International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 06 | Jun 2022 www.irjet.net p-ISSN: 2395-0072

E-Health Care Cloud Solution

Ajay Hasole[1], Aniket Khatavkar[2], Mahesh Kamble[3], Rushikesh Alase[4], Yatiraj Korade[5], Prof. V.A. Shevade[6]

[1,2,3,4,5] Students, B. Tech Computer Science and Engineering, SETI, Kolhapur, Maharashtra, India.
[6] Assistant Professor, Dept. of Computer Science and Engineering, Sanjeevan Engineering and Technology Institute Kolhapur, Maharashtra, India.

Abstract - *Previously, patient reports were submitted to hospitals in the form of documents. There will be more space to keep patient reports. When an old patient comes to the hospital, it takes a lot of time to find his document. Its total wastage of paper. The documentation report is not secure. anyone can destroy the document easily and can stop all this, we have come up with a new idea. It's called an E-health cloud solution. Each patient report will save on the cloud. This Data will be safe and secure. It is accessible very easily Cloud computing is a new way of delivering computing resources and services Many managers and experts believe it has the potential to improve healthcare services, advance healthcare research, and transform health-information technology. The information is critical for making decisions and providing the best possible care to patients. Cloud computing is a cost-effective method for collecting, storing, and exchanging real-time data between healthcare organizations. Cloud infrastructure is characterized by high throughput and large storage volumes, both of which are critical for effective data analysis of large patient populations. Security and sequestration are the major enterprises that are answered using pall- grounded healthcare services. Data security continues to be one of the top enterprises for cloud computing, an issue that is been boosted by recent high-profile attacks in healthcare. The encryption result has to be quick and easy to provision and give high situations of protection without immolating network performance. It's another way to give a critical subcaste of security to cover the guests. In this work, we're interested in data encryption in the healthcare pall. Authentication is the first step for data security, through which druggies can establish evidence of identity before data access from the system. In a pall computing terrain, conventional authentication styles don't give strong security against the moment's most ultramodern means of attack. Cloud needs a dynamic approach for stoner authentication, which should include more than one authentication credential. we propose a data security armature with a robust, dynamic, and doable Multi-Factor Authentication scheme which integrates further than one factor like OTP for cloud stoner authentication.*

***Key Words*: Health Care, Cloud Computing, AES Algorithm, Patient History Reports, MFA.**

1. INTRODUCTION

In this project, the hospital can just use the services of the cloud to upload patient data. In healthcare system can manage the administration and required IT requirements that have the potential to retrieve the real-time information of patients without any delay. The uploaded data we can access through the cellular network and remote devices we can share the medical history of a patient helps doctors to treat a patient properly. The e-health (electronic health) system is one of many cloud services that stores and shares patient medical data between healthcare service providers and patients using computer or electronic systems and cloud technology. The health data/patient records are kept in a semi-trusted third-party supplier that is the cloud. Therefore, its security has become the main concern as the data should not be accessible to an unauthorized person To remain cost-effective, efficient, and timely while providing high-quality services, health care, like any other service industry, requires continuous and systematic innovation. Many managers and experts predict that cloud computing can improve health care services, benefit healthcare research, and change the face of information technology (IT). Several informatics breakthroughs have shown that cloud computing has the potential to solve these problems. Despite the many benefits associated with cloud computing applications for health care, there are also management, technology, security, and legal issues to be addressed.

2. PROBLEM DEFINITION

Already, persistent reports were submitted to healing within the frame of difficult duplicate archives. There will be more space to keep understanding reports. When an ancient persistent comes to the clinic, it takes a part of the time to discover his report. It adds up to the wastage of paper. The hard copy documentation report isn't secure. Anybody can annihilate the archives effectively. So anticipate this, we have come up with an idea called an E-healthcare cloud solution. Each patient's report will spare on the cloud. In this, information will be secure and secure. It is available exceptionally effortlessly.

