Using Blockchain based Authentication Solution for the Remote Surgery in Tactile Internet

Tarik HIDAR[1], Anas ABOU EL KALAM[2], Siham BENHADOU[3], Oussama MOUNNAN[4]
Hassan II university, LISER IPI-LRI ENSEM, Paris-France, Casablanca-Morocco[1]
Cadi Ayyad University, ENSA-Team Laboratory, Marrakesh, Morocco[2]
Hassan II University, LISER IPI-LRI ENSEM, Casablanca, Morocco[3]
Ibn Zohr University, FSA-LabSI Laboratory, Agadir,Morocco[4]

***Abstract*—Since the Tactile Internet has been considered as a new era of Internet, delivering real-time interactive systems as well as ultra-reliable and ultra-responsive network connectivity, tremendous efforts have been made to ensure authentication between communication's parties to secure remote surgery. Since this human to machine interaction like remote surgery is critical and the communication between the surgeon and the tactile actor i.e. robot arms should be fully protected during the surgical procedure, a fully secure mutual user authentication scheme should be used in order to establish a secure session among the communicating parties. The existing methods usually require a server to ensure the authentication among the communicating parties, which makes the system vulnerable to single of point failure and not fit the design of such critical distributed environment i.e. tactile internet. To address these issues, we propose a new decentralized blockchain based authentication solution for tactile internet. In our proposed solution, there is no need for a trusted party; moreover, the decentralized nature of our proposed solution makes the authentication immutable, efficient, secure, and low latency requirement. The implementation of our proposed solution is deployed on Ethereum official test network Ropsten. The experimental results show that our solution is efficient, highly secured, and flexible.**

***Keywords*—Tactile internet; blockchain; human to machine interaction; authentication; remote surgery**

I. INTRODUCTION

Emerging industrial trends suggests that the new generation systems would increase the penetration robotics hardware, virtualization technologies and mobile platforms systems. Those new technologies will absolutely switch the role of machines to the human to machine interactions. Especially, the use of the next generation network such as Tactile Internet by mixing ultra-low latency, availability, reliability with high level of security, will represent a revolutionary level of development for society, health, economics and culture.

The mobile internet allowed us to exchange data and make human-to-human relationship. The next step is the Internet of things IoT, which is the interconnection and communication between objects through the internet like sensors and actuators. The Tactile Internet is the next evolution that will not only enable the control of the IoT in real time and low latency. But it will also add a new dimension to human-to-machine interaction by enabling tactile and haptic sensations. In other words, the Tactile Internet is the democratizing of skills and expertise to promote equity between people independently of age, gender and religion.

Now, we summarize some of the key requirements and challenges of industrial Tactile Internet architecture:

Latency: Latency is a measure of delay, in networks domains; it defines the time that takes a data packet to reach its destination. Typically, it is measured as the time taken by data to be transmitted to the recipient and returned to the transmitter. In other words, latency is the time required to make a round trip between two entities. It relies on four delays such as transmission and propagation delay, device-processing delay and storage delay. Ideally, it should therefore be as close to zero as possible. In Tactile Internet environment, latency must not exceed 1 ms in order to ensure real time interaction. Otherwise, the human to machine relationship will be established [1].

Reliability: Tactile Internet actors like, robots and 5G configured smartphone, need a reliable ubiquitous connectivity under all environments such as Tactile Internet environment guarantying high availability, almost 99.999 %, and decreasing the mean time between failures MTBF for optimal operation of all aspect of the applications including maintenance, assembly, construction and repair [1] [2].

Resilience: Several applications like e-Health require the scalability in terms of Tactile Internet architecture, that least should be resilient when several autonomous robot hardware, sensors, and Tactile Internet actors connect through the networks, offering a plethora of recovering from failures and other services. In order to realize that, Tactile Internet networking resilience have to be improved by enabling ubiquitous uptime and fastest main time to repair MTTR, in turn of creating an 'always on' system [3].

