Grenze International Journal of Engineering and Technology, Jan Issue

Medical Records with OTP Authentication

Nallani Mounika[1] and Prof.Priyanka H[2]
[1-2]PES University, Computer Science and Engineering, Dwaraka Nagar, Bengaluru, India
Email: nallanimounika86655@gmail.com, priyankah@pes.edu

***Abstract*—As we all know, a massive amount of data is released every day in this developing world. The healthcare industry, among many others, needs more attention because of its potential to improve the quality and efficiency of healthcare services. Integrity and confidentiality are, necessary for the authentication of medical documents. When clinical information are accidentally made available to dishonest outsiders, privacy is violated. The goal of this study is to make it safe to upload medical documents on the web. A one-time password, that is secret key allows for an authenticated [1] copy by providing confidentiality and integrity for sub-document authentication.**

***Index Terms*— Integrity, confidentiality, authentication, one time password, secret key, upload medical document.**

I. INTRODUCTION

Every day of our lives, we are all aware that effective medical data sharing is taking place. However, there is no data protection security. Pharmaceutical businesses, insurance companies, research institutes, and many other public entities may be forced to submit medical records to a study organization in order to improve the superiority and efficiency of health handling operations. Medical records, prescriptions, social security numbers, personal information, address and reimbursement information, credit card numbers, and medical history are all vulnerable and should be protected. Another important criteria for the tributary use of health information is that it should be kept confidential by using OTP authentication [2]. In self-generated mode, the true level of protection is nothing more than the password. However, unlike the password used to log in and passwords generated via email have security limitations, such as:

A. May Only be used Once

Once a password has been used, it cannot be used again. Intercepting the degenerated passwords of mobile token in this manner is pointless because the password cannot be used again. However, even if the pass word [3] is intercepted before it reaches the server, it is still a valuable password because the server password has not been used.

B. Can Only be used for a Short Period of Time

Passwords created by mobile tokens have a relatively short lifespan, probably between 2-3 minutes. Once the time period Identify applicable funding agency here. If none, delete this. has expired, the password can no longer be used. Even if it has never been used before. Time is critical in this mobile token system [4].

Grenze ID: 01.GIJET.9.1.85

II. RELATED WORK

One of the most important areas for researchers to look into is the hardware and software implementation of the AES algorithm [5]. Several research publications on the AES algorithm, which provides much more complexity and analyses the efficiency of popular encryption algorithms to encode and decode data, have been published in recent year.

In [6], Lu et al. introduced a new design technique for decreasing the complexity of the AES algorithm in Cryptanalysis and System Security 2017 when it is implemented on devices like mobile phones, online applications, and smart cards. To develop a fully functional AES crypto-engine, the encrypted and de- crypted versions of AES were combined. To accomplish so, they concentrated on a few key elements of AES, particularly the Encryption, Decryption, Sub Bytes and Mix column modules.

In [7], Berent A. This research analyses the performance of three methods for encrypting text files, including AES and RSA, using computation time, memory use, and output bytes are the three parameters. The time it would take to convert plaintext to cipher text was computed, and then these algorithms were compared to find which one encrypts a text file the slowest. According to their findings, RSA takes more time than other algorithms. RSA methods use more memory than AES algorithms for second parameters. Finally, the output byte of each algorithm was considered. AES has the same output byte level as RSA, while RSA has a lower output byte level.

In [8], Sagar Acharya. One-time passwords (OTPs) are passwords that are only valid for a single login session or transaction. OTP is commonly used as a one-time use password that is instantly forfeited rather than being stored in a database. The advantage of the OTP is that it is situated on a distinct application and has a static password that is stored in the database. The usage of encrypted static passwords is not safe against a key logger or similar attack, because if an attacker obtains the main password and OTP password, they can still log in and complete transactions, even though the password is no longer valid. The AES algorithm, which is extensively used, is used to generate code as encryption.

