Blockchain and Physically Unclonable Functions Based Mutual Authentication Protocol in Remote Surgery within Tactile Internet Environment

Tarik Hidar [1 †] and Anas Abou el kalam[2 † †], Siham Benhadou[3 † † †], Yassine Kherchttou[4 † † † †]
Hidar.tarik@gmail.com a.abouelkalam@uca.ac.ma benhadou.siham@gmail.com yassine.kherchttou@edu.ac.ma
LISER-IPI, LRI-ENSEM, Hassan II University, IPI Paris-France, Casablanca-Morocco[1†]
ENSA Team Laboratory, Cadi Ayyad University, Marrakesh, Morocco[2††]
LRI-ENSEM, Hassan II University, Casablanca, Morocco[3†††]
Critical care and anesthesia department, Mohammed VI University Hospital Center, Marrakesh, Morocco[4††††]

Summary
The Tactile Internet technology is considered as the evolution of the internet of things. It will enable real time applications in all fields like remote surgery. It requires extra low latency which must not exceed 1ms, high availability, reliability and strong security system. Since it appearance in 2014, tremendous efforts have been made to ensure authentication between sensors, actuators and servers to secure many applications such as remote surgery. This human to machine relationship is very critical due to its dependence of the human live, the communication between the surgeon who performs the remote surgery and the robot arms, as a tactile internet actor, should be fully and end to end protected during the surgery. Thus, a secure mutual user authentication framework has to be implemented in order to ensure security without influencing latency. The existing methods of authentication require server to stock and exchange data between the tactile internet entities, which does not only make the proposed systems vulnerables to the SPOF (Single Point of Failure), but also impact negatively on the latency time. To address these issues, we propose a lightweight authentication protocol for remote surgery in a Tactile Internet environment, which is composed of a decentralized blockchain and physically unclonable functions. Finally, performances evaluation illustrate that our proposed solution ensures security, latency and reliability.

Keywords
Tactile Internet, Mutual Authentication, Physically unclonable functions, blockchain, remote surgery.

1. Introduction

Internet has known many transformations in the last 20 years; it passed from human-to-human relationship, by implementing mobile communication, machine-to-machine relationship with the integration of internet of things and human to machine relationship as an evolution of the internet of things. That least is called Tactile Internet and it is considered as the next generation technology that promote equity of everybody independently of religion and time [1]. It will enable all Real Time responsive systems in different areas such as health, transport, gaming, augmented reality and education. Like any kind of technology, the deployment of that new next generation technology has to combine with ultra-low latency, high level of security, strong reliability and important throughput.

Latency: Latency is the sum of delays that packet consume to reach destination. In other words, it also considered, as the duration end to end that needs data to be transmitted to the actuator and returned to the sensor. In the Tactile Internet environment and for ensuring real time applications, the Latency must not exceed 1ms [2].

Reliability: Reliability of information refers to the degree of confidence that can be placed. The reliability of information depends on a bundle of interrelated elements, including clear identification of the source, accuracy of data and freshness of information. The Tactile Internet need thus a reliable ubiquitous connectivity in order to guarantee five nines of availability and improve quality of experience QoE [3].

Throughput: it is one of the important metrics of quality of Services QoS, it refers to how many packets of information, in a given amount of time, a system may process, it is ala measure of how much capacities could be transmitted in 1ms [4].

Security: The security aspect comprises confidentiality, availability, and data authentication. In the Tactile Internet applications, the security has to be implemented without gendering any negative impact on the latency time. In other words, traditional type of security implementation genders a header in the packet. Consequently, the end-to-end delay increase and exceed 1ms [5].

Fettweis et al [6]. shows that the implementation of Tactile Internet environment will be based on architecture dividing into three domains mentioned in figure 1:

Master Domain: it refers to the human interface, where Tactile agent covert human motion to tactile input, using its haptic device.

Network Domain: it provides infrastructure that allow entities the opportunity to communicate with each other.

Manuscript received September 5, 2022
Manuscript revised September 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.9.3

The core network of the architecture will be configured using Software Defined Network SDN and Network Function Virtualization NFV. The access network also will be based on 5G technology that provides high throughput.
Slave Domain: It is a Tactile edge composed of remotely controlled robots; it contains the actuator that execute the instruction transmitted by the master domain via the controlled Domain.
Problematic: Imagine if a surgeon, residing in a country, wants to operate a patient in another country. All data will be transmitted via internet, which relies on the life of human being with the strengthness and the robustness of the security system of that technology. Thus, we need to conceive and implement a framework that allow us the opportunity to use securely that technology without influencing on the end-to-end latency.

Contribution: This paper presents a decentralized blockchain and physically unclonable functions (PUFs) based mutual authentication protocol for remote surgery in the Tactile Internet environment.

