Data Delivery for Rural Areas Through Delay Tolerant Network"***.

[4] Ayman M. Eldeib-IEEE Senior Member ***"Interactive Telemedicine Solution Based on a Secure mHealth Application"***.

[5] Ying Yan and Lars Dittmann Department of Photonics Engineering, Technical University of Denmark ***"Security Challenges and Solutions for Telemedicine over EPON"***.

[6] Slobodan Kovacevic, Mario Kovac, Josip Knezovic Faculty of Electrical Engineerign and Computing, Zagreb, Croatia"***System for Secure Data Exchange in Telemedicine***".

[7]***"Jsonwebtoken"***,https://medium.com/vandium-software/5-easy-steps-to-understanding-json-web-tokens-jwt-1164c0adfcec.

[8]"***AESEncryption***",http://etutorials.org/Networking/802.11+security.+wifi+protected+access+and+802.11i/Appendixes/Appendix+A.+Overview+of+the+AES+Block+Cipher/Steps+in+the+AES+Encryption+Process/.

[9] "***Sha-1*** ", https://en.wikipedia.org/wiki/SHA-1.

[10]"***DataPartitioning***",https://www.c-sharpcorner.com/UploadFile/a72401/split-and-merge-files-in-C-Sharp/.

[11] H. Hacigumus, B. Iyer, C. Li, and S. Mehrotra, "***Executing SQL over encrypted data in the database-service-provider model***," in Proc. 21st ACM SIGMOD, Jun. 2002, pp. 216–227.

[12] B. Hore, S. Mehrotra, and G. Tsudik, ***"A privacy-preserving index for range queries***," in Proc. 30th VLDB, Aug. 2004, pp. 720–731.

[13] B. Hore, S. Mehrotra, M. Canim, and M. Kantarcioglu, ***"Secure multidimensional range queries over outsourced data,"*** in Proc. 21st VLDB, Jun. 2012, pp. 333–358.

[14] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, ***"Order preserving encryption for numeric data,***" in Proc. 23rd SIGMOD, Jun. 2004, pp. 563–574.

[15] A. Boldyreva, N. Chenette, Y. Lee, and A. O'Neill, ***"Order-preserving symmetric encryption,"*** in Proc. 23rd EUROCRYPT, Apr. 2009, pp. 224–241.

[16] A. Boldyreva, N. Chenette, and A. O'Neill, ***"Order-preserving encryption revisited: Improved security analysis and alternative solutions,"*** in Proc. 31st CRYPTO, Aug. 2011, pp. 578–595.

[17] R. Li, A. X. Liu, L. Wang, and B. Bezawada, ***"Fast range query processing with strong privacy protection for cloud computing,"*** in Proc. 40th VLDB, Oct. 2014, pp. 1953–1964.

[18] D. Boneh and B. Waters, ***"Conjunctive, subset, and range queries on encrypted data,"*** in Proc. 4th Theory Cryptograph. Conf., Feb. 2007, pp. 535–554.

[19] E. Shi, J. Bethencourt, T.-H. Chan, D. Song, and A. Perrig, ***"Multidimensional range query over encrypted data,"*** in Proc. 28th IEEE Symp. Secur. Privacy, May 2007, pp. 350–364.

[20] B. Sheng and Q. Li, ***"Verifiable privacy-preserving range query in twotiered sensor networks,"*** in Proc. 27th INFOCOM, Apr. 2008, pp. 46–50.