In [9], Dr.Virshree Tungare. A Study That was detailed in an advancement of mobile payment system. In comparison to all other payment systems, UPI might be considered the world's most advanced payment system. The UPI payment system allows money to be moved between any two bank accounts using a smartphone or web application transaction. It enables customers to make payments straight from their bank accounts to various retailers, both online and offline, without having to type credit card numbers, IFSC codes, or net banking/wallet passwords. Its goal is to provide a single interface that makes money transfers simple, quick, and painless. These aspects of UPI drive service sector respondents to utilize the technology, and the survey demonstrated that there is a considerable variation in UPI adoption.

They build a website and connect with doctors online using a chat box in the existing system. However, before we could interact with doctors, they need to transmit past reports and upload documents using images as a security measure. They could choose any image in the patient system. The report can be seen by the doctor using the same image that was provided by the patient as depicted in "Fig 1".

Client sends the image via any social media such as email, What's app, etc. In that case, there is a danger that the image will be hacked, so we recommend utilizing the OTP as an authentication [10] method.

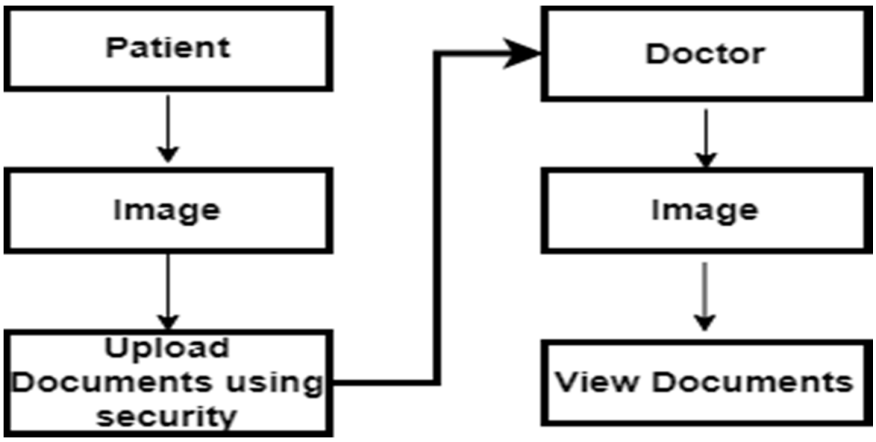

Figure 1. Architecture of Existing System

III. PROPOSED SYSTEM

We recommend securing the document before uploading it. Test results, diagnosis reports, and medicines will all be included. This functions as a digital safe de- posit box that can only be accessed by the patient and their authorized doctors. Viewing patient reports, generating prescriptions, checking payment details, and checking appointments are all functions available to the doctor as depicted in "Fig 2". Another feature provided to patients is the ability to submit documents, read prescriptions, pay bills, schedule appointments, and communicate with doctor by using chat box. To reduce the chances of reports being tampered with, neither side will be able to modify or delete them. Smart contracts will be used to secure and OTP services like secret key will be used for authentication [11] and authorization. We provide a payment module that can be used with any UPI [12].

A. Advantages

- To secure medical report.
- Interact doctor in easy manner.

