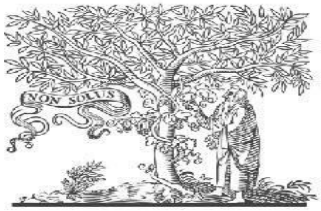
International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

# COPY RIGHT



ELSEVIER SSRN



IJIEMR Transactions, online available on 10th Apr 2023. Link :http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=Issue 04

**10.48047/IJIEMR/V12/ISSUE 04/99**

Title SECURITY IN E-HEALTH APPLICATION NETWORK SECURITY AND INFORMATION SECURITY

Volume 12, ISSUE 04, Pages: 799-806

Paper Authors

**Dr. Alla Kalavathi, M.Manjubhargavi, N.Harshini Sai, P.Ferdos, K.Naveena,P.Chandrika**


USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

# SECURITY IN E-HEALTH APPLICATION

## Network Security and Information Security

**Dr. Alla Kalavathi**[1], *M.Tech.Ph.D.*, Department of IT,
Vasireddy Venkatadri Institute of Technology, Nambur, Guntur Dt., Andhra Pradesh.

**M.Manjubhargavi**[2], **N.Harshini Sai**[3], **P.Ferdos**[4], **K.Naveena**[5],**P.Chandrika**[6]
[2,3,4,5,6]UG Students, Department of IT,
Vasireddy Venkatadri Institute of Technology, Nambur, Guntur Dt., Andhra Pradesh.
[1,2,3,4,5,6]kalavathi_alla@yahoo.com,mannepalli346@gmail.com,
harshisai599@gmail.com,patanferdos@gmail.com,naveenakondraganti@gmail.com,chandrikapatibandla666@gmail.com

**Abstract**

In today's world, The majority of hospitals keep electronic medical records since they are the primary repository for data on patient treatment. When the proof is needed to defend the service provider in relation to patient care, the medical record is helpful. The primary issue with current record management is that all of the records are kept centrally, meaning that all of the data is kept in one place. A third party or intruder has a greater chance of accessing and altering the data in such centralized storage systems. In this essay, we provide a website-based method to address this issue. The usage of e-Health applications has a significant positive impact on the country's healthcare system. When compared to manual methods, e-Health provides a wide range of e-health solutions to meet the needs of consumers' health problems everywhere, anytime, and at any age. Additionally, it offers remote access to particular data. This model contains PHP as the middle end, MYSQL connectivity, and HTML with CSS as the front end. E-Health is specifically designed to fulfill the needs of mid and large-size hospitals worldwide. The application is more extendable and user-friendly because of its database. From Patient Registration, Doctor, Admin, Patient Appointment, Record Modification, and all other pertinent modules, it is covered. Security measures like two-factor authentication and data encryption must be used in order to create such a system.

**Keywords:** Data Encryption, Two-step Authentication

**Introduction**

Several aspects of our daily lives have been impacted by the technological breakthroughs in the last few decades. We benefited from it in many areas of daily life, particularly in healthcare. In recent years, it has been noted that the healthcare sector has made considerable advancements. The majority of hospitals have their own record-keeping system. Several hospitals use cloud service providers or local databases to keep data locally. A hospital often owns or rents a server where the data is stored. Nevertheless, there are numerous problems with this sort of data storage,

including Data manipulation by hospital staff and unauthorised access to patient information. Healthcare systems may establish holistic views of patients, tailor therapies, devise treatment plans, encourage patient-physician contact, and enhance health outcomes thanks to data collecting. Healthcare data is extremely valuable because it comprises all of the patient's personal information, including name, medical history, lab results, and a variety of other details. This is why it's important to store healthcare data securely. The usage of telemedicine is a result of this pandemic. authentication using two factors. giving our application security. Every existing piece of data has been encrypted using the AES (Advanced Encryption Standard) to ensure the security of our project.

