A Stochastic Approach for an Enhanced Trust Management in a Decentralized Healthcare Environment

Chaima Khalfaoui*, Samiha Ayed*, Moez Esseghir*
*ICD/ERA, Troyes University of Technology, France
{chaima.khalfaoui, samiha.ayed and moez.esseghir}@utt.fr

Abstract—**Medical institutions are increasingly adopting IoT platforms to share data, communicate rapidly and improve healthcare treatment abilities. However, this trend is also raising the risk of potential data manipulation attacks. In decentralized networks, defense mechanisms against external entities have been widely enabled while protection against insider attackers is still the weakest link of the chain. Most of the platforms are based on the assumption that all the insider nodes are trustworthy. However, these nodes are exploiting of this assumption to lead manipulation attacks and violate data integrity and reliability without being detected. To address this problem, we propose a secure decentralized management system able to detect insider malicious nodes. Our proposal is based on a three layer architecture: storage layer, blockchain based network layer and IoT devices layer. In this paper, we mainly focus on the network layer where we propose to integrate a decentralized trust based authorization module. This latter allows updating dynamically the nodes access rights by observing and evaluating their behavior. To this aim, we combine probabilistic modelling and stochastic modelling to classify and predict the nodes behavior. Conducted performance evaluation and security analysis show that our proposition provides efficient detection of malicious nodes compared to other trust based management approaches.**

Index Terms—**Security, trust, authorization, On-Off attack, blockchain, smart contract, Markov chain.**

I. INTRODUCTION

With the emergence of innovative technologies such as Medical Internet of Things (MIoT) and Mobile Health (MH), healthcare industry is witnessing significant changes. Platforms dedicated to healthcare are playing a more and more important role in improving the health, safety, and care of billions of people [1]. However, these platforms among others are confronted to various security threats. Recent research presented that 24% of data loss incidents were caused by insiders including accidental and malicious acts and 55% of root causes of data breaches occurred as a result of unintentional employee action [2]. Recently, fundamental security requirements such as integrity and non-repudiation motivated several works to consider blockchain networks to promote medical services. Explications behind the choice of blockchain come down to the nature of its infrastructure. Blockchain [3] provides a decentralized, secure, tamper-proof technology. It is one of the most promising technologies to meet security requirements of IoT networks. Blockchain confirms integrity and validity of networks through computational-intensive tasks like Proof-of-Work (POW) or Proof-of-Stake (POS) [4]. However, providing tamper-proof interactions is a necessary but insufficient element to provide trust in medical IoT environments. Malicious insider participants may still intentionally provide erroneous data for their own benefit. Typically, they are either motivated by financial profit or aim to hide errors they made. For example, a malicious node may manipulate medical records to steal equipment. On-Off attack is one of the most dangerous attacks that healthcare institutions are facing. A malicious node may hide his intentions by performing alternatively bad and good behavior to make the system consider his bad behavior as an error. To defend against this type of attack, trust models based on authorization mechanisms are considered as the first line of defense. Conventional authorization approaches envisage static planned patterns [5]. However, the IoT environment is characterized by continuous change to which the authorization schemes are required to dynamically respond. Thus, healthcare providers behavior evolution have to be considered as an essential component to ensure security in decentralized networks. In this paper, we propose a fully decentralized trust based authorization mechanism combining probabilistic classification and stochastic modelling to manage the network nodes access rights and limit efficiently insider attacks. We believe that our approach allows detecting insider malicious nodes aiming to perform On-Off attack. To the best of our knowledge, our work is one of the first attempts to design distributed trust in medical blockchain systems using stochastic models. The contributions of our paper are summarized as follows:

1) We propose a three layer architecture based on a blockchain network to secure data from its creation to its final use.
2) We propose a trust based authorization mechanism with dynamic access rights using the combination of probabilistic Bayesian modelling and a stochastic Markov modelling.
3) We conduct simulations on the top of Ethereum Testnet Platform and Solidity smart contracts to evaluate the performance and analyze the security metrics of our approach. Experimental results show that our proposition provides efficient detection of malicious participants compared to other trust based management approaches.

The paper is organized as follows: Section II presents the related works. We detail our proposed system in Section III. Evaluation results are presented in Section IV. Section V draws some conclusions and presents the future works.