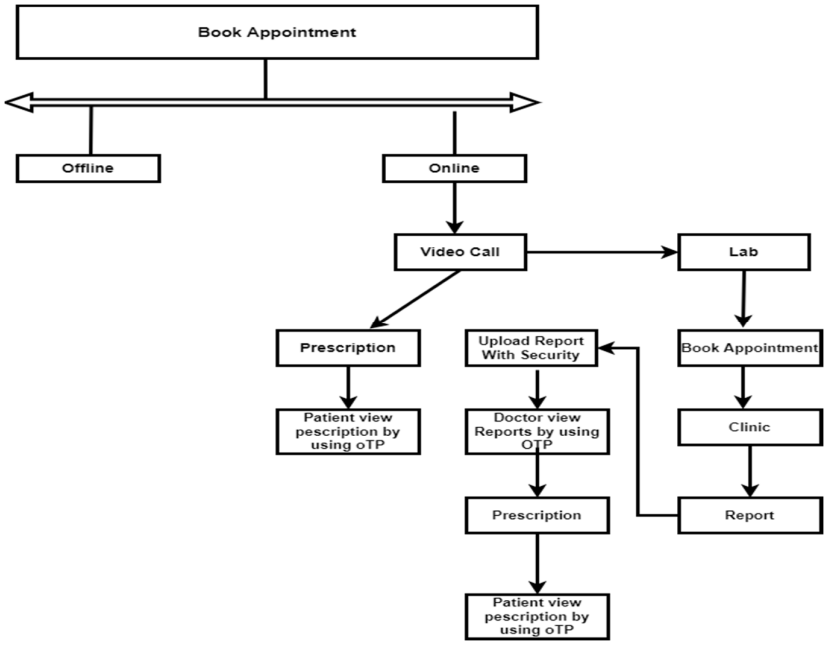

Figure 2. Architecture of Medical Document

We are using Advanced Encryption Standard algorithm it is a symmetric block cipher. Symmetric cipher, often known as secret key ciphers, use the same key to encrypt and decrypt data. The secret key must be known and used by both the sender and the receiver. The 128, 192, and 256-bit cryptographic keys, each cypher encrypts and decrypts data in 128-bit blocks [13]. We apply the AES algorithm to secure the report. The AES algorithm will operate in this approach as depicted in "Fig 3".

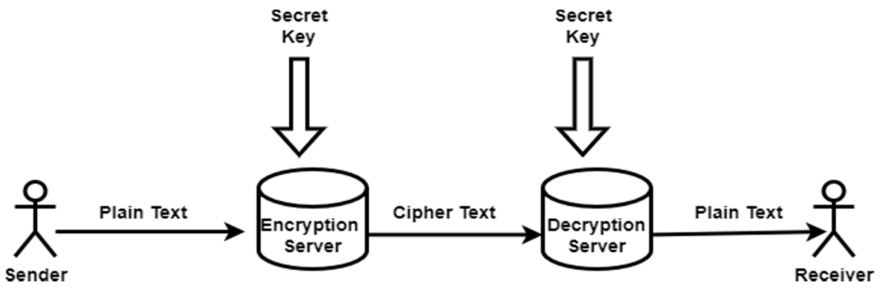

Figure 3. Architecture of AES

The data is in text format before encryption as depicted in “Fig 4”.

```
Patient Record
Common Information:
Patient ID:9876
Patient Name: shruthi
Fathers Name: Kaliappan
DOB: 02/07/1988
Address: Bangalore
Mobile number: 9902752525
Admitted at: Gayathri Hospital Vijayanagr
Doctor: Dr. Gandhi MBBS MD
Date of Admittion: 28/02/2021
Date of Discharge: 05/03/2021
=
Doctor Information:
Bp: Normal
Sugur: Normal
Infections: normal fever
Medicine prescribed: Dolo650 for three time in a day for 2 days
@
Personal Infomation:
Self made
anger
#
Eswar
eswar
1
fever
```

Figure 4. Text File

The AES encryption method generates cipher text [14], which is an illegible, effectively unreadable conversion of plain text data. Plain text data is the form that humans can read and understand. The AES cipher text, which is the out- come of the encryption process, can only be decrypted using a secret AES key. The data is encrypted after it has been encrypted as depicted in “Fig 5”.

Figure 5. Encrypted File

In AES-encrypted communications, the sender and recipient share the same AES secret key, which is used to convert data into cipher text and readable plain text. If a hacker intercepted this data, he or she would be unable to read it without the AES secret key, which would hopefully only be known by those sending and receiving encrypted data.

IV. Result and Discussion

The following are the modules that are included in medical records with OTP authentication.

