Chapter 56
Artificial Bee Colony-Based Approach for Privacy Preservation of Medical Data

Shivlal Mewada
https://orcid.org/0000-0001-5543-8622
Mahatma Gandhi Chitrakoot Gramodaya Vishwavidyalaya, India

Sita Sharan Gautam
Mahatma Gandhi Chitrakoot Gramodaya Vishwavidyalaya, India

Pradeep Sharma
Government Model Autonomous Holkar Science College, India

ABSTRACT

A large amount of data is generated through healthcare applications and medical equipment. This data is transferred from one piece of equipment to another and sometimes also communicated over a global network. Hence, security and privacy preserving are major concerns in the healthcare sector. It is seen that traditional anonymization algorithms are viable for sanitization process, but not for restoration task. In this work, artificial bee colony-based privacy preserving model is developed to address the aforementioned issues. In the proposed model, ABC-based algorithm is adopted to generate the optimal key for sanitization of sensitive information. The effectiveness of the proposed model is tested through restoration analysis. Furthermore, several popular attacks are also considered for evaluating the performance of the proposed privacy preserving model. Simulation results of the proposed model are compared with some popular existing privacy preserving models. It is observed that the proposed model is capable of preserving the sensitive information in an efficient manner.

DOI: 10.4018/978-1-7998-8954-0.ch056

1. INTRODUCTION

In last two decades, there is tremendous growth in the field of medical data science. Large number of e-healthcare systems are developed for the help of practitioners, hospital management and doctors. The main task of these system is to process the medial and health care data for finding meaningful information (Wang et al., 2015). Nowadays, cloud computing paradigm is widely adopted in healthcare for transferring and storing the data at cloud layer. Moreover, cloud computing provides pervasive data access for on demand services with reduced cost Wang et al., (2015); Zhang et al., (2014). It is also seen that electronic health records (EHR) are widely used for improving health of patients in different healthcare and medical services Gardner et al., (2013). These systems determine the need of patients on the basis of medical assembling and information relationship. A multi-disciplinary team of specialist and professional can access the information and provide a clear and structured description with minimized medical errors. It is observed that during the communication process, some security threats such as privacy, security, confidentiality are one of the major concerns of the users (Majeed, 2019; Wang et al., 2012). These threats can increase when information is outsourced from individual user account or cloud (Demir & Tugrul, 2018; Wang et al., 2018). General procedure for securing the medical data is to encrypt the medical data before sending Perera et al., (2011); Tamersoy et al., (2012). The encryption of data also having some performance issues such as cost of communication, computational complexity, maintenance etc. One of the possible solution of aforementioned problems is data anonymization (Gao et al., 2017; Poulis et al., 2017). It can be described as data sanitization and it can be acted as privacy preserving. Privacy preserving can be described as the process of encrypting or hiding the sensitive information from the dataset prior to communication. It can be achieved through concealed or mask data or arbitrary sequence of data. Through this, privacy of information or data can be preserved by minimizing the link to sensitive data or individual information. Hence, anonymization process can be beneficial for privacy of data that ensure the protection of individual end user data Newhauser et al., (2014). Most of anonymization algorithms work in two steps (Li et al., 2010; Otgonbayar et al., 2018). In first step, tuple troops are designed which can optimize the utility and privacy of data and further, imposes an anonymization principle. In second step, k-anonymity is considered as privacy measure (Amin et al., 2016; Zhao et al., 2018). Various optimization methods are used to develop anonymization algorithms. These algorithms can be described as single objective, multi objective and constrained algorithms. The objective of these algorithm is to attain supreme utility and privacy of sensitive information or data. But, none of algorithm can maintain utility and privacy preserving of information as desired. Hence, there is a need for an effective anonymization model to preserve the medical data.

1.1 Contribution and Scope of the Paper

The main contribution of this paper is to develop a privacy preserving model for medical data. The proposed model focuses on sanitization and restoration process of sensitive information. The aim of proposed privacy preserving model is to determine the optimal key for hiding the information. The main contribution of the paper is summarized as below.

- To proposed a privacy preservation model for medical datasets.
- To generate the optimal key for sanitization process using ABC based algorithm.
- Restoration analysis and attack analysis are adopted to assess the performance of proposed model.