The organization of the remaining sections of our paper is structured as follows. We begin, in the next section, with a presentation of some recent works concerning authentication protocols. Section III defines the primitives, which composed our proposed solution. In section IV, we give a description about the model of the decentralized and physically unclonable functions PUFs based mutual authentication protocol for the remote surgery use case. Before presenting, in sections V and VI our protocol and its security analysis using AVISPA formal security analysis, section VII studies the evaluation and the implementation of the proposed framework by computing the communication cost of the solution and comparing it to the existing schemes. Then, we conclude our paper by a conclusion in section VIII.

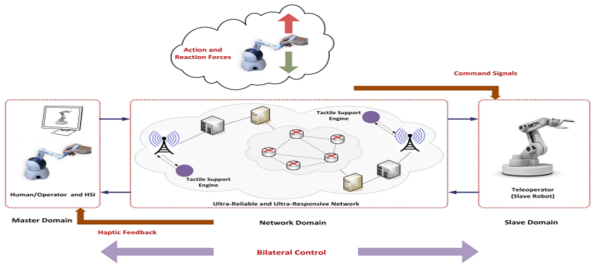

Fig. 1. Tactile Internet Architecture

2. Related Works

Tremendous studies have tackled the security, latency and reliability requirements in the Tactile Internet from software to hardware, and the combination between the hardware and software solutions.

Wu et al. [7] proposed a robust authentication scheme for the wireless medical sensor networks, which combines between the security requirements. But their solution suffers from user tracking attacks. Das et al. [8], in their article, proposed a smart card-based authentication protocol for healthcare. Tarik et al. [9] presented the physically unclonable functions as a solution to ensure the security in the Tactile Internet environment. However, the proposed solution was vulnerable to the Single Point of Failure (SPOF) and does not scalable. To mitigate these existing problems, Hidar et al. [10] proposed a private blockchain based authentication solution for the Tactile Internet.

Furthermore, Pauls et al. [11] suggested a Co design hardware-software for enhancing hash based digital signature for the XMSS algorithm, their solution ensure the security and the latency. But, it needs more computational efforts. Also, Jiang et al. [12] gave a scheme with comprehensive security analysis for mutual authentication protocols. However, their solution can be vulnerable to privileged-insider attacks and also to the distributed denial of service DDos attacks. Alladi et al. [13] present an establishement of mutual authentication protocol for the WMSNs based on physically unclonable functions PUFs.

In [14], Li et al. designed a secure Elliptic Curve Cryptography (ECC) based authentication protocol using input biometric information for the wireless medical sensor networks WMSNs. The solution handles DDOs attacks, key exposure attack, desynchronization attacks and mobile stolen attacks. Acevedo et al. [15] proposed a hardware accelerator cryptography for the Tactile Internet, the solution presented an implementation of cryptographic algorithms on a hardware system in order to ensure security with guarantee of the latency which must not exceed 1 ms.

Dean et al. [16] presented that the fact of injecting data encryption into physical layer does not only reduce the complexity of decryption, but also enhance the computational power. Shantarama et al. [17] an enhanced AES algorithm based on the FPGA to accelerate the execution of the hash operations.

To summary, the presented works in this section cannot ensure latency, security, and reliability, especially in a critical case like a remote surgery where the live of human being is included. Consequently, we need to conceive a new concept for user authentication in the Tactile Internet environment without influencing on the latency time and guarantying reliability. To the best of our knowledge, we propose an authentication mechanism basing on Blockchain, Smart Contract and physically unclonable functions for prototype remote surgery in a human to machine relationship.

3. Preliminaries

After presenting the different related works. We briefly, describe in this section the technologies that we will use in our contribution, which are : Blockchain, Smart contract, physically unclonable functions

3.1 Blockchain

Blockchain is one of the leading technologies in the IT world. Blockchain is a revolutionary technology that has changed how transactions work. It intends to provide a safe and secure mode of transactions, by using digital cryptocurrencies that cannot be manipulated by anyone with ulterior motives. Blockchain makes possible to store and exchange data on the internet without a centralized intermediary. It is the technological engine of cryptocurrencies, the Decentralized Web and its corollary decentralized finance.

A blockchain is a database that contains the history of all exchanges between its users since its creation. This database is secure and distributed: it is shared by its various users, without intermediaries, which allows everyone to check the validity of the chain.

A blockchain is also a distributed software network that serves as a digital record as well as a system for transferring assets securely without the use of a third party. It's a technology that allows for the digital exchange of value units. A blockchain network can tokenize, store, and trade anything from currency to land rights to votes [18][19][20].

3.2 Smart Contract

A smart contract (or intelligent contract) is a computer code that simplifies the execution of certain contractual agreements by eliminating the need to go through an intermediary. Smart contracts are closely linked to blockchain technology, because the latter is the platform on which they are based. In other words, smart contracts are on the blockchain. There are countless applications based on smart contracts and many possible uses [21].