A. Admin

The server logs in with a valid user name and password in this module. As depicted in Fig 6 represents the admin home page:

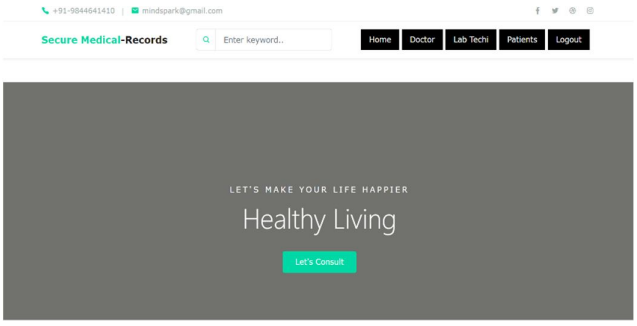

Figure 6. Admin Home Page

B. Patient

After successfully log in with a valid user name and password, the patient's home page is displayed. As depicted in "Fig 7"represents the patient's home.

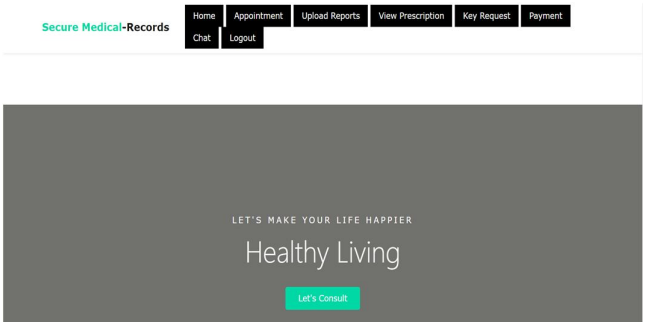

Figure 7. Patient Home Page

Patients can schedule appointments in one of three ways: online, offline, or in the lab. "Fig 8" shows the screenshot of the appointment booking.

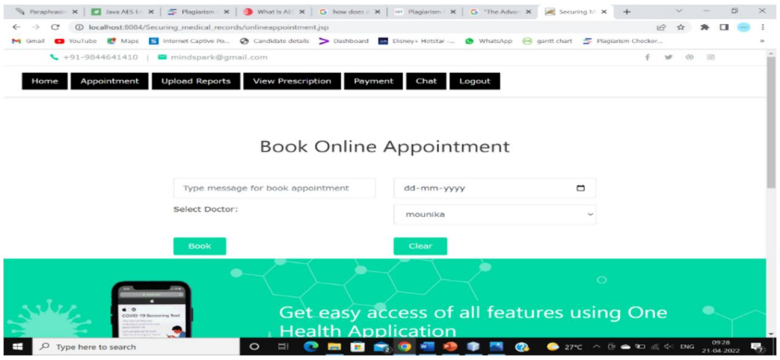

Figure 8. Booking Appointment

Patients can also upload reports in .txt format, as well as mention the patient's name and the report's URL. "Fig 9" shows the screenshot of the report uploading.

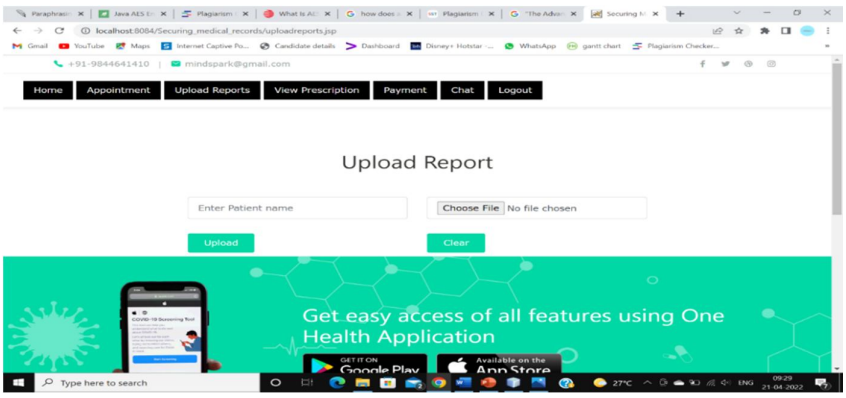

Figure 9. Upload Report

C. Doctor

A doctor [15] can check the patient's appointment and also can communicate with the patient, as well as suggest a prescription and treatment to the patient. As depicted in "Fig 10" represents the doctor home page:

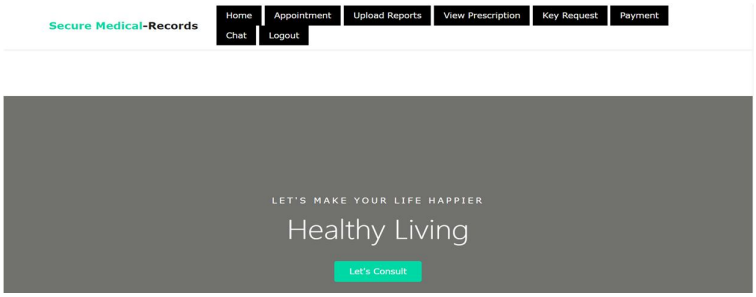

Figure 10. Doctor Home Page

The report can be seen in two ways by the doctor. One is to use a secret key that is sent to us in the mail, which we may input and download, and another is to ask the patient to generate a key "Fig 11" shows the screenshot of the view the report.

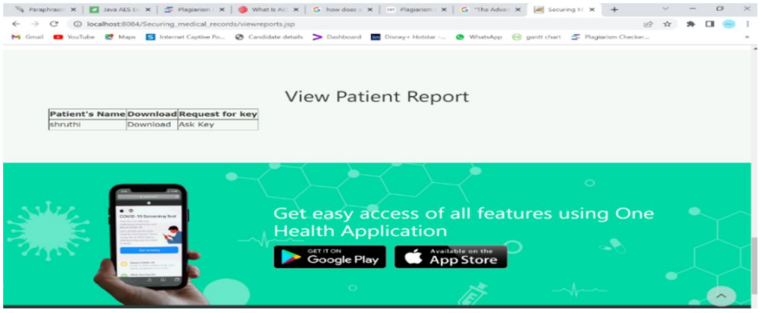

Figure 11. View Patient Report

If the doctor wants to see the report, doctor must first download it. The doctor can enter the OTP that was generated by the patient to get the report. OTP can be viewed by a doctor by mail, which is in the form of a secret key. The "Fig 12"of this module is depicted below.

Test Case Id	Description	Expected Output	Actual Output	Pass/Fail
01	Test case for encryption	Upload Reports in txt format it get successful	Display Successful.	Pass
02	Test case for decryption enter correct secret key	Download Report	Download Successful.	Pass
03	Test case for decryption enter incorrect secret key	Download Report	Incorrect secret key.	Fail
04	Doctor ID and password are blank	Successfully Login	Incorrect user name and password.	Fail
05	Enter correct patient ID and password	Successfully Login	Display Patient home page.	Pass
06	Doctor ID and password are blank	Successfully Login	Incorrect user name and password.	Fail
07	Enter correct Doctor ID and password	Successfully Login	Display Doctor home page.	Pass

The completion of our proposed model prototype, we launched the website that allows users to securely upload reports. User can find online medical [16-17] records to be more secure, as depicted in "Fig 3".

