A Behavioral Trust Model for Internet of Healthcare Things using an Improved FP-Growth Algorithm and Naïve Bayes Classifier

Saiful Azad[1], Amin Salem Saleh[2], Mufti Mahmud[3], M. Shamim Kaiser[4], Md. Saefullah Miah[2]
[1]Department of Computer Science and Engineering, Green University of Bangladesh, Dhaka, Bangladesh
[2]Faculty of Computing, College of Computing & Applied Science, University Malaysia Pahang, Malaysia
[3]Department of Computer Science, Nottingham Trent University, Clifton, NG11 8NS Nottingham, UK
[4]Institute of Information Technology, Jahangirnagar University, Savar, 1342 Dhaka, Bangladesh
Email: sazadm684@gmail.com, mufti.mahmud@ntu.ac.uk, mskaiser@juniv.edu, md.saefullah@gmail.com

2021 3rd International Conference on Sustainable Technologies for Industry 4.0 (STI) | 978-1-6654-0009-1/21/$31.00 ©2021 IEEE | DOI: 10.1109/STI53101.2021.9732588

***Abstract*—Healthcare 4.0 has revolutionized the delivery of healthcare services during the last years. Facilitated by it, many hospitals have migrated to the paradigm of being smart. Smartization of hospitals has reduced healthcare costs while providing improved and reliable healthcare services. Thanks to the Internet of Healthcare Things (IoHT) based healthcare delivery frameworks, integration of many heterogeneous devices with varying computational capabilities has been possible. However, this introduced a number of security concerns as many secure communication protocols for traditional networks can not be verbatim employed on these frameworks. To ensure security, the threats can largely be tackled by employing a Trust Management Model (TMM) which will critically evaluate the behavior or activity pattern of the nodes and block the untrusted ones. Towards securing these frameworks through an intelligent TMM, this work proposes a machine learning based Behavioral Trust Model (BTM), where an improved Frequent Pattern Growth (*i*FP-Growth) algorithm is proposed and applied to extract behavioral signatures of various trust classes. Later, these behavioral signatures are utilized in classifying incoming communication requests to either trustworthy and untrustworthy (trust) class using the Naïve Bayes classifier. The proposed model is tested on a benchmark dataset along with other similar existing models, where the proposed BMT outperforms the existing TMMs.**

***Index Terms*—Internet of things, secure healthcare framework, FP-growth algorithm, Naïve Bayes classifier.**

I. Introduction

Internet of Healthcare Things (IoHT) [1] aims to facilitate the ministration of care services to patients through improved analytics of gathered health data to expedite the healthcare decision making and service delivery process. It also assists healthcare professionals by taking off some workload through (semi-)automated remote monitoring of patient health, their treatment progress, etc. [2]. According to an estimation reported in [3], despite being slow in adopting new technologies, the healthcare sector will observe an incredible growth of 50 million connected devices worldwide by 2021.

Since these devices are connected to the global information superhighway for their ubiquitous access, they are targeted by many bandits. This vulnerability is even exacerbated, in comparison to the conventional network, as most of these IoHT frameworks (IoHTF) are comprised of heterogeneous devices with varying computational and memory capabilities to which many existing secure communication protocols can not be verbatim applied. To the rescue of such a situation, a Trust Management Model (TMM) can be additionally employed alongside the communication protocols to tackle these threats and attacks by exploiting the activity patterns of the connected devices [4], and hence, is the focus of this paper.

Over the last years, several TMMs have been proposed targeting different applications [5], [6], [7]. However, one of the major drawbacks of many of these available models is that, they are unable to adapt to the dynamically evolving threat profiles. An effective TMM is required to learn about the evolving threat profiles and automatically account for those changes and adapt its safeguarding strategy. It is, therefore, imperative to teach the TMM these dynamic threat profiles and set the retaliation strategy on whether or not to authorise specific connection requests. To partially achieve this, several intelligent models have been proposed in the literature.

Among the existing ones, an Adaptive Neuro-Fuzzy Inference System based trust model targeting Neuroscience applications has been proposed in [4] which suffers from low accuracy in a generalized scenario. Another trust model for pervasive computing based on Apriori association rules learning (AARL) and Bayesian classification has been proposed in [8]. Limitations of the AARL methods is well-known (see [9]) and scalability is a major one. That is, when the size of a database becomes large, the AARL algorithm fails to fit it into the memory, warranting a large number of memory reads in each iteration of the algorithm. In such scenarios, the Frequent Pattern Growth (FP-Growth) algorithm performs better as it scans a database only twice in comparison to the AARL algorithm which scans the transactions in each iteration. Moreover, the FP-Growth algorithm extracts more relevant frequent patterns (also referred as behavioral signatures) and their respective association rules over AARL [10]. This work improved the standard FP-Growth algorithm to reduce the execution time in exploring the behavioral signatures of the devices and classify them to appropriate trust classes using the Naïve Bayes classifier.

978-1-6654-0009-1/21/$31.00 ©2021 IEEE