3.3 Physically unclonable functions

Physically unclonable functions can be defined as the one and only physical property of an equipment, in other word, the physically unclonable functions PUFs are an expression of inherent characteristic of a physical object. The main property of this embedded system is that it cannot be reproduced by using security primitives; it also requires a physical basis [9]. Moreover, we adopt the idea of using the PUFs in remote surgery within Tactile Internet environment because they act like human beings, every device and every sensor will have each unique PUF that cannot be cloned. Based on complex embedded, a PUF is also convert a set of challenges C to responses R. Furthermore, a Physical Unclonable Function PUFs represent a function which give us the opportunity to map challenges Cs with defined forms to a responses Rs with preserving the same form. We define a PUF by the following function R= P(C) [22]. The combination of Cs and Rs is called challenges responses pairs CRPs.

4. Framework

In this section, we present a primarily discuss system model of our framework, then we derive to describe in the next section, the details of our proposed blockchain and physically unclonable functions-based authentication protocol in Tactile Internet environment.

First, we present a general description about the components that we can use in surgery room. The composition of the surgical room differs according to the possible acts carried out, in view of the surgical and anesthetic imperatives; nevertheless, we can classify the tools and the equipment used to the monitoring equipment and the effective means. Concerning the monitoring equipment, it is a question of multiple sensors and biosensors that collect dynamic information on the patient's condition ensuring continuous monitoring during the intervention. We distinguish the basic monitoring means such as the pulse oximeter, the electrocardioscope, non-invasive pressure sensor, the anesthesia machine, capnography, temperature monitoring and curarization [23-24], while the imperatives imposed by the surgical procedure itself may require other means of monitoring such as continuous measurement of invasive blood pressure , bi-spectral index, central venous pressure, ultrasound (echo) monitoring such as transesophageal ultrasound during surgery cardiac, an electroencephalogram [25]. The collected data is displayed via monitors with the ability to intelligently collect, analyze, display and store data.

Robotic surgery adds effective means, these are surgical instruments, which are varied according to the surgery performed, the approach and the technology chosen. In any case, the robotic systems are based on two physically separate subsystems: the surgeon works as a “master” and the robotic arms as “slave” [26].

In view of the distances between the surgeon's console which houses the display system, the user interface and the electronic controllers on one side, and the operating room on the other side. Means of audiovisual telecommunication are imperative to the process of remote robotic surgery, mainly allowing visualization of the operating field with endoscopes [26], it should be noted that certain tele-manipulators such as the Da Vinci Surgical Systems, offer depth perception, thus allowing more precise and efficient endoscopic manipulations [27].

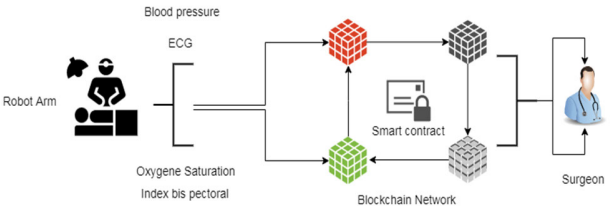

Fig. 2. Network model of the proposed protocol

In order to ensure the security, reliability, and latency in the remote surgery, we need to define some entities as illustrated in figure 2:
Robot Arm RA: located in front of the patient and equipped with Physically Unclonable Function PUF, it will be controlled remotely by the surgeon.
Sensor nodes SNs: allow the surgeon to know all data about the state of the patient like: Blood pressure, oxygen saturation, electrocardiogram ECG, the SNs collect somatic data from patient and transmit them to the surgeon. They must be register with the blockchain and negotiate a secret key with the surgeon. All SNs are equipped with PUF.
Blockchain Network BN: relies on Robot Arm and sensor nodes with the surgeon, dotted with smart contract where all access control policies are described, BN provide the RA, SNs and the surgeon to conduct mutual authentication and session key generation, the communications are transmitted using IEEE 802.11 and 802.15.4 protocols for low consummation [28].

Surgeon: need to input his password and biometric for registration and authentication in BN. After, the SNs will deliver patient's data. Hence, the surgeon can perform his remote surgery using the RA as well as monitoring the state of the patient against any complications. Note that the surgeon has on-premises PUF.

5. Proposed Protocol

In this section, we present our Authentication proposed protocol based on the implementation of blockchain and physically unclonable functions, for the remote surgery in Tactile Internet environment.
Our proposed protocol will be divided into four steps which are: 1) Initialization; 2) Slave domain Registration; 3) Master Domain Registration and mutual Authentication. All the used notations are presented in Table 1.