Security: The Tactile Internet architecture cannot be secured with the traditional technics of internet technologies. For example, Tactile Internet actors are vulnerable and not secure against the distributed denial of service (DDoS) attacks, which decrease the availability, remote hijacking, cloning attacks and man in the middle. Any single Tactile Internet actor could represent a single point of failure (SPOF) for the entire network and thus damage the availability of data, confidentiality and integrity. Which could cause many disasters especially in health field.

Nobody can deny that Tactile Internet will allow doctors in devastated areas, far from the border, to operate remotely their patients. Therefore, doctors from large hospitals will be able to help colleagues from smaller institutions. That kind of surgery deals with the life and death situations of patients.

In order to make the remote surgery in Tactile Internet environment commercially successful, some factors like security decide the performance of such next generation technologies [25].

Consequently, we have to conceive a model for authentication in order to secure human to machine interactions, like remote surgery, in Tactile Internet environment. Thus, a surgeon can now authenticate to a robot arm using good-shared session key and build a high level of security in communication.

The reminder of this paper is organized as follows: We present firstly an overview of the different related work in Section II, we derive with a detailed description of all components of our architecture including the functions and events in Section III, after we proceed our contribution with an implementation of that solution in Section IV. We present then the security analysis and evaluation of the proposed blockchain based authentication solution in Section V. Finally, we conclude our paper with future work and conclusion.

II. Related Work

Before presenting the related works, we introduce this section with a brief paragraph describing how internet of skills work.

The tactile internet, principally, gives human senses the opportunity to enhance, enable and improve interactions with new technologies.

Haptic interactions will be enabled by the internet of skills using visual feedback. This least will not only include robotic systems and actuating robots that can be controlled in real time. But also, it encompasses the audiovisual interaction.

Different technologies will be mixed by the Tactile Internet, at the network and application level of the open system interconnection (OSI) model. At the edges, robots or 5G configured smartphones will enable the Tactile Internet. Touch in terms of data will be transmitted over a 5G network via the air interface and optic fiber between the e-nodes, while artificial intelligence, especially reinforcement learning, will be enabled close to the user equipment through mobile edge computing (MEC). At the application level, automation, robotics, remote surgery, telepresence, augmented reality (AR) and virtual reality (VR) will all play a part.

Many use cases of authentication schemes have been proposed in different domains. We can consequently use the features of these mechanisms in order to propose our new authentication model for securing one of the most critical use case of the Tactile Internet, which is the remote surgery, which will be the object of section II of our paper.

Challa et al. [4] proposed in their work a user authentication scheme for next generation network like Internet of things applications. The scheme proposed is based on Elliptic curve cryptography (ECC) signature, it also provides user intractability and anonymity features. But, this model requires more computation in internet of things environment.

Hsieh and Leu [5] presented a new model to enhance authentication in the proposed solutions cited in [6] [8]. Wu et al. [8] proposed after a security analysis for Hsieh et al.'s model and gave then a proof that their solution was vulnerable to different attacks like user forgery, offline guessing, physical capture and privileged insider. Furthermore, the proposed model by Leu et al. lacks mutual authentication and does not ensure session key security. To resolve this problem, Wu et al. and Vaidya et al. conceived a user authentication model in the wireless sensor networks WSNs and adopted it to the Internet of Things environment [7] [8].

Li et al. [9] studied the model of Jian et al. [10] and proved that their proposed mechanism was susceptible to key session attack. Then, they improve the solution by proposing an enhanced model for user authentication. Later, He et al. [11] Proposed an architecture based on hierarchical cryptography for the Mobile Healthcare Social Networks. However, owing to the identity based cryptography technic, this solution requires more computation and communication. Another user authentication model is also proposed by Feng et al. [12], their work entitled ideal lattice based anonymous authentication protocol for mobile devices provided a high level of security. Nevertheless, it also need some computation efforts.