3. LITERATURE SURVEY

During a writing overview, we gathered a portion of the data about the basic health care application and how it works as a system.

3.1 Survey on Big-Health Application System based on Health Internet of Things and Big Data.

Big Health Application System based on Health Internet of Things and Big Data. By using this paper, we got that the world is facing problems, such as uneven distribution of medical resources. This paper presents the big health operation system grounded on the health Internet of effects and big data. The system architecture, key technologies, and typical applications of big health system are introduced in detail. It will indicate current status of health is from health to low-risk status, to high-risk status of your health. To collect primary medical services, big health could use mobile medical health systems, big data, wearable devices, and a new generation of mobile communications technology. This system only collect the real time data and process it.

3.2Survey on Internet of things for Smart Healthcare: Technologies, Challenges, and Opportunities.

Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities. This check paper also presents the state- of- the- art exploration relating to each area of the model, assessing their strengths, sins, and overall felicity for a wearable IoT healthcare system. Security, privacy, wearability, and low-power operation are among the challenges that healthcare IoT faces, and recommendations for future research directions are made. The method chosen must have no negative consequences for the human body. This information should be sent to a database where it can be securely accessed by relevant parties (caretakers or doctors). In this paper, we found out that the Previous patient data/history cannot be stored.

3.3 Security and privacy issues in e-health cloud-based system: A comprehensive content analysis.

In this paper, they focused on an extensive review of current and existing literatures of various approaches and mechanisms being used to handle security and privacy related matters in e-Health Security and privacy requirements as recommended by Health Insurance Portability and Accountability Act n were also discussed and provided. reflections and recommendations were made regarding the review process and unborn directions on security and sequestration of e-Health in pall computing was also handed. It provides High security and privacy. In this limited data can be stored.

3.4 Development of Smart e-Health System for Covid-19 Pandemic

This paper presents development of smart e-health system for Covid- 19 epidemic. It's a smart Telemedicine system where case can consult with croakers staying at home The doctors arespecialized and highly professional in their field. Website has blog and shop site where doctor post different health issue to make awareness among the society and patient can buy their medicine. In this paper the doctor treat patient through video calling. There is a blog system where the article is published by doctors. It is a monitoring system so data can't be saved.

4. PROPOSED SYSTEM

Examine the existing healthcare applications in order to develop a reliable system that improves the consistency of patient-doctor communication. Create a reliable system for storing patient data in the cloud. Using various network scenarios, evaluate the performance of proposed routing protocols. To overcome the drawbacks of existing applications, compare the proposed healthcare application. Data security remains one of the most pressing concerns for cloud computing, a problem that has been exacerbated by recent high-profile attacks in the healthcare industry. One of the most pressing concerns for cloud computing is data security, which has been exacerbated by recent high-profile attacks in the healthcare industry. The encryption solution must be simple to set up and provide high levels of security without slowing down network performance. It's yet another way to protect clients by adding an additional layer of security. We're interested in data encryption in the cloud for healthcare. Authentication is the first step in data security, allowing users to establish proof of identity before gaining access to system data. Traditional authentication methods do not provide strong security in the cloud computing environment against today's most modern forms of attack. As a result, the cloud requires a dynamic approach to user authentication that includes multiple authentication credentials. We propose a data security architecture with a Multi-Factor Authentication scheme that integrates multiple factors such as OTP for cloud user authentication that is robust, dynamic, and feasible.

5. METHODOLOGIES

5.1 Advanced Encryption Standard

The Advanced Encryption Standard (AES) was created by the US National Institute of Standards and Technology (NIST) in 2001 as a specification for the encryption of electronic data. Despite being more difficult to implement, AES is widely used today because it is much stronger than DES and triple-DES. The AES cypher is a block cypher. The key can be 128, 192, or 256 bits long. Data is encrypted in 128-bit blocks. Sub Bytes, Shift Rows, Mix Columns, and Add Round Key are the four steps in each round.

