جامعة محمد الخامس بالرباط
Université Mohammed V de Rabat

École Nationale Supérieure d'Informatique et d'Analyse des Systèmes
Centre d'Études Doctorales en Sciences des Technologies de l'Information et de l'Ingénieur

AVIS DE SOUTENANCE DE THÈSE DE DOCTORAT

Monsieur Driss EL MAJDOUBI

Soutiendra publiquement sa thèse de Doctorat en Informatique

Le Vendredi 10 Mars 2023 à 16H00 au Grand amphi à l'ENSIAS

Intitulé de la thèse

A SMART BLOCKCHAIN-ENABLED END-TO-END LEGAL COMPLIANT SUSTAINABLE APPROACH FOR TRUST, SECURITY AND PRIVACY IN SMART HEALTHCARE ENVIRONMENTS

Devant le Jury composé de :

Président :

Pr. Faissal El Bouanani, PES, ENSIAS, Université Mohammed V de Rabat

Directeur de thèse :

Pr. Hanan El Bakkali, PES, ENSIAS, Université Mohammed V de Rabat

Rapporteurs :

Pr. Nidal Nasser, Professor, Alfaisal University, Kingdom of Saudi Arabia

Pr. Abdellatif Kobbane, PES, ENSIAS, Université Mohammed V de Rabat

Pr. Abdelhamid Belmekki, PH, Institut National des postes et télécommunications, Rabat

Examinateur :

Pr. An Braeken, Associate Professor, Vrije Universiteit Brussel (VUB), Belgium

UNIVERSITE MOHAMMED V - RABAT
ENSIAS

Abstract: Digital technologies are part of a long line of innovations in public health that have been fundamentally integral to disease prevention and containment strategies for centuries. Public health has been slower to embrace digital innovations compared to other sectors. However, the unprecedented humanitarian and economic needs presented by the COVID-19 pandemic have driven many governments to take advantage of new technological advances (e.g, AI, Cloud, BigData), moving them faster toward smart healthcare. This shift has brought new challenges to software engineers related to data Trust, Security, and Privacy (TSP) management, restrictive laws and regulations, in addition to technological complexity and heterogeneity. From a societal perspective, citizens' lack of trust in such smart services and their perception of the way public health authorities (PHAs) and other stakeholders store and process their data, as well as the lack of transparency, represent a bottleneck to the wide adoption of smart healthcare applications. On the other hand, from a technical perspective, multiple organizations (PHAs, cloud providers, external services) might be required to handle patients' sensitive data differently. This raises serious concerns regarding the accountability of the involved stakeholders. The existing TSP engineering frameworks and models do not support a multi-level (organizational, threat, and business process) analysis of TSP issues, nor do they enable PHAs to take patients' preferences and data protection laws into account so as to make their services transparent. Furthermore, they fail to combine such analyses with autonomy and scalability while ensuring high performance and energy efficiency.

In this context, we designed and developed a smart Blockchain-enabled End-to-End (e2e) sustainable framework for trust, security, and privacy in smart healthcare environments that leverages the power of AI and Blockchain to provide solutions to both societal and technical challenges discussed above. We present here our research journey to our proposed e2e framework.

We begin with an overview of our framework, its stakeholders, TSP threats, and requirements. Considering its core functional requirements, we design a layered flexible, and service-oriented Macro-architecture deploying several components. Then we take an incremental approach in developing and testing individually the selected key components of the security architecture through three milestones.

The first one consists of ensuring data TSP law compliance through a new semantic ontology-based approach. As the patient does not have enough experience and expertise in TSP domains to take advantage of his/her legal rights, semantic modeling becomes fundamental to inferring the required TSP obligations. To this end, the proposed approach enables the automatic incorporation of data protection laws and regulations while considering both patients' preferences and service providers' policies. It also allows the generation of a common TSP Agreement (TSPA) between the patient and the service provider based on a TSP Agreement

Generation Algorithm. (TSPAGA). Still, this approach cannot fully enforce the TSPA. That was our motivation for the two next milestones.

In the second milestone, we used Blockchain technology, the PV-SAS-MCA Message Cross-Authentication Protocol based on Short Authenticated Strings (SAS), and Elliptic Curves Light-weight Cryptography (ECLC) to design a new decentralized trust establishment protocol. This protocol is, indeed, the first line of defense on the way to the enforcement of the TSPA. More specifically, it leverages the ECLC for digital certificate generation so as to address smart devices' constrained storage and processing capabilities. Besides, it is the first to use Blockchain as an extra distributed and authenticated channel to exchange SASs without physical interaction. This helps entities in smart environments not only to identify each other but also to exchange their public keys in a secure manner. Experimental results reveal that the time required to complete the authentication process is less than 90 ms which is a superior performance when compared to state-of-the-art decentralized authentication mechanisms.

In the third milestone, we leveraged the two previous contributions and complemented them by dealing with the security and privacy issues related to the targeted e2e framework. Correspondingly, we designed a Multi-Channel Blockchain-based framework that guarantees the TSPA self-enforcement throughout the life cycle of healthcare data, including the phases of data collection, sharing, processing, and storage. This Framework relies on Smart Contracts for data fine-grained access control and data usage auditing, as well as an Homomorphic Encryption-based Group-level data aggregation mechanism for data processing. Although experiment results have proven the functional effectiveness of this framework in a realistic scenario, the consensus protocol efficiency overhead was not acceptable. We were expecting these poor performance results, and we considered them a great opportunity for improvement. That was the whole purpose of the last milestone, in which Smart Blockchain, an AI-powered extension of blockchain technology, was identified as an effective and efficient solution for these challenges. On this basis, we introduced the S4DP Ledger : A smart ledger driven by a new Blockchain dilemma model aiming to optimize security, scalability, sustainability, decentralization, and performance Then, as a core part of S4DP Ledger, we designed Smart Proof of Maturity and Honesty: a novel consensus protocol in which only trustworthy nodes are allowed to insert new blocks in the chain. To this end, SPoMH leverages Machine Learning and uses a multidimensional trust evaluation model relying on a maturity-based supervised classifier and a multi-level outlier-based intrusion detector. SPoMH is also backed by optimized information exchange combining a tree topology with unicasting-enhanced gossiping, as well as by specifically-designed data structures for Blockchain transaction and state management.

Simulation results show that SPoMH's throughput scales linearly with the number of active masternodes, supporting Visa-level workloads and beyond, while confirming transactions in under

2 seconds as well as drastically reducing energy consumption and CO2 footprint by more than 99% in comparison with existing energy efficient consensus protocols.

Keywords: Trust, Security, Privacy, Law Compliance, TSP Agreement, Smart Healthcare, Smart Blockchain, Smart Ledger, Smart Blockchain Pentalemma, Outlier-based Intrusion Detection, Homomorphic Encryption, Bloom Filter, IPFS, Supervised Classification, Lightweight ECC, Data Protection Laws, Ontology, Consensus Protocol.

.