Farash et al. [13] provided a scheme for key agreement and user authentication in heterogeneous wireless sensor networks architecture and in Internet of Thing environment. Later, Amin et al. [14] improved performances of the Farash et al. mechanism. After, they gave a proof that their solution knew many security failures. As cited in their work, the Farash et al suffers from offline guessing, specific temporary information leakage and spoofing attacks. Srinivas et al. [15] observed and analyzed in other work that the mechanism of Amine et al. was susceptible to user impersonation, spoofing and stolen smart card attacks. Consequently, they provided an enhanced mechanism for user authentication in WSNs and Internet of Things field in future research [17-18].

Khalil et al. [16] proposed the integration of WSNs into the IoT. Like the WSNs. In the other hand, Yeh et al. [19] proposed Elliptic Curve Cryptography (ECC) technic for user authentication in wireless sensor networks. However, their technic lacks mutual authentication. To overcome this limitation, Shi and Gong [20] Discussed about another elliptic curve cryptography base user authentication model, which will be applied in the wireless sensor networks. Later on, Turkanovic et al. [21] presented a new method to enhance key agreement and user authentication in WSNs. But, their method suffers from many problems such as offline password and identity of guessing, impersonation and smart card stolen attacks. Furthermore, it does not provide secure mutual authentication [22].

Hidar et al. [1], which is our previous work, proposed physical unclonable function to ensure performances and security in the tactile internet; they proposed a mutual authentication protocol basing on the PUFs to resolve the

problem of security with guarantying the same latency, but this solution suffer from the problem of single point of failure (SPOF).

Furthermore, Friedrich Pauls et al. [23] propose a latency-optimized accelerator for hash-based digital signature processing for the Extended Merkle signature scheme XMSS algorithm. Their architecture improves the latency of establishing sessions and the verification into the sub-millisecond range. But it also needs more computational efforts.

Most of the available mechanism presented in this section for user authentication and key agreement are not protected against different attacks. In addition, some of the schemes discussed above are not lightweight, as they require more computational efforts. To summary, the existing related work presented in this section cannot be adequate for ensuring security, especially in a critical case like a remote surgery. Therefore, we need to design a concept for user authentication in the Tactile Internet environment. To the best of our knowledge, we propose a generalized authentication mechanism basing on Blockchain and Smart Contract for remote surgery in a human to machine relationship.

III. Blockchain Mutual Authentication Solution

In this section, we begin with a general background, and then we present our proposed authentication solution for the remote surgery.

A. Blockchain

According to Nakamoto Satoshi in 2008 [24], the blockchain is a distributed database for transactions between entities. All those transactions are stored into ledgers, which ensure security. The non-trusting entities can thus exchange data with each other with a cryptographically verifiable way.

The blockchain paradigm is based on four fundamental blocks:

Source and destination's identifying: All users in a blockchain send and receive transactions with digital identities called addresses. The address must not only give any idea about its owner (Anonymous), but also it should be independent of any given authority (self-generated).

Smart contract: An entity control the condition of auto processing for transactions. In other words, Smart contract.

Transaction: It refers to the act of transmitting data from source to destination. It is generated by sender and broadcasted within the network. All nodes must mine transactions in order to be valid.

Consensus: In blockchain technology, each user or node has absolutely the same ledger as all other users in the network. Consequently, a complete consensus from all nodes is ensured.

B. Proposed Solution

In this part, we provide a description of a generalized user authentication mechanism in the Tactile Internet environment such as remote surgery using our decentralized blockchain user authentication solution.

Our architecture will be described as: a remote surgeon performs a remote surgery on a patient residing in other country, using a robot arm. The surgeon thus does not only need to be physically near to the patient that he operates, but also that least does not need to change his place in critical cases.

To ensure Security and implement our contribution, we propose the following transactions between actors as displaying in Fig. 1:

1) The Surgeon with his remote surgery system authenticates to the smart contract using his wallet address.

2) If the transaction is valid, the smart contract spread a Token access and the IP address of sender. Then, the surgeon and Robot Arm, residing in a smart home, receive the broadcasted data from the blockchain.

3) The surgeon creates a message containing Access token, IP address and the blockchain public key. This package will be signed using the blockchain private key then sent with its corresponding public key.