5.1.1 Encryption:

1. Sub Bytes: This is where the substitution is put into action. Each byte is replaced by another byte in this step. (A lookup table, also known as the S-box, is used.) This substitution is carried out in such a way that a byte is never substituted by itself, nor by another byte that complements the current byte. As before, the result of this step is a 16byte (4 x 4 matrix). The permutation is implemented in the next two steps.

2. Shift Rows: This is exactly what it sounds like. A certain number of times each row is shifted. The first row isn't shifted in any way. The second row is shifted to the left once more. The third row has been shifted to the left twice. The fourth row has been shifted three times.

3. Mix Columns: This is where the matrix multiplication happens. Each column is multiplied by a specific matrix, resulting in a change in the position of each byte in the column. In the final round, this step is skipped.

4. Add Round Keys: The previous stage's resultant output is XORed with the corresponding round key. The 16 bytes are not considered a grid in this case, but rather 128 bits of data.

5.1.2 Decryption:

The rounds' stages can be easily undone because they have an opposite that, when performed, reverses the changes. Depending on the key size, every 128 blocks go through 10,12, or 14 rounds. The following are the stages of each round of decryption: Inverse Mix Columns, Shift Rows, and Inverse Sub Byte are all added to the round key. The encryption and decryption processes are very similar. It is carried out in the reverse order.

1. Inverse Mix Columns: This step is similar to the Mix Columns step in encryption, but the matrix used in the operation is different.

2. Inverse Sub Bytes: An inverse S-box is a lookup table that is used to substitute bytes during decryption.

6. SYSTEM ARCHITECTURE

In the system architecture we are implemented some pages as follows,

6.1 Home page:

We created the home page using HTML and CSS language and it is used for our system details and accessing the login page.

6.2 Registration page:

This module is created for users can create their account on the website for getting a username and password. To login into our system.

6.3 Login page:

This page was created for accessing the system by the authorized user using a username and password.

6.4 Data Encryption/Decryption:

In this module, we can store the user's data in encrypted format in the database and retrieve data in decrypted format.

6.5 E-mail confirmation:

It's used after registration user can get the confirmation mail for a successfully created account in the system and get the username and password.

6.6 OTP authentication:

We are providing multifactor authentication for security purposes.

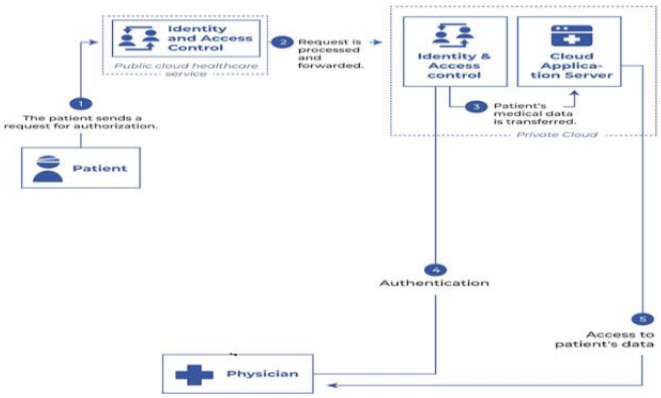

Fig -1: System Architecture

7. MODULES

7.1 Home Page Module

It is for access to the website. We give the patient login and Physician login buttons. In the home page module, we give the doctor login and the patient login along with the contact us, about us.

7.2 Physician/Patient Registration Module

In the Physician and patient registration module, a patient or doctor creates their account on the E-health cloud

solution website. To login into an account, a user has to give their Aadhar number as a login id and give the password he/she gives at the time of registration.