**2. Literature survey**

[1] - The user's registered mobile phone number receives an OTP as part of the proposed 2FA system's operation. To finish the authentication procedure, the user must input the OTP in addition to their login and password. The authors underline the security precautions used to prevent unwanted access while going into technical depth about how the OTP is produced and sent to the user's cell phone. [2] - In order to assess the security and adaptability of authentication and access control mechanisms in cloud-based e-health systems, the study suggests a 2FA architecture. The framework contains a 2FA technique for further protection, as well as a fine-grained data access control method that enables granular control over access to patient data. [3] - In the paper, a decentralized EMR system based on blockchain technology is suggested, enabling safe, open, and unchangeable record-keeping. The technical components of the system, including the use of smart contracts to enforce access control and data-sharing policies, are thoroughly explained by the authors. [4-5] - In order to guarantee the security and privacy of patient data, the paper suggests a framework that makes use of various levels of security measures, such as access control, encryption, and authentication techniques. The adoption of a secure key management system for data encryption and decryption is just one of the technical components of the framework that the authors thoroughly explain. [6] - The paper starts out by giving a general review of EHRs and the security and privacy issues they raise. The potential of blockchain technology to remedy these issues is then discussed. The authors suggest a decentralised network of nodes that can store and manage EHR data as part of a blockchain-based solution for EHR management. The system uses cryptographic methods to guarantee the confidentiality and accuracy of EHR data. [7] - The authors suggest a solution that includes encrypting the information in electronic health records, putting access control measures in place, and guaranteeing secure user interaction. They also suggest the use of two-factor authentication and biometric verification to ensure only

authorized individuals have access to the records. [8] - To guarantee the confidentiality and integrity of data, the suggested approach comprises steps including the use of encryption, access control, and authentication systems. Additionally, the authors recommend using backup and recovery protocols to guarantee that data will be accessible in the case of a catastrophe or system failure. [9] - The study offers a workable solution to the problems with authentication and access control in cloud-based e-health systems. It is a valuable resource for academics and professionals working in the healthcare IT industry, as well as for legislators and regulators interested in enhancing the security of e-health systems. [10] - To guarantee the secrecy and integrity of data, the suggested system uses cutting-edge cryptography methods like homomorphic encryption and secure multiparty computation. The authors also suggest using blockchain technology to offer an electronic health record storage solution that is safe and decentralised.

**3. Problem Identification**

The current system generates a lot of paperwork because it is heavily dependent on paper documents and forms. Maintaining sales and service records manually takes a lot of time. As the database grows, maintaining it will become a major undertaking. And of retrieving already-enrolled patient records from the current system may be challenging and time-consuming. Any disputant of the records in your system has no claim to the records' security. The earlier method does not supply any crucial detail of this type for someone who wants to check the specifics of the doctors who are currently available. All of this work is done manually by the receptionist and other operational staff, and there are many papers that need to be processed and taken care of. Physicians may find it difficult to recall all the many types of medications and treatment options available for diagnosis, which increases the risk that they would overlook better solutions that might be more suitable or beneficial for their patients' needs. Being a real-time project, it required website and data security to operate more efficiently. The flaws are utilised as ports of entry to launch an attack on that specific website. Cybercriminals are continuously looking for ways to weaken and exploit websites since it is a lucrative business for them to do so. This may entail a variety of strategies, including breaking into computer systems, obtaining private information, and deploying malware or phishing assaults. The potential impact of such attacks has expanded as the internet has become more essential to our daily lives, making it crucial for website owners to take proactive measures to defend their sites.

**4. Proposed Methodology**

The Telemedicine Service System is a suggested piece of software that would take the place of the existing paper-based patient information management system currently in use in hospitals. The existing technology is sluggish and unable to give

real-time updates on patient lists throughout the hospital's many departments.

The main objective of the Telemedicine Service System is to improve patient treatment accuracy while decreasing overtime compensation in order to boost the efficiency of patient care. Doctors will be able to swiftly and precisely retrieve and update patient records thanks to this technology, which will electronically store patient information. The system will also enable remote consultations using video conferencing and let doctors create patient lists based on a variety of parameters. The technology will also be able to collect patient histories and follow their development over time. It will also be able to issue electronic prescriptions to pharmacies.

