Volume 9, Issue 10, October – 2024 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24OCT1787

Maintaining Integrity and Confidentiality of Patients' Records Using an Enhanced Security Technique

Ononiwu Chamberlyn C.
Department of Computer Science
School of Applied Sciences
Imo State Polytechnic Omuma, Nigeria

Mgbeafulike Ike J.
Department of Computer Science
Chukwuemeka Odumegwu Ojukwu University, Uli, Nigeria

Abstract:- Medical record storage on paper is currently being phased out and replaced by more sophisticated Electronic Health Record (EHR) systems. However, the ease of access to data and the digitization of medical records also come with the potential of misuse of personally identifiable information and healthcare data breaches. How technology will protect patient privacy is one of the primary concerns about EHRs. Network connectivity is another major issue, therefore keeping private health information online may expose it to major information leaks to external parties. Around the world, data management and privacy are major concerns. The main concerns that prevent businesses from using cloud computing are security and information authenticity, as they fear that data may be lost to unauthorized parties. The quantity of patient-oriented data in the healthcare system is continuously increasing, and the current medical systems are confronted with security issues such as weak access control, data breaches or unauthorized disclosure, and insufficient authorization and authentication. An Enhanced Security Model was created in this study to secure and protect Electronic Health Records. The records were encrypted for security and privacy utilizing the Advanced Encryption Standard (AES), One Time Password (OTP), and National Identity Number (NIN). The system was designed using Object Oriented Analysis and Design Methodology (OOADM). The New System improved patient record security by utilizing NIN for cloud identity management, OTP for authentication, and AES for privacy and security. While the MySQL server was used to implement the database, HTML, CSS, PHP, and JavaScript were used to program the system. Comparing the new system to the old system, the results of the performance assessment analysis based on security, user-friendliness, dependability, and privacy show that the new system has very good performance efficiency and integrity.

Keywords:- *Electronic Health Records (EHR); NIN; OTP; AES; Cloud Computing.*

I. INTRODUCTION

Electronic health record (EHR) systems have been increasingly popular in hospitals and clinics in recent years. The paperless answer to a disjointed healthcare system that relies on a chain of paper files is electronic health records, or EHRs. New opportunities are created, productivity is increased, administrative hassles are lessened, and medical errors are decreased. At the point of care, EHR gives physicians quicker access to potentially life-saving information. The foundation for better patient care is the storage and retrieval of this massive amount of medical data. Nevertheless, it is expensive and time-consuming to manually capture and store the enormous volume of medical record data that is produced from many sources. It presents significant difficulties when trying to analyze this data in a useful way or even prevent data destruction.

The quantity of patient-oriented data in the healthcare system is always increasing. More hospitals with a variety of departments and units are opening. Medical equipment, lab findings, computerized prescriptions, treatment choices, and clinically observed values by doctors and nurses can all produce patient-oriented data. These data are fragmented and must be accessed by submitting a request to the different hospital departments. In addition to taking a lot of time, this is insecure and outdated. The current issues facing the healthcare system are as follows:

- Access Control Vulnerabilities: Unauthorized access to electronic health records may result in privacy violations and jeopardize patient confidentiality.
- Unauthorized disclosure and data breaches: These provide serious privacy threats to patients and may lead to fraud, identity theft, or harm to healthcare institutions' reputations.
- Inadequate Authorization and Authentication: Unauthorized users may be able to access electronic health records due to inadequate authorization and authentication procedures. The integrity of the records may be jeopardized as a result of patient data tampering or alteration.

Information loss to unauthorized parties is a fear many people have. Therefore, in order for hospitals to have a more safe method of sharing data within the healthcare sectors without compromising data security and privacy, it is necessary to find a more dependable and secure method of securing electronic health records.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24OCT1787

II. REVIEW OF RELATED WORKS

Hospitals' primary duty is to ensure the lives and health of its patients. Effective medical care requires highly qualified medical professionals that have both theoretical understanding and compassion for their patients. Additionally, it requires high-end facilities and equipment. Maintaining accurate records serves as a guide for the health care plan that is created, outlining the most fundamental aspects of medical care. As the patient provides it, it requires precision and accuracy. Based on this data, a thorough, updated report informs medical professionals on the best course of action. Neglecting to do so leads to misunderstandings and incorrect diagnoses of a patient's information and symptoms, this may have life-threatening repercussions. Healthcare professionals must constantly use extreme caution when maintaining patient records since even the smallest error could have serious consequences. A patient's health record is a representation of the hospital's role in their life, from which research, statistical, and medical reports may be derived [1].