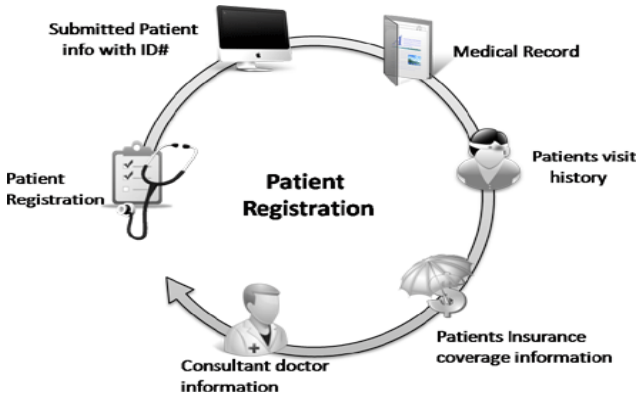

Fig -2: Registration Module

7.3 Data Encryption/Decryption Module

In this module, we can store the user's data in encrypted format in the database and retrieve data in decrypted format.

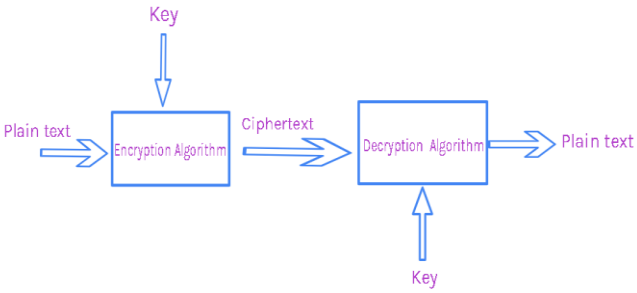

Fig -3: Data Encryption/Decryption module

Plain text is sent by the sender for encryption and is encrypted using an encryption algorithm. The Key is a 128-bit block cipher key that is added to the plain text for encryption. The encryption algorithm is applied to the Sender side for encryption. The decryption algorithm is applied to the receiver side for decryption. The ciphertext is an encrypted /converted plain text with a key using an encryption algorithm.

7.4 Physician and patient Login Module

Physicians and patients can log in to the system using their id and password given by our system. The physician can store the data of the patient in the cloud. A patient only read the data into the system.

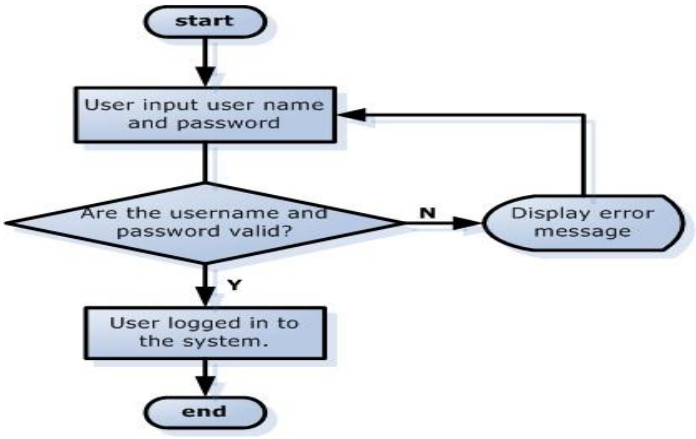

Fig-4: Login module

7.5 OTP Login Module

Physicians and patients can log in also using OTP. It's useful for quick login and it is also useful for when a user forgot their id and password.

7.6 Cloud Module

We are using the cloud service to store patient data. And it can access by an authorized person anywhere. In our project, we used the good cloud service which is AWS cloud service. Particular amazon E3 is used because it gives 12-month free cloud storage services.

8. PROJECT RESULTS

8.1 Home

We created a home page using HTML and CSS language and it is used for our system details and accessing the login page.

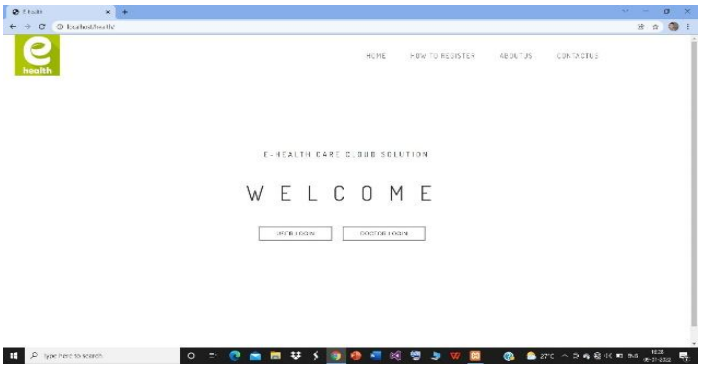

Fig -5: Home Page

8.2 Registration

This module is created for the user can create his account on the website for getting a username and password. To login into the system.