4) When the robot receives the message, it checks if:

- Both received public keys are similar.
- The signed message is real.
- The public key belongs to the sender address.
- Access token is massively valid.
- The two IP addresses of message and sender are similar.

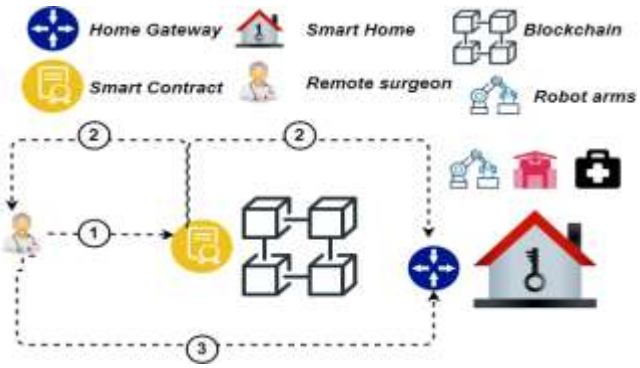

Fig. 1. Steps for user Authentication Model in Tactile Internet based Remote Surgery.

IV. Implementation

We consider an organization that would like to manage the remote surgery using blockchain. First, we create our surgery smart contract using the high-level language programming solidity of Ethereum blockchain [26]. 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 [27]) and to the public blockchain (i.e., Ethereum official test network Ropsten [28]). First, we generate a keypair of Externally Owned Account (EOA), the public key (i.e., o.EOA) and corresponding private key (i.e., o.EPK). This keypair of public and private keys are used to create our

remote surgery smart contract (surgery -SC) and execute the functions of the surgery -SC (see Fig. 2). Then, we add via, our smart contract, the authorized users (i.e., remote surgeon) into the smart contract. It includes the smart contract's address and some other information (e.g., surgeon notes). Our surgery smart contract allows to easily add users as well add access policies to the system and to manage and modify the remote surgery access control in a fully decentralized, secure, and transparent manner. Our surgery smart contract ensures the flexibility in the process of adding and removing access control policies.

Moreover, each access control transaction is verified by all nodes of blockchain (i.e., miners), thus ensuring the decentrazlid and trustworthiness of our proposed access control.

To show that our proposed is cost effective, we have estimated the cost of our surgery smart contract as well as the execution of each of its functions. When conducted the experiment, the gasPrice is set to 1Gwei, where 1Gwei=10^{-9} ether, and 1 ether is equal to 379.26 USD. Fig. 3 shows the surgery smart contract functions costs of different functions implement by our proposed access control. We have varied the number of users from 1 to 100. The cost of the execution of different functions of our proposed solution is 0.017, 0.0050.007 And 0.006 USD for add policy, remove policy, delete policy, and check policy functions, respectively. We observe that all the operations have low costs.

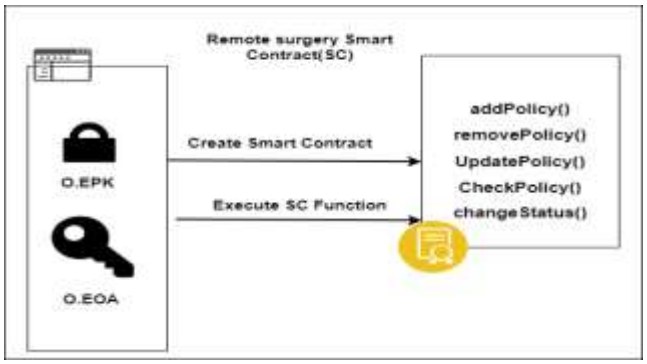

Fig. 2. Surgery Smart Contract.

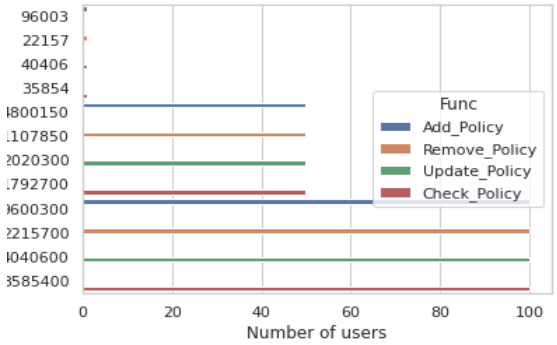

Fig. 3. Surgery Smart Contract Functions Costs.