5.1 Initialization step

In this step, the system developer needs to initialize the blockchain network and publishes the smart contract in order to share the secret key between sensor nodes, robot arms and the surgeon. The blockchain must prevent some potential attacks like single point of failure, xss attacks, third party attacks, DDos attacks.

TABLE 1. NOTATIONS

Notation	Description
ID_S, ID_{RA}	Identity of surgeon,robot arm
MD, S, RA	Mobile device, surgeon,Robot Arm
SC, BN	Smart contract, blockchain network
EC_S	Ephemeral credential of surgeon
EC_{RA}	Ephemeral credential of Robot Arm
Gen(.)	Fuzzy extractor generation function
Rep(.)	Reproduction function
H()	Hash function
PWD_s	Password of surgeon
$\|_s$, $\oplus$	Concatenation, XOR operation
DB, θ, σ	Biometric input,secret key, rep para
$session_{key}$	Session keys
$Register_s$, $Register_{RA}$	Registration functions
(C,R)	Challenge response pair
K_{RA}, K_S	Random secret keys

5.2 Slave domain registration

For the registration in the blockchain network, RA and SNs, in slave domain, should invoke registration function within the smart contract; the blockchain network needs to execute the following steps.

1) The RA generates its own ID_{RA}, the length of the identity number is 160 bits, it also generates the registration function called $Register_{RA}$ and a set of Challenge Response Pair CRP (C_{RA},R_{RA}) by the associated PUF. Then, the following informations will be sent to the blockchain network: ID_{RA}, $Register_{RA}$, (C_{RA},R_{RA}).
2) After receiving the informations from the Robot Arm, the blockcahin network verifies if ID_{RA} are in the verification table T, if the identifiers are in the list of IDs, the Smart Contract in the blockchain network will reject the request. Else, they did not appear in the table, the Smart Contract SC choose two 160 bits random secret key K_{RA} and computes the Ephemeral credentials of RA $EC_{RA}=H(K_{RA} \| ID_{RA})$}.
3) The Smart Contract saves K_{RA}, EC_{RA}, and (C_{RA},R_{RA}).

5.3 Master domain registration

To retrieve patient's data from SNs and control the RA legitimately, the surgeon S, as master domain, also needs to register in the blockchain network in advance. The detailed procedures are illustrated as follows.

1) First and foremost, S chooses a 160-bit random number as his identity ID_S, a nonce N_S, a password PWD_S, and a biometric input DB and generates a set of CRs (C_S , R_S) using his PUF.
2) S computes $RPWD_S = h (PWD_S \| N_S)$ and sends parameters {ID_S, $RPWD_S$, (C_S, R_S), $Register_S$ } to the Blockchain Network.
3) Smart Contract SC verifies the correctness of ID_S, it checks whether $ID_S \in$ Table T, ID_S appears in the Smart Contract SC table, it rejects this registration request. Otherwise, Smart contract SC maps the DB to the fuzzy extractor probabilistic generation function (Gen) [29] and generates Gen (DB) = {θ, σ}, where θ is a

biometric secret key and σRep(.) is a reproduction parameter given by the fuzzy extractor.

4) Smart contract SC generates a 160 bits random secret key as K_S and computes RB = h ($\theta \| ID_S$), A = h ($K_S \| \sigma \| RB$) $\oplus$ RPW_S , EC_S = h($K_S \| ID_S$), and B = $EC_S \oplus RPWD_S$. SC stores {σ, θ, ID_S, $RPWD_S$, K_S, (C_S , R_S)} in its database.
5) SC submits {RB, A, B, σRep(.)} to S in a private channel.
6) S stores {RB, A, B, σRep(.), $RPWD_S$, N_S} in its mobile device or in its pc workstation.

5.4 Mutual Authentication

At this stage, the surgeon S needs to authenticate to his MD mobile device or pc workstation at first. Hence, if S would like to login to the Robot Arm RA in order to begin surgery, the corresponding three parties (i.e., Robot Arm, Blockchain Network and Surgeon) must be included to ensure the mutual authentication. The description of details is listed as the following steps.