Predicate Based Encryption (PBE) is a security approach that was presented by [4] in 2019. The asymmetric encryption family known as PBE is derived from Identity Based Encryption. By combining asymmetric encryption with Attribute Based Access Control (ABAC), this method makes it possible to implement a single encryptor/multi-decryptor environment with a single scheme. The implementation of Predicate Based Encryption is concentrated on Platform as a Service and Software as a Service. Additionally, this suggested method prevents unintended disclosure, unintended leaking, and other unintended breaches of cloud resident data confidentiality.

A novel authentication system that is appropriate for hybrid cloud services in mobile communication environments was proposed in the paper Secure Authentication System for Hybrid Cloud Service in Mobile Communication Environments [6]. Five server-side subcomponents make up the suggested system. Using RADIUS and the two-factor token technique, the first module verifies device authentication and external user authorization. Data integrity between the user and the mobile device access point is checked by the second module, a hash machine. The third part is Connect Manager. This module verifies the session between the user's mobile device and the hybrid cloud service server. The user manager comes in at number five. This module adds, removes, edits, and verifies user data, including ID, time stamp, and RND, in these databases. Lastly, the service manager module uses the attribute certificate technique to give users access to software cloud services. The outcome demonstrated that the suggested system could guarantee secrecy and integrity while supporting device and user authentication services. On the other hand, hybrid cloud services will offer very little authentication and security in a wired/wireless integrated network environment. This represents the work's primary research gap.

A novel application for protecting sensitive data on Android mobile devices was proposed by [9] using a current cryptographic technique and including biometric information into the algorithm. They believe that when it comes to storing data in the Dropbox cloud, fingerprint authentication can enhance the security of critical information. Android smartphones allow multiple users to access this data by supporting up to three distinct fingerprint scans. The main issue with this feature is that it makes it impossible for another remote user to access the encrypted data. Compared to other accessible security strategies in cloud computing, the AES method, which is used in the application to encrypt data, may be the most reliable and secure way to protect data in the cloud. While encryption keeps our data safe from unwanted access, it doesn't stop data loss, which is the loss of the keys that unlock our data.

In [7], a novel fine-grained two-factor authentication (2FA) access control system for web-based cloud computing applications was presented. To be more precise, their suggested 2FA access control solution uses an attribute-based access control mechanism that requires a lightweight security device in addition to the user secret key. Since a person cannot access the system if they do not possess both, this approach can improve system security, particularly in situations where multiple users share a single machine for web-based cloud services. Furthermore, attribute-based control in the system allows the cloud server to protect user privacy by limiting access to users who share the same set of attributes. A thorough security study reveals that the suggested 2FA access control system satisfies the necessary security standards. They proved the construction is "feasible" through performance evaluation. They depart as part of ongoing efforts to increase efficiency while preserving the system's lovely qualities.

A Hash-Based Method for Using Digital Signatures to Provide Privacy and Integrity in Cloud Data Storage cloud computing has been envisioned as the next phase of IT enterprise design, according to [8]. Data integrity is one of the numerous problems with cloud computing. Since this problem, many consumers are hesitant to embrace cloud technology since they cannot be sure that their data will be secure. Prior to this, a number of frameworks were put up to address this problem, but none of them offered complete security. Using the conventional network security techniques in cloud storage, the study suggested a signature scheme to improve efficiency and address the problem of user data integrity. Additionally, cost is minimized by the use of multiple cloud concepts and platforms for distinct categories.