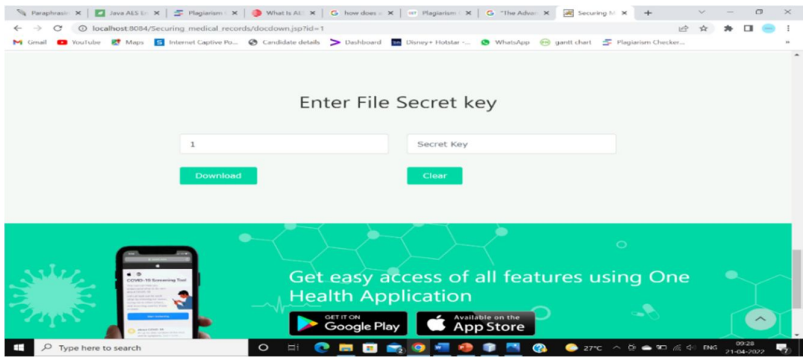

Figure 12. Secret Key

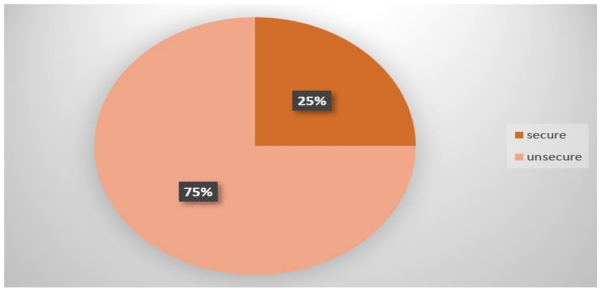

Figure 13. Users Finding Online Medical Records More Secured

Another major module is being used. Users of UPI/BHIM apps are categorized as depicted in “Fig 14” based on how they use apps to process transactions. “Fig 10” illustrates that the majority of users make UPI payments [18] through third- party apps such as Phone pay, Paytm, Amazon Pay, Google Pay, and others. The cashback and other cashback-related incentives provided by third-party app providers, as well as their promotion, stimulate the use of a third-party app for UPI [19] and below is the test strategy as show in “Table 1”.

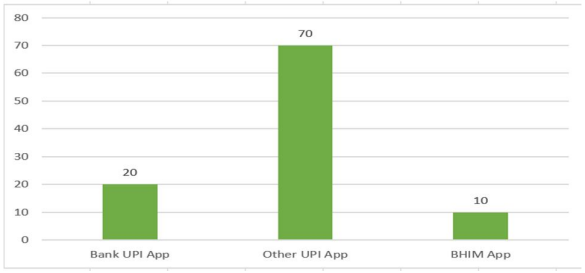

Figure 14. Bar Chart

V. Conclusion

This paper focuses on the full stack web architecture for the implementation of uploading medical reports that will be used in the healthcare system. We are not only securing patient medical records, but we are also making them easily accessible, allowing doctors to gain a better understanding of the patient by analysing previous records, allowing patients to skip going through files of paper work before seeking treatment, and hospitals will no longer be required to keep individual patient records. Our main goal is to make the process of making a person’s medical records widely available so that their life might be saved as soon as possible. At the same time, we can send reports to a secure site where medical records can be preserved without exposing any personal information about the patient. The reports can be downloaded if a doctor views them and provides a secret key. This strategy benefits both the doctor and the patient since it makes their work easier and safer.

We can add a payment module to our app so that users may pay for their consultations directly on the platform, after scheduling an appointment and discussing their health problems with the doctor. We can communicate with doctors in live time via the internet using Zoom, Google Meet/Teams, or any other social media platform [20].

REFERENCES

[1] G. Muthukumar S. Santhosh kumar ."Authenticated medical documents releasing with privacy protection and release control". Published in International Journal of Trendy Research in(IJTRET) Engineering and Technology Volume 4 Issue 3 June 2020 ISSN NO 2582-0958.

[2] Al-Sahwan, Ghadeer M., et al. "A Strong and Practical Authentication Mechanism Using Pass Text and OTP." 2018 21st Saudi Computer Society National Computer Conference (NCC). IEEE, 2018.

[3] Nilesh A. Lal Salendra Prasad."A Review Of Authentication Method".Proceedings of the International Journal of Scientific Technology research VOLUME 5, ISSUE 11, NOVEMBER 2016 ISSN 2277-8616.