V. Evaluation and Security Analysis

After the implementation of our proposed solution for ensuring mutual authentication by using blockchain in a Tactile Internet environment. We move to the next section of our paper wish is the evaluation and the security analysis.

In this section, we present an evaluation of our proposed solution in order to assure its quality, we compare it to the previous solutions presented in related work. The metric of this evaluation will be based on if our offered authentication solution solved problems occurring in the other authentication mechanisms proposed in different.

Table I shows a comparison between our solution and the other proposed solutions in section II based on:

- Availability.
- Decentralization.
- Scalability.
- Session key leakage.
- Online and offline password guessing.
- Man in the middle.
- Denial of services.
- Physical capturing of devices.

Table I shows how our proposed solution for the remote surgery is secured againt all the attacks proposed.

TABLE I. Comparison of Security Features and Attacks

Features	Challa	Amin	Li	Jiang	Turkanovic	Farash	Hidar	Our solution
	et al. [4]	et al.[14]	et al.[9]	et al.[10]	et al. [21]	et al.[13]	et al.[1]	
Availability	×	✓	×	×	×	×	✓	✓
Scalability	✓	✓	×	✓	×	×	×	✓
Decentralization	×	×	✓	✓	×	×	×	✓
Privileged insider	✓	×	✓	✓	×	×	✓	✓
Session key agreement	✓	✓	✓	✓	×	✓	✓	✓
Password guessing	✓	×	✓	✓	×	✓	✓	✓
Man in the middle	✓	✓	✓	✓	✓	✓	✓	✓
Denial of service	✓	✓	✓	✓	✓	×	✓	✓
Physical capturing	✓	✓	✓	×	×	×	✓	✓

VI. Conclusion

In this paper, we present a real contribution for Tactile Internet security, which is based on the deployment of the blockchain and smart contract for user authentication in a remote surgery within a Tactile Internet environment. After discussing the existing related work, concerning Tactile Internet and other fields such as wireless secure networks and Internet of things, we showed some vulnerabilities of these proposed solutions, we then propose a general user authentication model by describing highly all various steps needed by remote surgeon in order to get access to the Tactile Internet environment and then operate the patient via the arm robot. After we presented an implementation of our contribution, then we evaluated our work with presenting a comparison between our solution and the others described in related works. In our future work, as the Tactile Internet based remote surgery architecture requires real time reaction, extra low latency and ultra-fast authentication. We are now working on an extension of this paper; we focus on the latency aspect of our mechanism by integrating some technologies like Fog Computing [25] in order to ensure a high level of quality of experience.

References

[1] Hidar, T., El Kalam, A. A., & Benhadou, S. (2019, April). Ensuring the Security and Performances in Tactile Internet using Physical Unclonable Functions. In 2019 4th World Conference on Complex Systems (WCCS) (pp. 1-6). IEEE.

[2] AMAN, Muhammad Naveed, CHUA, Kee Chaing, SIKDAR, Biplab. Mutual authentication in IoT systems using physical unclonable functions. IEEE Internet of Things Journal, 2017, vol. 4, no 5, p.1327-1340.

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

[4] CHALLA, Sravani, WAZID, Mohammad, DAS, Ashok Kumar. Secure signature-based authenticated key establishment scheme for future IoT applications. IEEE Access, 2017, vol. 5, p. 3028-3043.

[5] HSIEH, Wen-Bin, and Jenq-Shiou Leu. "A robust user authentication scheme using dynamic identity in wireless sensor networks." Wireless personal communications 77.2 (2014): 979-989.

[6] DAS, Manik Lal. Two-factor user authentication in wireless sensor networks. IEEE transactions on wireless communications, 2009, vol. 8, no 3, p. 1086-1090.