[5] examined the state of security in cloud computing in 2015 and the ways in which various cloud providers have addressed the problem of user authentication when an individual wants to access a cloud service. A small percentage of users logged in using static passwords, while others utilized two-factor authentication with one-time passwords. Either approach fails to meet the requirements for affordability, flexibility, and security. They provide three distinct methods in their thesis for safely and conveniently utilizing OTPs and a user's mobile phone as an authentication

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24OCT1787

device to log in to a cloud service. Additionally, there have been three distinct approaches for registering new customers for the user-friendly and secure cloud service. In terms of speed and security, the optimal encryption technique for cloud services was assessed. The recommendations resulted in a functional solution that uses a very secure registration system, mobile OTP authentication for the login process, and RC4 encryption for all traffic transmissions. The approach is still user-friendly while offering users great security. It offers advantages over the two-factor and static password security systems currently in use for authentication. This approach differs significantly from others that use static passwords in that the password is only valid once, which is a significant security benefit. It has an edge over other cloud providers' two factor authentication solutions because the passwords are provided by the user's mobile device and the entire solution is built on open source technology. Given that millions of people utilize cloud services, security must be excellent to safeguard private information. It must also be quick, adaptable, and simple enough for users with varying levels of technological expertise to use. All of those goals are achieved with the authentication, registration, and encryption technique suggested and put into practice in this thesis. The time synchronization between the server and phone should be improved for further projects. Given that the OTP is only valid for three minutes and that time is a component of the hash that generates it, there can be no more than three minutes between the phone and the authentication server.

An introduction to dynamic mobile token applications were made in a paper presentation by [2] titled "Securing the Cloud Environment Using OTP." To generate a code using OTP (One Time Password), this smartphone application is utilized. You can only use this OTP code once to log in. They detail one of the OTP approaches in the study. It consists of two stages: the registration stage and the login stage. Before entering the login step, the user must first register by filling out the form with their credentials. An OTP will be generated during the login step. Three parameters—the current time, the four-digit PIN code, and the initial secret—are used to generate the OTP. This code is only good for the next three minutes. This guarantees defense against attacks by man-in-the-middle actors and eavesdroppers. They thereby demonstrate that OTP is quite safe.

[3] suggested combining One Time Passwords (OTPs) with hash encryption methods to create website and data storage solutions that are more secure. The newly proposed plan is simple to implement, has improved security, and has a low system overhead. Using two forms of identification—one usually a tangible token, like an application, and the other usually something that is learned, like a password or security code—is known as multi-factor authentication.

III. METHODOLOGY

The object-oriented analysis and design methodology (OOADM), a set of guidelines for system analysis and application design, was used in this project. It approaches information system design and analysis formally and methodically. In order to generate implementation specifications, analytical models are elaborated by object-oriented design (OOD). In contrast to other types of analysis, object-oriented analysis organizes requirements around objects that integrate states (data) and actions (processes) modeled after actual things that the system interacts with.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24OCT1787