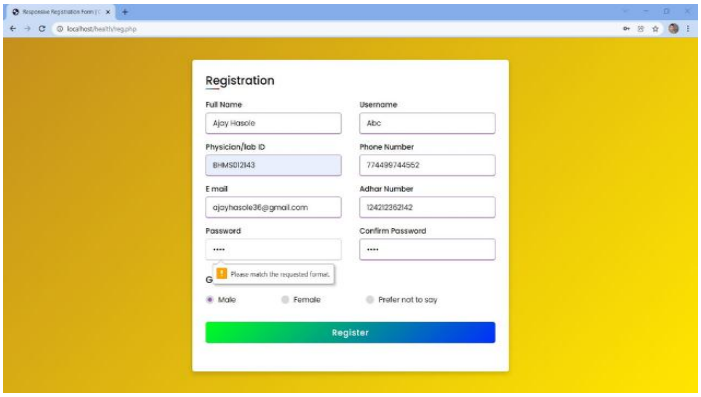

Fig -6: Registration Form

3.Database

In this module, we can store the user's data in encrypted format in the database and retrieve data in decrypted format. In this project, a MySQL database is used in that the PhpMyAdmin admin panel is used for better performance.

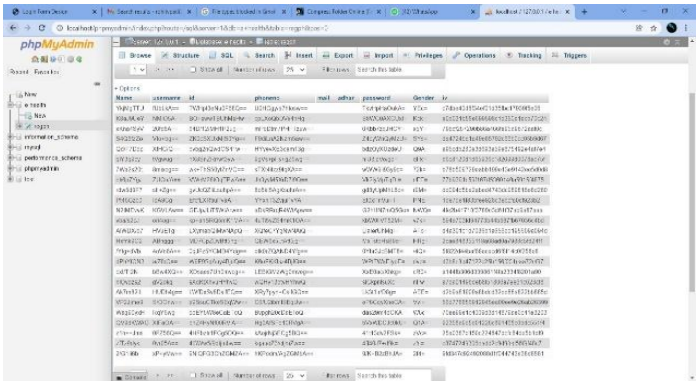

Fig -7: Data Base Store Encrypted data

4.Registraion Confirmation Mail

It's used after registration user can get the confirmation mail for a successfully created account in a system and get the username and password.

Fig -8: Registration Confirmation Mail

5.Login Form

This page was created for accessing our system only for the authorized user using a username and password.

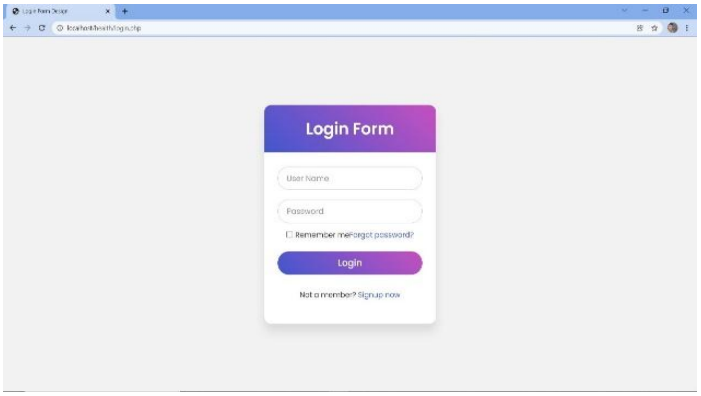

Fig -9: Login Form

6.OTP Generation

In the OTP generation module, we are providing multifactor authentication for security purposes. In OTP generation the OTP is always generated when the user wants to log in to the system. We used the Fast SMS service for the OTP generation.

