COST-EFFECTIVE AND EFFICIENT PRIVACY FRAMEWORK BASED ON CRYPTOGRAPHIC TECHNIQUES FOR E-HEALTH SYSTEMS BUILT ON EMPIRICAL CASE FINDINGS.

Manthrige Lalendra Jerome Dias

A dissertation submitted in partial fulfilment of the requirement for
Master of Science degree in Cybersecurity and Forensics

School of Computing

Informatics Institute of Technology, Sri Lanka

in collaboration with

University of Westminster, UK

2023

Abstraction

The central issue at hand revolves around the pervasive problem of distrust and concerns surrounding Health Information in the Sri Lankan Health Sector. Presently, the data is stored within databases, and the transmission of this data occurs in plaintext, rendering it susceptible to unauthorized access. Individuals possessing the necessary knowledge and expertise can effortlessly extract valuable and sensitive information pertaining to a patient's health without obtaining their consent. This glaring lack of security presents a significant challenge in upholding patient privacy and confidentiality.

The primary objective of this research is to bolster the security of E-Health systems in Sri Lanka by carefully selecting an appropriate algorithm that can be implemented without hardware constraints. The primary focus lies in addressing specific security challenges confronted by E-Health systems while ensuring compatibility with the existing hardware infrastructure. The goal is to fortify the overall security of E-Health systems, safeguard patient data, and establish a secure environment for data transmission. By enhancing the client-server architecture with the selected algorithm, potential risks and vulnerabilities can be mitigated, leading to a substantial improvement in healthcare information security throughout Sri Lanka.

Moreover, the research also dedicates attention to rectifying patient privacy concerns, managing the flow of data, and alleviating distrust in E-Health solutions prevalent in Sri Lanka. The study endeavors to develop a comprehensive approach that considers the cultural, social, and regulatory aspects of the country while ensuring the secure and confidential handling of patient data. This entails gaining an understanding of the cultural and social factors that contribute to the prevailing distrust, engaging with stakeholders to glean valuable insights, and formulating tailored security measures and privacy-preserving techniques. The research places significant emphasis on fostering open communication and collaboration among stakeholders to establish trust and transparency, taking into careful consideration the cultural sensitivities and concerns of the Sri Lankan population. The overarching objective is to establish secure and culturally sensitive E-Health systems that resonate with the unique context of Sri Lanka.