Overall, it is anticipated that the Telemedicine Service System will improve patient care quality, increase hospital operational effectiveness, and lower the cost of overtime pay.

**4.1.Data Security**

The protection of data from illegal access, use, disclosure, destruction, or alteration is referred to as data security. Data is one of the most precious assets for both companies and people, making data security essential. A data breach can have serious repercussions, including lost revenue, reputational harm, and legal liabilities.

**4.1. Two-factor authentication**

Websites and online accounts are both protected by the two-factor authentication (2FA) security measure. With 2FA enabled, users are required to provide two types of verification to access their accounts. Even in the case that a hacker succeeds in obtaining the user's password, this aids in preventing unauthorized access.

The website's security can be considerably enhanced, and user data can be protected, by implementing 2FA. It's vital to keep in mind, though, that it could cause some people inconvenience and isn't always reliable. In addition to 2FA, it's still crucial to promote the use of strong passwords and other security precautions.

Email 2-factor authentication (2FA) is a security mechanism that gives your email account an additional degree of security. In addition to your standard email password, when email 2FA is activated, you will also need to provide a one-time, unique code that was either created by an authentication app or delivered to your phone or alternative email address, in addition to your regular email password.

**5. Implementation**

The system must offer continuously dependable services to let medical professionals carry out their daily tasks while having an intuitive user interface.

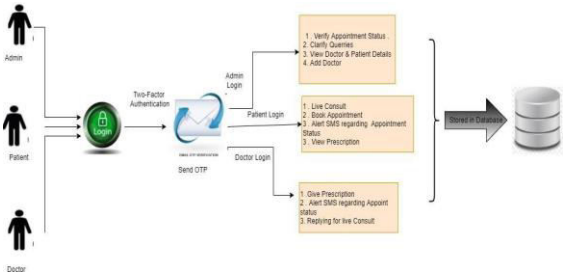



Fig 1. System Architecture

Figure 1 shows the system architecture for patients, doctors, and administrators to log into the website.

**Prerequisites**

To follow along the reader will need the following:

1. Xampp or MySql installed on your system.
2. A dataset should be available in the form of a CSV file.

**Description of Algorithms**

We utilize OpenSSL to encrypt the data in the database for e-health application security.

A variety of cryptographic operations, including symmetric encryption, public-key encryption, digital signatures, and hash functions, are offered by the widely used C library known as OpenSSL. These procedures are employed to guarantee the privacy and security of data sent over the internet. The Secure Socket Layer (SSL) protocol, which is a popular mechanism for safeguarding network connections, is also implemented by OpenSSL.

**Advanced Encryption Standard(AES):**

Websites can use the popular encryption algorithm AES (Advanced Encryption Standard) to prevent sensitive data from being intercepted or accessed by unauthorized parties. AES can be used to encrypt data such as passwords, credit card numbers, and other personal information when it is implemented on a website. This makes it more challenging for attackers to access the data while it is at rest and in transit. To use AES on a website, the data must first be encrypted using an encryption key. The encrypted data is then sent over the internet to the website's server, where it is stored securely. When the data is needed again, it is retrieved from the server and decrypted using the same encryption key.

It's important to note that while AES can provide a high level of security for data, it is not a foolproof solution. Websites must also implement other security measures, such as secure connections (HTTPS), strong password policies, and user authentication, to ensure that data is protected from all angles.

Fig 2 shows the AES structure.