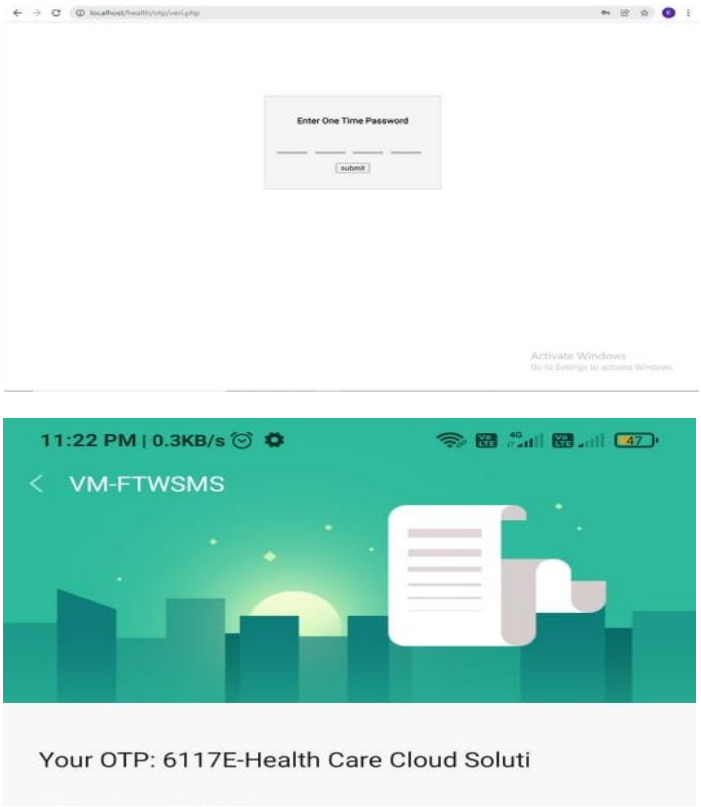

Fig -10: OTP Generation

9. CONCLUSION

Everybody has to be well educated and concerned almost the quality of care. Everybody implies patients and their families, shopper operators and advocates, wellbeing experts, chairmen of wellbeing plans and offices, buyers of wellbeing care administrations, and policymakers at all levels. The messages to these groups of onlookers are 1) that the quality of care can be measured and made strides and that quality of care thought to not be overlooked in the interest of fetched control. Fortifying these messages implies making beyond any doubt that quality of care remains on the wellbeing care-delivery motivation, with clear distinguishing proof of the dangers and openings that are postured by the changes in wellbeing care within the Joined together States. It moreover implies portraying how well-being plans, well-being care organizations, and clinicians ought to be responsible to patients and society and, on the other hand, how people can take suitable obligation for their claimed well-being.

10. REFERENCES

[1] Big Health Application System Based on Health IoTs and Big Data. https://www.ieee.org.comY. Ma, Y. Zhang, J. Wan, D. Zhang, and N. Pan, Robot and cloud-assisted multi-modal healthcare system,'' Cluster Compute.

[2] Vinit Atul Shevade, D. A. Kulkarni: Redundancy Prevention and Secure Audit of Encrypted Big Data in HDFS Cloud using Cloud Guard+ System. https://www.sciencepubco.com/

[3] IoT for Smart Healthcare: Technologies, Challenges, ,Opportunities. http://www.ieeeexplorer.ieee.org. inJ.Zhou,Z.Cao,X. Dong, and A. V. Vasilakos,Security and privacy for cloud-based IoT: Challenges,'' IEEE Communicate.

[4] Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud http://www.engpaper.in/www.ieeepels.org I. X. Yi, Y. Miao, E. Bertino, and J. Williamson, ``Multiparty privacy protection for electronic health records,'' in Proc. IEEE Global Communicate.