IV. SYSTEM DESIGN AND IMPLEMENTATION

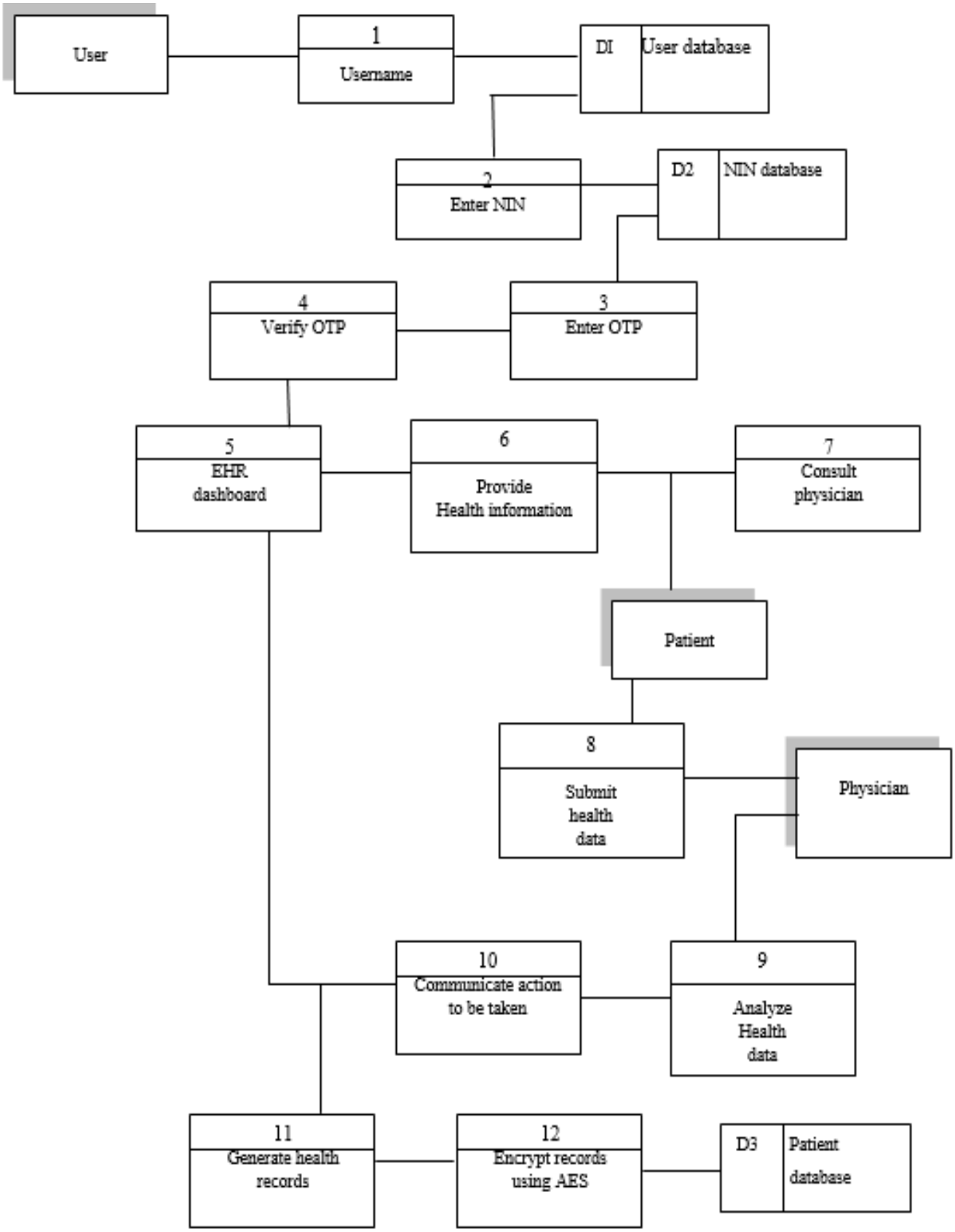

Fig 1: Data Flow Diagram of the New System

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24OCT1787

➢ *Activity Diagram for Security Model*

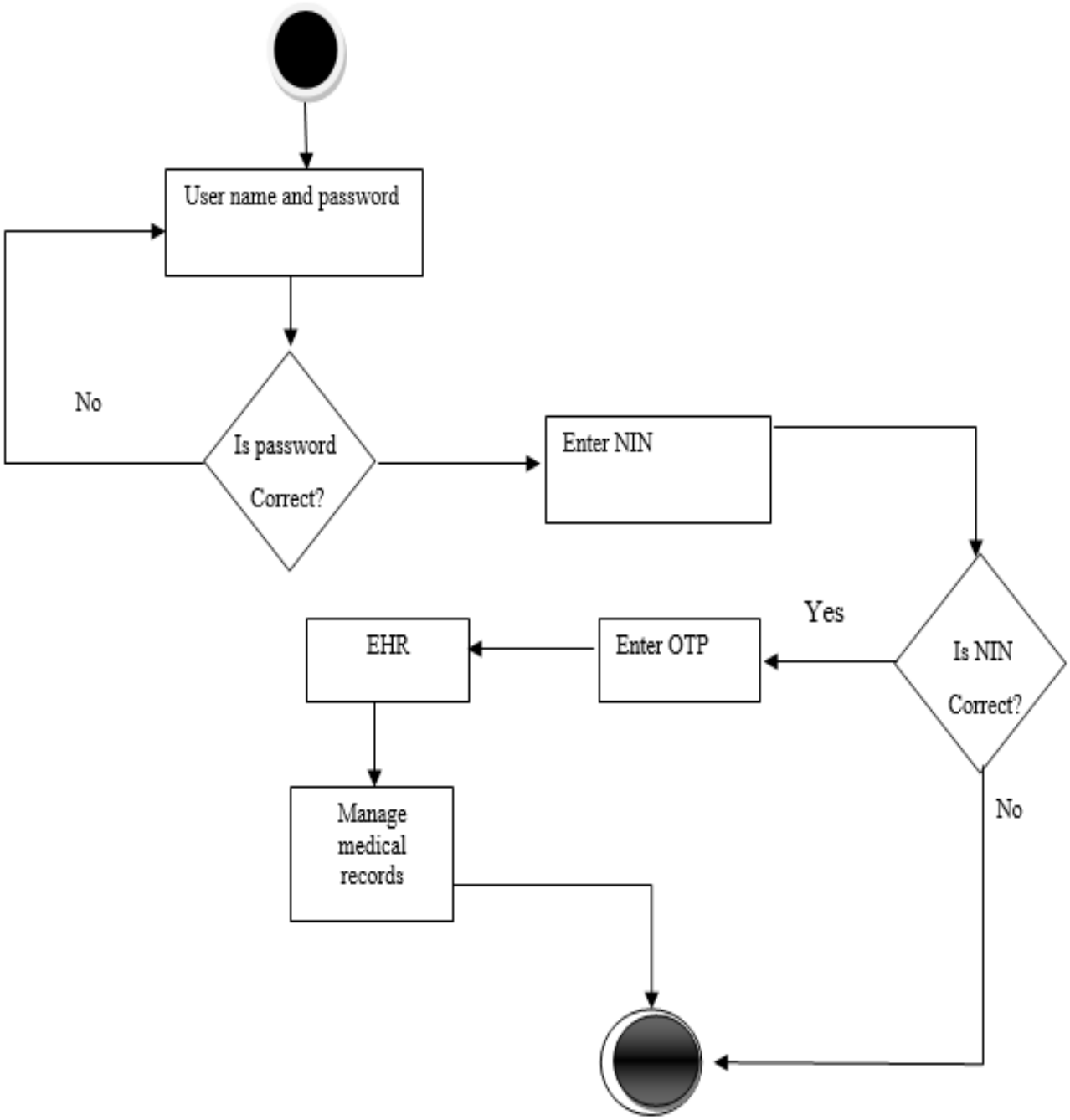

Fig 2: Activity Diagram of the security model

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24OCT1787

➢ *Sequence Diagram (Physician)*

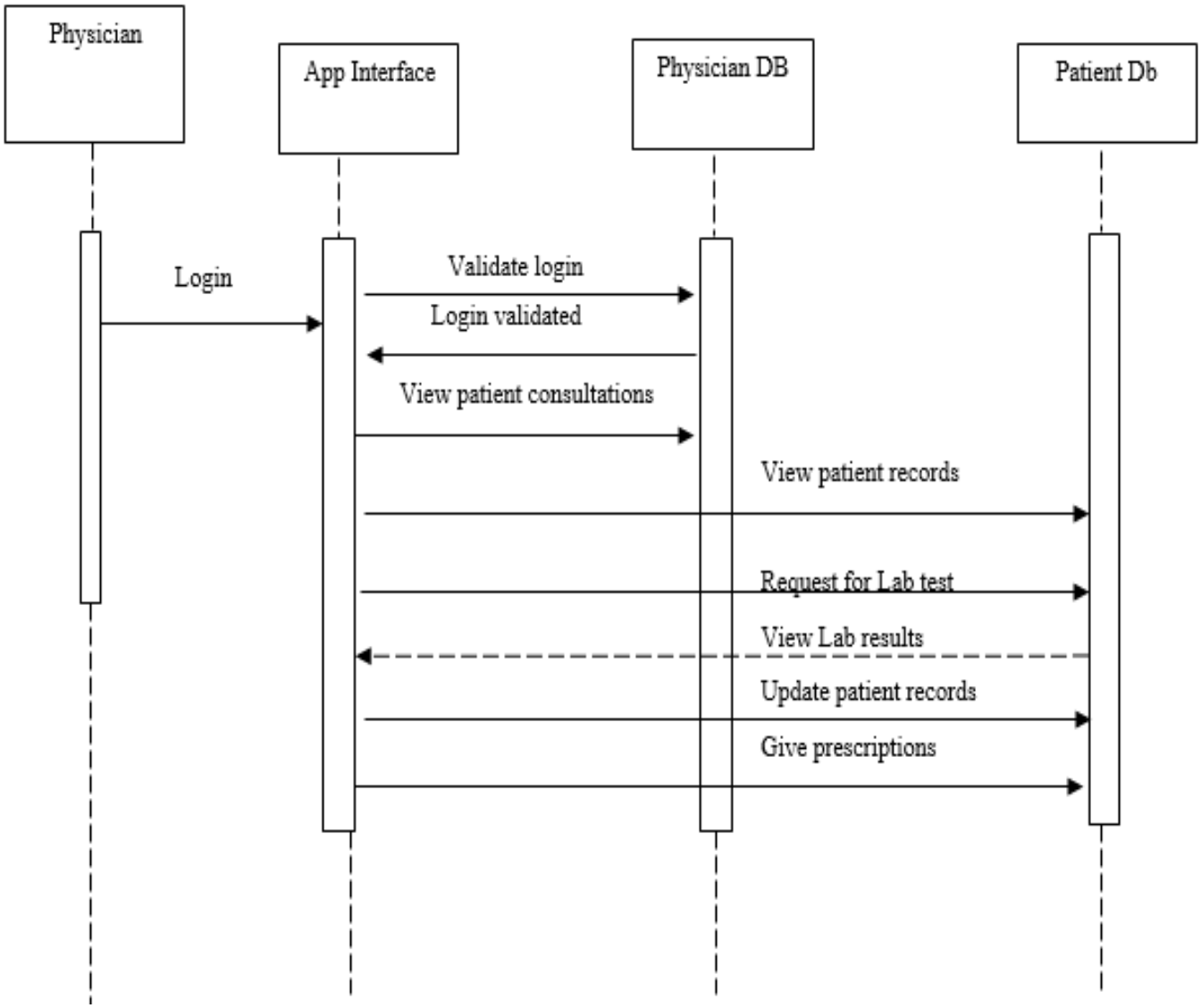

Fig 3: Sequence Diagram (Physician)

V. CONCLUSION

User credentials for first-, second-, and third-tier authentication are the main strength of this paper authentication technique. In order to gain access to the requested service, the attacker must breach every tier of authentication. The user's login credentials are validated at the initial level. By connecting to the NIN database and confirming the number supplied, the NIN is validated at the second tier. An OTP is delivered to the user's phone number at the third layer, and the user must enter it for final identification. Additionally, the cloud-based