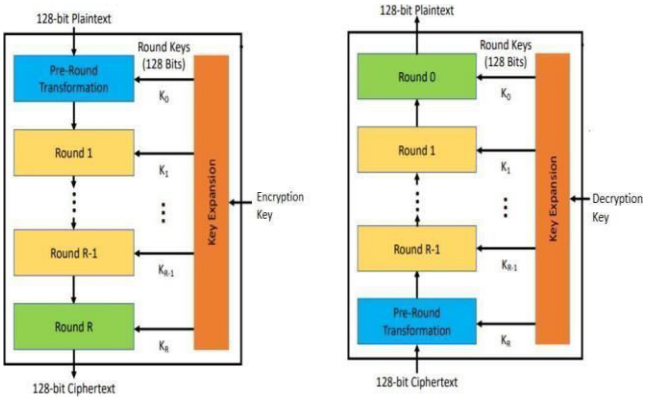



Fig.2.AES Structure

**AES Algorithm**

**Input**: Plain text

**Output:** Cypher text

1. Change the plain text's format to one that uses hexadecimal numbers.

2. The column-wise 4*4 state array will be filled using the hexadecimal format.

3. Building a 4 by 4 state array.

[[0 for x in range(4)]] in the state array x in the range(4)]

I in range(4): block = range(256); j in range(4):

Block[32*i + 8*j:32*i + 8*(j+1)] = statearray[j][i]

4. For encryption each round consists of four steps

1. Replace bytes 2. shift rows 3. combine columns 4. add round key

5. After the encryption operation we achieve ciphertext

6. Using the ciphertext as a decryption side input

7. Each cycle of decryption entails the following four processes.

Rows with an inverse shift 2. Inverted replacement bytes 3. Add round Key Fourth, reverse mix columns

8. Achieve plain text as the output

**Simple Mail Transfer Protocol(SMTP)**

Figure 3 shows the model of the SMTP protocol. SMTP is a protocol used for sending and receiving email messages between servers.

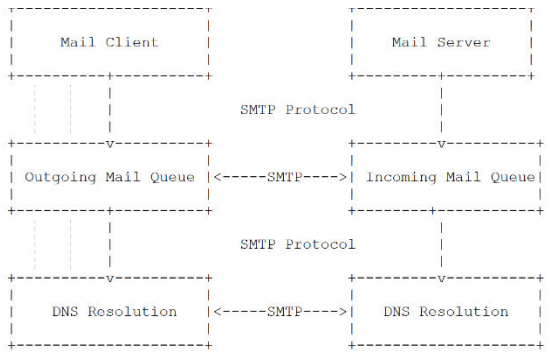



Fig.3.Model of SMTP system

In this diagram, we have two main components: the Mail Client and the Mail Server. While the Mail Server receives and delivers email messages, the Mail Client composes and sends email messages.

The Mail Client composes an email message and places it in the Outgoing Mail Queue. The SMTP Protocol is used to transfer the email message from the Outgoing Mail Queue to the Incoming Mail Queue of the Mail Server.DNS Resolution is used to identify the recipient's email server, and the SMTP Protocol is used to transfer the message to the recipient's Incoming Mail Queue.

The recipient's Mail Client retrieves the message from the Incoming Mail Queue.

Each step in the process involves specific SMTP commands and responses, as well as DNS queries and responses, to ensure successful message transmission.

Php Mailer

1.$mail->SMTPDebug = 2;

2.output $mail->isSMTP();

3.$mail->Host = 'smtp.gmail.com;

4.$mail->SMTPAuth = true;

5.$mail->Username = 'user@gfg.com';

6.$mail->Password = 'password';

7. $mail->SMTPSecure = 'tls';

8.$mail->Port = 587;

**Datasets and Tools**

Database design is a crucial process that involves creating a detailed blueprint of a database system. The design includes the logical and physical design choices as well as the physical storage parameters necessary to generate a data definition language that can be used to build the database. The goal is to create a fully attributed data model that includes detailed attributes for each entity. The phrase "database design" can be used to describe a variety of features of the overall database system, but it primarily refers to the logical layout of the fundamental data structure that holds the data.