[5] Development of Smart e-Health System for Covid19pendamic.http://www.ieeecas.org.in/www.ieeemce.org.

[6] Y. Zhang, M. Chen, S. Mao, L. Hu, and V. Leung, CAP: Community activity prediction based on big data analysis, IEEE Netw, vol. 28, no. 4, pp. 52–57, Jul./Aug. 2014.

[7] J. Wang, Y. Zhang, J. Wang, Y. Ma, and M. Chen, „PWDGR: Pair-wise directional geographical routing based on wireless sensor network,‟ IEEE Internet Things J., vol. 2, no. 1, pp. 14–22, Feb. 2015.

[8] D. V. Dimitrov, „Medical Internet of Things and big data in healthcare, "Healthcare Inform. Res., vol. 22, no. 3, pp. 156–163, Jul2016.[Online].Availablehttp://ww.ncbi.nlm.nih.gov/pmc/articles/PMC4981575.

[9] Y. J. Fan, Y. H. Yin, L. D. Xu, Y. Zeng, and F. Wu, „IoT-based smart rehabilitation system,‟ IEEE Trans. Ind. In format., vol. 10, no. 2, pp. 1568–1577, May 2014.

[10] Polisena J, Coyle D, Coyle K, McGill S (2009) Home telehealth for chronic disease management: a systematic review and an analysis of economic evaluations. Int J Technol Assess Health Care.

[11] Finkelstein SM, Speedie SM, Potthoff S (2006) Home telehealth improves clinical outcomes at a lower cost for home healthcare. Telemed J e-Health12(2):128136.

[12] Peter M Yellow lees, "Successfully developing a telemedicine system", Journal of Telemedicine and Telecare, vol. 11, no. 7, pp. 331-335, 2005.

[13] BH Stamm, "Clinical applications of telehealth in mental health care", Prof Psychol Res Pract, vol. 29, no. 6, pp. 536, 1998.

[14] SM Finkelstein, SM Speedie, and S Potthoff, "Home telehealth improve clinical outcomes at a lower cost for home healthcare", Telemed J e-Health, vol. 12, no. 2, pp. 128-136, 2006.

[15] An Introduction to the Basics of Video Conferencing, 2012, 28 Jan 2014, [online] Available:http://www.polycom.co.uk/content/dam/polycom/common/documents/brochures/video-basics-br-engb.pdf.

[16] W.U. Hasan, M. Sultan Khaja, S. Ahmed and M.M. Khan, "Wireless Health Monitoring System", 2nd Borneo International Conference on Applied Mathematics and Engineering, 2018.

[17] Fayezah Anjum, Abu Saleh Mohammed Shoaib, Abdullah Ibne Hossain and Mohammad Monirujjaman Khan, "Online Health Care", 8th Annual Computing and Communication Workshop and Conference (CCWC), 2018.

[18] E. Stefanov, M. van Dijk, A. Juels, and A. Oprea, "Iris: A scalable cloud file system with efficient integrity

checks," in Proceedings of the 28th Annual Computer Security Applications Conference, ser. ACSAC '12. New York, NY, USA: ACM, 2012, pp. 229–238.

[19] Advanced Encryption Standard (AES) – GeeksforGeeks.https://www.geeksforgeeks.org/advanced-encryption-standard-aes.

[20] Tanveer Reza, Sarah Binta Alam Shoilee, Sirajum Munira Akhand and Mohammad Monirujjaman Khan, "Development of Android Based Pulse Monitoring System", Second International Conference on Electrical Computer and Communication Technologies (ICECCT), 2017.

[21] L.F. Wei, H.J. Zhu, Z.F. Cao, X.L. Dong, W.W. Jia, Y.L. Chen, and A.V. Vasilakos, "Security and privacy for storage and computation in cloud computing," Information Sciences, 2014, vol. 258, pp. 371-386, doi:10.1016/j.ins.2013.04.028.