[7] VAIDYA, Binod, MAKRAKIS, Dimitrios, MOUFTAH, Hussein T. Improved two-factor user authentication in wireless sensor networks. In: 2010 IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communications. IEEE, 2010. p. 600-606.

[8] F Wu, L Xu, S Kumari, and X Li "A privacy-preserving and provable user authentication scheme for wireless sensor networks based on internet of things security." Journal of Ambient Intelligence and Humanized Computing 8.1 (2017): 101-116.

[9] LI, Xiong, NIU, Jianwei, KUMARI, Saru. A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments. Journal of Network and Computer Applications, 2018, vol. 103, p. 194-204.

[10] JIANG, Qi, ZEADALLY, Sherali, MA, Jianfeng. Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks. IEEE Access, 2017, vol. 5, p. 3376-3392.

[11] Yeh, H. L., Chen, T. H., Liu, P. C., Kim, T. H., & Wei, H. W. (2011). A secured authentication protocol for wireless sensor networks using elliptic curves cryptography. Sensors, 11(5), 4767-4779.

[12] FENG, Qi, HE, Debiao, ZEADALLY, Sherali. Ideal lattice-based anonymous authentication pro ocol for mobile devices. IEEE Systems Journal, 2018, vol. 13, no 3, p. 2775-2785.

[13] FARASH, Mohammad Sabzinejad, TURKANOVIĆ, Muhamed, KUMARI, Saru, An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment. Ad Hoc Networks, 2016, vol. 36, p. 152-176.

[14] Amin, R., Islam, S. H., Biswas, G. P., Khan, M. K., Leng, L., & Kumar, N. (2016). Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks. Computer Networks, 101, 42-62.

[15] Srinivas, Jangirala, Sourav Mukhopadhyay, and Dheerendra Mishra. "Secure and efficient user authentication scheme for multi-gateway wireless sensor networks." Ad Hoc Networks 54 (2017): 147-169.

[16] KHALIL, Nacer, ABID, Mohamed Riduan, BENHADDOU, Driss, Wireless sensors networks for Internet of Things. In: 2014 IEEE ninth international conference on intelligent sensors, sensor networks and information processing (ISSNIP). IEEE, 2014. p. 1-6.

[17] FARASH, Mohammad Sabzinejad, TURKANOVIĆ, Muhamed, KUMARI, Saru, An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment. Ad Hoc Networks, 2016, vol. 36, p. 152-176.

[18] Challa, Sravani, "Secure signature-based authenticated key establishment scheme for future IoT applications." IEEE Access 5 (2017): 3028-3043.

[19] Yeh, H. L., Chen, T. H., Liu, P. C., Kim, T. H., & Wei, H. W. (2011). A secured authentication protocol for wireless sensor networks using elliptic curves cryptography. Sensors, 11(5), 4767-4779.

[20] Shi, Wenbo, and Peng Gong. "A new user authentication protocol for wireless sensor networks using elliptic curves cryptography." International Journal of Distributed Sensor Networks 9.4 (2013):730831.

[21] TURKANOVIĆ, Muhamed, BRUMEN, Boštjan, HÖLBL, Marko. A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion. Ad Hoc Networks, 2014, vol. 20, p. 96-112.

[22] AMIN, Ruhul et BISWAS, G. P. A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks. Ad Hoc Networks, 2016, vol. 36, p. 58-80.

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

[24] Nakamoto, Satoshi, and A. Bitcoin. "A peer-to-peer electronic cash system." Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf (2008).

[25] STOJMENOVIC, Ivan et WEN, Sheng. The fog computing paradigm: Scenarios and security issues. In : 2014 federated conference on computer science and information systems. IEEE, 2014. p. 1-8.

[26] "Solidity", Accessed: Jan. 1, 2020. [Online]. Available: https://solidity.readthedocs.io/en/develop/.

[27] Ganache. Accessed: Jan. 1, 2019. [Online]. Available: https://truffleframework.com/docs/ganache/overview.

[28] Go Ethereum. Accessed: Mai. 1, 2019. [Online]. Available: https://geth.ethereum.org/.