Chapter 9
A Security and Privacy Validation Methodology for E-Health Systems Using Cloud Storage

Aparna Datta
https://orcid.org/0009-0006-2552-9017
Meghnad Saha Institute of Technology, India

Sanchayan Sen
Meghnad Saha Institute of Technology, India

ABSTRACT

E-Health applications enable one to acquire, process, and share patient medical data to improve diagnosis, treatment, and patient monitoring. Despite the undeniable benefits brought by the digitization of health systems, the transmission of and access to medical information raises critical issues, mainly related to security and privacy. This paper describes a safe e-health data management system that employs the MERN stack (MongoDB, Express, React, and Node.js) and strong encryption algorithms. The solution improves security by using client-side encryption with the AES-256-CBC technique to encrypt e-health files before uploading them to MongoDB. To improve security, encrypted files and keys are stored separately. User authentication employs bcryptjs for password hashing and JSON Web Tokens (JWT) for permission, ensuring that only authorized users can access and decrypt data. The study demonstrates the efficiency of coupling MERN stack development with encryption in protecting sensitive patient information, establishing confidence, and boosting the adoption of e-health solutions.

DOI: 10.4018/979-8-3693-9235-5.ch009

INTRODUCTION

E-Health Data, also known as Electronic Health Data, is any digital information relating to a person's overall health. These data include but are not limited to records or imaging relating to the person's health. Such data range from:

- Medical records that may consist of a person's past medical history, diagnoses, procedures, prescribed medications, allergies or side effects of the medication, immunizations, as well as a variety of laboratory tests such as blood tests, urine tests, and many others.
- Patient monitoring data mainly include data or vital signs of a person such as heart rate, blood pressure, oxygen saturation, and others. These data can be measured or obtained through different means and devices, as hospitals and clinics have monitoring devices, and nowadays many people can acquire, through which vital signs, through daily life at home, can be measured and recorded in real time through monitoring devices or nowadays through wearable devices that measure it all day. It is also used in some measurement devices that measure sugar through the body without the need for a blood test.
- Imaging data or radiological examinations include X-rays, CTs, and MRIs stored in digital forms.
- Genomics data, which include data related to DNA sequencing in the field of personalized medicine.
- Lifestyle data, such as data related to the person's amount of activity, amount and quality of sleep or weight, all of which can be obtained through the use of wearable technology such as different watches and bands as Fitbit.
- Self-reported outcomes from patients, which include data that the patient self-reports regarding their health such as the extent of the disease, symptoms, and health effects on them.

Historical Incidents of E-Health Data Breaches

The use of e-health data is increasing, and that makes it a target for cybercriminals. Here are some of the historical incidents that show the need for better security and why we should not make the same mistake:

- ***Anthem (2015):*** The attack has leaked personal information of around 78 million health insurance customers associated with Anthem. The affected data has touched upon such points as names of the clients, their social security, addresses, information about birth, and the place of work for these users. It was one of the most devastating data breaches that have occurred, which