database's data was encrypted using the AES algorithm to further secure it. The electronic health records' data security is ensured by the aforementioned security measures.

REFERENCES

[1]. Sheridan, P.T., Meyers, S., Pech, E. (2013). Prussia, PA: Merion Matters: Advance for Health InformationProfessionals.*URL:http://healthinformation.advanceweb.com/Features/Articles/EHR-andHIM-Transitions-in-a- Time-of-Mergers-Part-1.aspx.*

[2]. Pandey, V. (2017). Securing the Cloud Environment Using OTP. *International Journal of Scientific Research in Computer Science and Engineering*

[3]. Niharika, G., Rama, R. (2015) Implementing High Grade Security in Cloud Application using Multifactor Authentication and Cryptography. *International Journal of Web & Semantic Technology (IJWesT) Vol.6, No.2,*

[4]. Muijnck-Hughes, J.(2019) Data Protection in the Cloud, 12 Jan, 2019 [Online], Available: http://www.ru.nl/ds

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24OCT1787

[5]. Markus, J. & Faruque, A.S.M (2015) Mobile One Time Passwords and RC4 Encryption for Cloud Computing. School of Information Science, Computer and Electrical Engineering Halmstad University

[6]. Jin-Mook, K. and Jeong-Kyung, M. (2014) Secure Authentication System for Hybrid Cloud Service in Mobile Communication Environments. *Division of Information Technology Education, Sun Moon University, No.100 Galsan-ri,Tangjeong-myeon, Chungnam.Asan-si336708,RepublicofKorea*

[7]. Joseph, K., Liu, M., Xinyi, H., Rongxing, L., Jin, L. (2020) Fine-grained Two-factor Access Control for Web-based Cloud Computing Services

[8]. N Gwotham, K., and Praveen Kumar Rao (2014) Hash Based Approach for Providing Privacy and Integrity in Cloud Data Storage using Digital Signatures: *International Journal of Computer Science and Information Technologies, Vol. 5(6), 2014, 8074 – 8078.*

[9]. Ivana, Kostadinovska (2016) Cloud Security – An approach with modern cryptographic solutions. A Thesis Submitted to the Faculty of Computer Science and Information Science in Partial Fulfillment of the requirements for the Degree of Master of Science, University of Ljubljana, Slovenia.