[4] Aujla, S. G. "A Review of One Time Password Mobile Verification." International Journal of Computer Science Engineering 4.3 (2014): 113-118.

[5] Jianghua Liu Jinhua Ma. Authenticated medical documents releasing with privacy protection and release control".Published in IEEE Volume: 18, Issue: 1, Jan.- Feb. 1 2021 DOI: 10.1109/TDSC.2019.2892446.

[6] Lu, Chih-Chung, and Shau-Yin Tseng. "Integrated design of AES (Advanced Encryption Standard) encrypter and decrypter." Proceedings IEEE International Conference on Application-Specific Systems, Architectures, and Processors. IEEE, 2002.

[7] Jindal, Poonam, Aryan Kaushik, and Keshav Kumar. "Design and implementation of advanced encryption standard algorithm on 7th series field programmable gate array." 2020 7th international conference on smart structures and systems (ICSSS). IEEE, 2020.

[8] Berent, Adam. "Advanced Encryption Standard by Example." Document available at URL http://www. networkdls.com/Articles/AES by Example. pdf (April 1 2007) Accessed: June (2013).

[9] Acharya, Sagar, Apoorva Polawar, and P. Y. Pawar. "Two factor authentication using smartphone generated one time password." IOSR Journal of Computer Engineering (IOSR-JCE) 11.2 (2013): 85-90.

[10] Tungare, Dr Virshree. "A study on customer insight towards upi (unified payment interface)-an advancement of mobile payment system." International Journal of Science and Research (IJSR) 8.4 (2019): 1408-1412.

[11] Mahesh, A., and Ganesh Bhat. "Digital Payment Service in India-A Case Study of Unified Payment Interface." International Journal of Case Studies in Business, IT and Education (IJCSBE) 5.1 (2021): 256-265.

[12] Shah, Syed W., and Salil S. Kanhere. "Recent trends in user authentication–a survey." IEEE access 7 (2019): 112505-112519.

[13] Pitchaiah, M., and Philemon Daniel. "Implementation of advanced encryption standard algorithm." (2012).International Journal of Scientific Engineering Re- search Volume 3, Issue 3, March -2012 1 ISSN 2229-5518.

[14] Kaur, Jagpreet, Shweta Lamba, and Preeti Saini. "Advanced Encryption Standard: Attacks and Current Research Trends." In 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), pp. 112-116. IEEE, 2021.

[15] Ariel Belasen Alan T. Belasen(2018)."Doctor-Patient communication a review and a rationale for using an assessment framework".Journal of Health Organization and Management Emerald Publishing Limited1477-7266DOI 10.1108/JHOM-10-2017- 0262.

[16] Nalamothu. Aravind Sakala Ro."Analysis on authorization of medical documents provision with secured privacy scheme".Published in Journal of Xi'an University of Architecture TechnologyJ Volume XII, Issue III, 2020 Issn No : 1006-7930.

[17] Shaik Mohammad Aafreen Sulthana(2021). "Privacy protection authenticated medical documents releasing with and release control". Published in UGC care group 1 listed journal ISSN: 2278-4632 (UGC Care Group I Listed Journal) Vol-11 Issue-01 2021.

[18] Islamiati, Dewi Sandy, Dias Agata, and Adnan Rahmat Anom Besari. "Design and implementation of various payment system for product transaction in mobile application." In 2019 International Electronics Symposium (IES), pp. 287-292. IEEE, 2019.

[19] Wan, Fucheng, Jiajia Li, Ning Ma, Xiangzhen He, Yaru Cao, and Heng Yang. "Research and Design of E-commerce Payment System." In 2017 International Conference on Computer Technology, Electronics and Communication (ICCTEC), pp. 1294-1297. IEEE, 2017.

[20] CLN, Abu Umaru Isaac, and Isaiah Michael Omame CLN. "Application of social media and video conferencing in smart library services." Library Philosophy and Practice (2020): 1-13.