In a relational database design, the data is organised into tables consisting of rows and columns. A Relational Database Management System (RDBMS) is an excellent tool for organising large amounts of data and defining the relationship between the datasets consistently and understandably. An RDBMS provides a structure that is flexible enough to accommodate almost any kind of data. Relationships between the tables were built by generating unique columns (keys), which contain the same set of values in each table. The tables can be joined in different combinations to extract the needed data.

These are the tables and views in the relational model. Entities and relationships in an object database map directly to object classes and named relationships, posing threats to the Openssl algorithm and encryption. However, the term database design typically refers to the process of creating the base data structure used for storing data, it can also refer to the overall process of designing the entire database system, including the forms, queries, reports, and other user interfaces used to interact with the data.

In addition to creating the tables and fields that make up the base data structure, a comprehensive database design process should also include the design of user interfaces that allow users to view and manipulate the data. This may involve designing forms for data entry and editing, as well as designing queries and reports to extract data from the database for analysis and reporting purposes.

**6. Results & Conclusion**

In a risky online environment, the proposed E-Health Application model places security first. Cyber attacks, such as denial of service attacks, can bring down websites, show malicious content, and hack into users' personal information, placing them at risk of both financial and personal harm. The system incorporates telemedicine services, which make it possible for patients to get clinical care from doctors without having to travel to a physical location. The AES encryption method and two-factor authentication, which uses both password-based and email-based OTP to offer an additional layer of security, are utilised to ensure security. In conclusion, the model offers strong security safeguards to safeguard private patient information and uphold the integrity and confidentiality of the E-Health Application.

**7. Limitations & Future Scope**

Future improvements to the proposed work's effectiveness and security are conceivable. These upcoming extensions consist of:

Creating enhanced email security features: To safeguard the system against hazardous emails sent by the sender, complex email security mechanisms can be designed and integrated into the system. This would enable the system to detect and block any emails that are considered a security threat, thus improving the overall security of the system.

Including extra features on the website: The website can be enhanced by adding new features to boost its usability and functionality. For example, new features such as online appointment booking, patient feedback and reviews, and online payment options can be introduced to the website to make it more convenient and user-friendly.

Improving security measures: Further security measures could be put in place in the future to offer better protection. This could involve adopting multi-factor authentication, conducting frequent security audits, and educating staff members on the most recent security procedures. This would make it easier to maintain the system's security and safeguard it against security threats.

**References**

1. "OTP-Based Two Factor Authentication Using Mobile Phone," IEEE, by Mohamed Hamdy Eldefrawy and Khaled Alghathbar.

2. Authentication and Access Control in e-Health Systems in the Cloud(2016),IEEE. Nafiseh Kahani and Khalid Elgazzar.

3. C. Thimmaiah, S. Disha, D. Nayak, B. Diya, and H. Gururaj, "Decentralized Electronic Medical Records," *International Journal of Research and Analytical Reviews,* vol. 6, no. 1, pp 199-203, 2019.

4. Improved e-health framework for security and privacy in the healthcare system, presented at the 2016 Sixth International Conference on Digital Information Processing and Communications in Beirut, Lebanon.

5. "Security & Privacy-Preserving Problems in e-Health Systems Utilizing Cloud Computing," Chenthara, K. A. H. W. a. F. W. S., IEEE, vol. 7, pp. 74361-74382, 2019.

6. Y. Sharma and B. Balamurugan, "Preserving privacy of electronic health records utilizing blockchain," in Procedia Computer Science, vol. 173, 2020, pp. 171–180.

7. In the International Conference on Computer, Information and Telecommunication Systems (CITS), Alsace, Colmar, France, 2018, J. V. et al., "Ensuring Privacy and Security in E-Health Records,"

8. E-Health and Bioengineering Conference (EHB), 2017, pp. 721–724; "A security strategy for health care information systems";

9. Kahani, N., Cordy, J. R., & Elgazzar, K. (2016, April). E-health system authentication and access control in the cloud, IEEE (2016).

10. Kavitha, G.; Sonya, A. (2021). Cloud environment with advanced cryptography and a blockchain for secure electronic health records.