1) First, S inputs his identity ID_S, password PWD_S', and the biometric information DB' tactile agent.
2) Tactile agent as mobile device or pc workstation applies DB' to a deterministic reproduction function as Rep (DB', σ) = θ'. Then, S figures out RB' = h (θ' || ID_S), $RPWD_S$' = h(PWD_S' || N_S) and checks if RB' equal RB and $RPWD_S$' equal $RPWD_S$. If both equations hold, S logins successfully. Otherwise, the Tactile Internet system aborts this process.
3) S chooses a pair of ($C1_S$, $R1_S$) from its preloaded CRs (C_S , R_S) in the PUF and calculates EC_S = B $\oplus$ $RPWD_S$, M1 = h(EC_S || N_S || $R1_S$), M2 = h(A || $RPWD_S$) $\oplus$ M1, and M3 = M2 $\oplus$ $R1_S$. Finally, S sends a set of messages S1 = {ID_S, M1, M3, $C1_S$, T_{S1}, invokeAuth } to the Blockchain Network BN via Mobile device or pc workstation in the public channel, where invokeAuth is the invoked function and T_{S1} is the current timestamp.
4) BN obtains the S1and first checks the freshness of T_{S1}. If T_{S1} is fresh, BN establish a transaction with S1 to the smart contract SC.
5) SC searches the related $R1_S$' on the basis of generated $C1_S$ from its database. Subsequently, SC calculates M_2' = M_3 $\oplus$ $R1_S$', M_4 = h(A || $RPWD_S$) = h(K || σ || RB || $RPWD_S$), M_4' = M_2' $\oplus$ M_1 and confirms if M4' = M4. If they are equal, S is authenticates successfully. Otherwise, the authentication to the SC will be rejected.
6) SC also chooses a new Challenge Response pair ($C2_S$, $R2_S$) from existing CRPs (C_S , R_S) and computes M5 = h(M4 || $R2_S$) $\oplus$ A. Then, Smart contract SC transmit a set of messages S2 = {M_5, $C2_S$, T_{S2}} to the S via the BN..
7) After receiving S2, as usual, S checks,initially, the freshness of T_{S2}. If T_{S1} is fresh, S selects response $R2_S$' from on-premises set (C_S, R_S) and figures out M_5' = h (M1 $\oplus$ M_2 || $R2_S$') $\oplus$ A. At the final step, S checks if M_5' = M_5. If it is equal, then BN is considered legitimate
8) Furthermore, to retrieve Robot Arm, BN automatically invokes the RA_{AUTH} function in the SC. Then, the Smart contract SC chooses a CRP ($C1_{RA}$, $R1_{RA}$) from the accessible CRPs set (C_{RA}, R_{RA}) and computes M6 = h ($R1_{RA}$ || EC_{RA}), M7 = M4 $\oplus$ M6. Finally, SC sends a set of messages S4 = {ID_S, M7, $C1_{RA}$, T_{S3}} to RA via BN.
9) While RA receives M3, it first checks the freshness of T_{S3} and selects $R1_{RA}$' according to received $C1_{RA}$. Then, RA calculates M6' = h ($R1_{RA}$' || EC_{RA}) and checks whether M6' = M6. When the equation holds, SNi selects a new pair of ($C2_{RA}$, $R2_{RA}$) from PUF and computes M4 = M7 $\oplus$ M6, M8 = h (EC_{RA} || ID_{RA} || $R2_{RA}$), session key as $Session_{keyRA}$ = h (M4 || M8) and masked session key as Msk_{SNi} = $Session_{keyRA}$ $\oplus$ $R2_{RA}$. Finally, RA returns a set of messages S4 = {M8, Msk_{RA}, $C2_{RA}$, T_{S4}, RA_{AUTH}} to BN, where T_{S4} is the current timestamp and SN_{AUTH} is the SC function name.
10) Once obtaining {M8, Msk_{RA},$C2_{RA}$, T_{S4}, RA_{AUTH}}, BN verifies the timeliness of TS4. If verification succeeds, BN calls RA_{AUTH} function in the SC to retrieve $R2_{RA}$' according to $C2_{RA}$ and compute M8' = h (EC_{RA} || ID_{RA} || $R2_{RA}$'), then checks if M8' = M8. If the equation holds, SC restores $session_{keyRA}$ = Msk_{RA} $\oplus$ $R2_{RA}$ and computes M9 = M8 $\oplus$ EC_S, M10 = $session_{keySNi}$ $\oplus$ EC_S . Otherwise, the same counter calculates failure times of RA. Finally, SC transmits a set of messages S7 = {ID_{RA}, M9, M10, TS5} to S. The Robot Arm simultaneously has the same procedure.
11) When Surgeon S gets S5 and TS5 does not expire, S extracts M8 = M9$\oplus$ EC_S, $session_{keyRA}$= M10 $\oplus$ EC_S and calculates $session_{keyS}$= h(M4 || M8). If $session_{keySNi}$ = $session_{keyS}$, $session_{keySN}$ and $session_{keyS}$ can be used for the subsequent communication through the blockchain network BN.

6. Security Analysis

After presenting our proposed protocol, we move to evaluate the effectiveness and the correctness of the

solution. For that, we use formal Security analysis based on AVISPA Software.

6.1 Avispa

AVISPA Automated validation of internet security protocols and application is a push-button tool. It provides expressive formal language to specify if a protocole is safe against attacks or not, it can be downloaded as virtual machine and enabled with virtualbox using linux operating system. The AVISPA allow us the opportunity to check the correctness and the efficiency of our proposed protocols, it also gives, in case of unsafe, the intruder scenario that help us to resolve problem within the protocol [30].

6.2 Results

In our proposed protocol, we choose OFMC, ATSE and TA4SP backends to prove if our framework is vulnerable or not against: Blockchain, surgeon and robot arm impersonation attack, physical attack, blockchain system attack, DDos attack. The figures 3,4,5 show that our proposed protocol achieve the security requirements under ATSE, OFMC and TA4SP respectively.

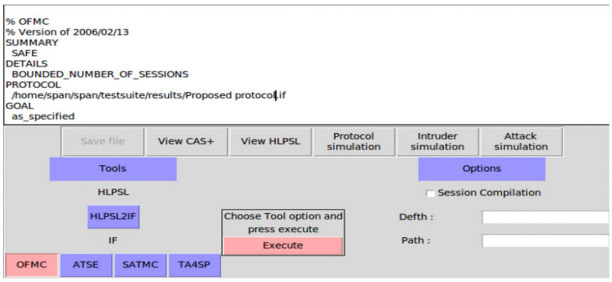

Fig.3. Formal security analysis AVISPA OFCM results

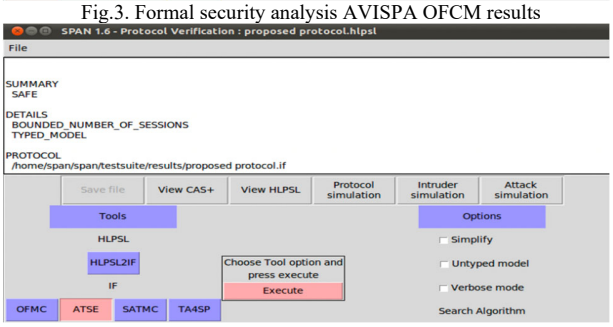

Fig.4. Formal security analysis AVISPA ATSE results

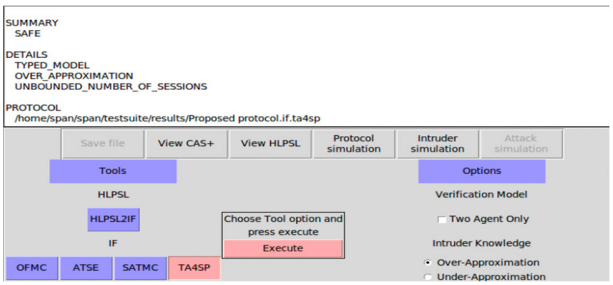

Fig.5. Formal security analysis AVISPA TA4SP results

7. Implementation and Performances

In this section, we first describe the implementation of our proposed protocol and then evaluate its performances with comparing it the proposed protocols cited in section II. Finally, we compute the time end to end for the security system.

7.1 Implementation

The implementation is composed of two parts, including PUFs circuits and Blockchain. The physically unclonable functions need to provide Challenge response pair CRPs for the Robot Arm and the Surgeon system in order to ensure authentication. Consequently, we improved the fuzzy extratctor [29] as well as the Bistable Ring BR-PUFs on Xilinx Virtex-5 FPGA development board [31], XUPV5 LX110T.we choose the BR-PUFs because it make the circuit for efficient and reduce the response time to 10 ns.For the Blockchain network, we create our surgery smart contract using the high-level language programming solidity of Ethereum blockchain [10]. Then, we compile our remote surgery smart contract into Ethereum Virtual Machine (EVM) byte code. Afterwards, we deploy our remote surgery smart contract to the private blockchain (i.e., Ganache [32]) and to the public blockchain (i.e., Ethereum official test network Ropsten [33]).For the measurements, we used desktop with OS: Win 11 64 bits, RAM: 16 GB, CPU: Intel core i7 2.75 GHz.

7.2 Performances

The experiments show that our proposed protocol for ensuring authentication between Robot Arm (Slave Domain) and Surgeon (Master Domain) register 0.007ms in total, dispatched as follow: 0.002ms for Robot Arm (Slave Domain), 0.0035 for the Surgeon (Master Domain) and 0.0015ms for the Blockchain (Blockchain Domain or Gateway). Comparing to all the proposed protocols in the related works, the evaluation study judged that our solution is reduced by around 65% at mean to other protocols. The figure 6 show the comparison between the existed protocols and ours in term of computation cost.

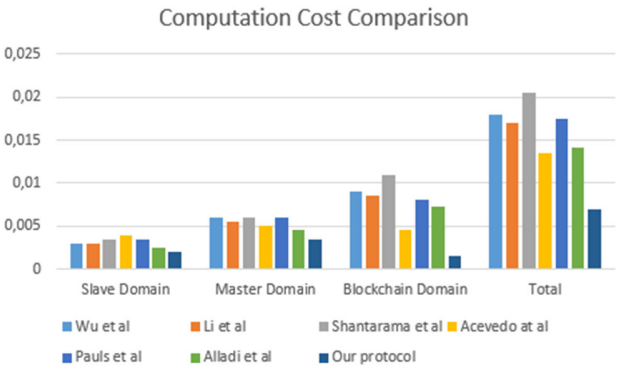

Fig. 6. Computation cost comparison

7. Conclusion

Our paper present Blockchain and Physically unclonable functions based mutual authentication protocol in remote surgery within Tactile Internet environment, our protocol ensure authentication between surgeon, robot arm which is near from the patient and the blockchain network including smart contract, the tactile edge are equipped by PUFs. The security analysis shows the correctness and efficiency of the protocol. Then, the implementation and the performances study prove that our protocol is compatible with latency time of tactile Internet, which must not exceed 1 ms. In our future work, we will focus on the security of the sensor nodes which transmit patient's data (e.g., Blood pressure, Oxygen saturation, ECG ….). In addition, we will think about integrating Artificial Intelligent AI in order to enhance the quality of service.

References

[1] SIMSEK, Meryem, AIJAZ, Adnan, DOHLER, Mischa, *et al.* 5G-enabled tactile internet. *IEEE Journal on Selected Areas in Communications*, 2016, vol. 34, no 3, p. 460-473

[2] Fettweis, Gerhard P. "The tactile internet: Applications and challenges." *IEEE Vehicular Technology Magazine* 9.1 (2014): 64-70.

[3] TANWAR, Sudeep, TYAGI, Sudhanshu, BUDHIRAJA, Ishan, *et al.* Tactile Internet for autonomous vehicles: Latency and reliability analysis. *IEEE Wireless Communications*, 2019, vol. 26, no 4, p. 66-72

[4] MESHRAM, Dewanand A. et PATIL, Dipti D. 5G enabled tactile internet for tele-robotic surgery. *Procedia Computer Science*, 2020, vol. 171, p. 2618-2625.

[5] WAZID, Mohammad, DAS, Ashok Kumar, et LEE, Jong-Hyouk. User authentication in a tactile internet based remote surgery environment: Security issues, challenges, and future research directions. *Pervasive and Mobile Computing*, 2019, vol. 54, p. 71-85.

[6] FETTWEIS, Gerhard P. et BOCHE, Holger. 6G: the personal tactile internet—and open questions for information theory. *IEEE BITS the Information Theory Magazine*, 2021, vol. 1, no 1, p. 71-82.

[7] Wu, F., Li, X., Sangaiah, A. K., Xu, L., Kumari, S., Wu, L., & Shen, J. (2018). A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks. *Future Generation Computer Systems*, *82*, 727-737.

[8] DAS, Ashok Kumar, SUTRALA, Anil Kumar, ODELU, Vanga, *et al.* A secure smartcard-based anonymous user authentication scheme for healthcare applications using wireless medical sensor networks. *Wireless Personal Communications*, 2017, vol. 94, no 3, p. 1899-1933.

[9] HIDAR, Tarik, ABOU EL KALAM, Anas, et BENHADOU, Siham. Ensuring the Security and Performances in Tactile Internet using Physical Unclonable Functions. In : *2019 4th World Conference on Complex Systems (WCCS)*. IEEE, 2019. p. 1-6.

[10] HIDAR, Tarik, ABOU EL KALAM, Anas, BENHADOU, Siham, *et al.* Using blockchain based authentication solution for the remote surgery in tactile internet. *International Journal of Advanced Computer Science and Applications*, 2021, vol. 12, no 2.

[11] Pauls, Friedrich, Robert Wittig, and Gerhard Fettweis. "A LatencyOptimized Hash-Based Digital Signature Accelerator for the Tactile Internet." International Conference on Embedded Computer Systems. Springer, Cham, 2019

[12] JIANG, Qi, MA, Jianfeng, YANG, Chao, *et al.* Efficient end-to-end authentication protocol for wearable health monitoring systems. *Computers & Electrical Engineering*, 2017, vol. 63, p. 182-195.

[13] T. Alladi, V. Chamola, and Naren, "HARCI: A two-way authentication protocol for three entity healthcare IoT networks," IEEE J. Sel. Areas Commun., vol. 39, no. 2, pp. 361–369, Feb. 2021

[14] Li, Jiliang, et al. "PSL-MAAKA: Provably Secure and Lightweight Mutual Authentication and Key Agreement Protocol for Fully Public Channels in Internet of Medical Things." *IEEE Internet of Things Journal* 8.17 (2021): 13183-13195.

[15] ACEVEDO, Javier, ULBRICHT, Marian, GABRIEL, Jennifer, *et al.* Hardware Accelerated Cryptography for Tactile Internet. In : *European Wireless 2021; 26th European Wireless Conference*. VDE, 2021. p. 1-8.

[16] DEAN, Thomas R. et GOLDSMITH, Andrea J. Physical-layer cryptography through massive MIMO. *IEEE Transactions on Information Theory*, 2017, vol. 63, no 8, p. 5419-5436.

[17] SHANTHARAMA, Prateek, THYAGATURU, Akhilesh S., et REISSLEIN, Martin. Hardware-accelerated platforms and infrastructures for network functions: A survey of enabling technologies and research studies. *IEEE Access*, 2020, vol. 8, p. 132021-132085.

[18] Outchakoucht, Aissam, ES-SAMAALI Hamza, and Jean Philippe Leroy. "Dynamic access control policy based on blockchain and machine learning for the internet of things." *International journal of advanced Computer Science and applications* 8.7 (2017).

[19] Es-Samaali, Hamza, Aissam Outchakoucht, and Jean Philippe Leroy. "A blockchain-based access control for big data." *International Journal of Computer Networks and Communications Security* 5.7 (2017): 137.

[20] MOUNNAN, Oussama, EL MOUATASIM, Abdelkrim, MANAD, Otman, *et al.* Privacy-aware and authentication based on blockchain with fault tolerance for IoT enabled fog computing. In : *2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC)*. IEEE, 2020. p. 347-352.

[21] MOUNNAN, Oussama, EL MOUATASIM, Abdelkrim, MANAD, Otman, *et al.* Privacy-aware and authentication based on blockchain with fault tolerance for IoT enabled fog computing. In : *2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC)*. IEEE, 2020. p. 347-352.

[22] Zhang, J. L., Qu, G., Lv, Y. Q., & Zhou, Q. (2014). A survey on silicon PUFs and recent advances in ring oscillator PUFs. *Journal of computer science and technology*, *29*(4), 664-678.

[23] Standards for Basic Anesthetic Monitoring. Committee of Origin: Standards and Practice Parameters (Approved by the ASA House of Delegates on October 21, 1986, last amended on October 20, 2010, and last affirmed on October 28, 2016) https://www.asahq.org/~/media/Sites/ASAHQ/Files/Public/Resources/standards-guidelines/standards-for-basic-anesthetic-monitoring.pdf (Accessed on July 18, 2022)

[24] Klein AA, Meek T, Allcock E, Cook TM, Mincher N, Morris C, and al. Recommendations for standards of monitoring during anaesthesia and recovery 2021: Guideline from the Association of Anaesthetists. Anaesthesia. 2021 Sep;76(9):1212-1223. doi: 10.1111/anae.15501.

[25] Chilkoti G, Wadhwa R, Saxena AK. Technological advances in perioperative monitoring: current concepts and clinical perspectives. J Anaesthesiol Clin Pharmacol. 2015;31:14–24. doi: 10.4103/0970-9185.150521.

[26] K. Tiwari, S. Kumar, and R. K. Tiwari, Fog assisted healthcare architecture for pre-operative support to reduce latency, Procedia Computer Science, vol. 167, pp. 1312–1324, 2020.

[27] Freschi C, Ferrari V, Melfi F, Ferrari M, Mosca F, Cuschieri A.Technical review of the da Vinci surgical telemanipulator. Int J Med Robot Comp. 2013;9(4):396-406.

[28] PETROVA, Marina, RIIHIJARVI, Janne, MAHONEN, Petri, *et al.* Performance study of IEEE 802.15. 4 using measurements and simulations. In : *IEEE Wireless Communications and Networking Conference, 2006. WCNC 2006.* IEEE, 2006. p. 487-492.

[29] DODIS, Yevgeniy, REYZIN, Leonid, et SMITH, Adam. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In : *International conference on the theory and applications of cryptographic techniques*. Springer, Berlin, Heidelberg, 2004. p. 523-540.

[30] Vigano, Luca. "Automated security protocol analysis with the AVISPA tool." *Electronic Notes in Theoretical Computer Science* 155 (2006): 61-86.

[31] Zhang, Y., Li, B., Liu, B., Hu, Y., & Zheng, H. (2021). A privacy-aware PUFs-based multiserver authentication protocol in cloud-edge IoT systems using blockchain. *IEEE Internet of Things Journal*, *8*(18), 13958-13974.

[32] Abou El Houda, Z., Hafid, A. S., & Khoukhi, L. (2021, June). Blockchain-based Reverse Auction for V2V charging in smart grid environment. In *ICC 2021-IEEE International Conference on Communications* (pp. 1-6). IEEE.

[33] Abou El Houda, Z., Hafid, A., & Khoukhi, L. (2019, December). Co-IoT: A collaborative DDoS mitigation scheme in IoT environment based on blockchain using SDN. In *2019 IEEE Global Communications Conference (GLOBECOM)* (pp. 1-6). IEEE.