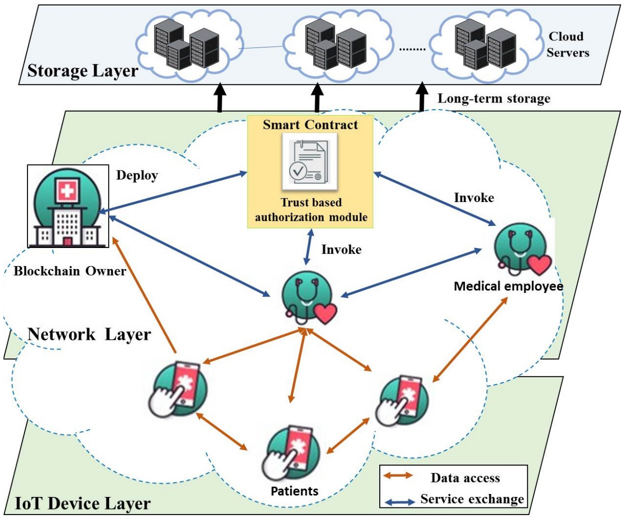


Figure 1: System architecture

II. RELATED WORKS

A. Blockchain based authorization

Several domains such as Industry 4.0, Smart Grid, Vehicular networks, Energy trading or Healthcare made use of the blockchain for data management. Others, focused on enhancing the security of IoT applications using blockchain networks. Lin *et al.* [6] gave a full survey on blockchain security issues and challenges. Novo *et al.* [7] proposed a distributed access control system for IoT based on a blockchain and studied its performance on large-scale networks. Dorri *et al.* [8] proposed an authorization approach to manage smart home IoT devices where the gateways are the blockchain miners.

B. Trust-based mechanisms

Duma *et al.* [9] presented a peer to peer overlay for intrusion detection against insider threats. However, they created a single point of failure by using only one event manager. MENG *et al.* [10] introduced a blockchain based schema to defend medical smartphones against insider attacks using a lightweight IDS system and relying only on Naive Bayesian classification. In this latter work, authors limited their judgment criteria to users feedback which may lead to subjective decisions. In the vehicular domain, Lu *et al.* [11] proposed to establish trust using a reputation evaluation algorithm relying on interactions and opinion history. Evaluations rely on the honesty level of the owners. Consequently, most of the recent studied works proposed to limit insider attacks through authorization mechanisms are either relying on centralized architectures or try to adapt centralized approaches to decentralized architectures. Some rare works are taking into consideration the decentralized nature of the IoT, yet they do not consider either the dynamicity of the environment or relations between the stakeholders.

III. PROPOSED SYSTEM

A. Problem formulation

Our main purpose is to build an authorization module able to protect distributed healthcare environments against insider manipulation attacks and more precisely On-Off attack. In general, these attackers, obtain authorizations, remain trustworthy for a period of time and then change their behavior to act maliciously for short periods without being detected. We propose to integrate a trust based authorization module on the top of a blockchain network. This latter aims to detect efficiently malicious nodes behavior and limit their access rights. Our authorization consists of the main following steps. First, nodes activities are observed to learn about their behavior. Next, a stochastic approach is used to classify them according to their trustworthiness and predict the evolution of their behavior in the future. Finally, accorded authorization permissions are updated dynamically using ABAC protocol. Even though ABAC model have been widely used to manage access control, the novelty of our proposition compared to existing approaches is combining probabilistic classification and stochastic modelling to manage ABAC access control rules in a fully decentralized way.

B. System Architecture

As shown in Figure 1, the proposed system architecture consists of three layers namely: storage layer, network layer and IoT devices layer. Storage layer consists of an interconnected collection of cloud servers that provide long-term or heavy storage. The network layer contains the blockchain main components: (1) The Healthcare providers, denoted $N = \{N_1, N_2, ..., N_n\}$, represent the blockchain miners. They are expected to interact and exchange data such as updating patients profiles or monitoring the medical equipment using the authorization mechanism module. (2) The medical institute owner is at the same time the blockchain owner and an active node. This latter is a highly trusted authority and the only node allowed to deploy smart contacts in the blockchain and (3) The trust based authorization mechanism module is deployed in a smart contract to ensure its autonomous and secure execution. Finally, the IoT devices layer contains external entities such as patients devices. We consider them as lightweight nodes. Since they are often resource constrained, they do not contribute to validating transactions.

C. Authorization mechanism modelling

We propose a decentralized authorization mechanism based on ABAC model where the nodes' of the blockchain behavior are periodically observed, then malicious nodes are detected and classified. Finally an update to their access permissions is easily performed since ABAC allows changing access decisions by simply changing its attribute values.

1) Initialization phase: The blockchain owner initiates the access control mechanism with temporary elements (object entities, resources, access permissions and rules) that will be updated later as illustrated in Figure 2. He defines: the blockchain nodes as object entities, a set of medical files (F) and a set of clinical equipment (C) as resources and three access permissions: read (r), write (w) and delete (d). db_{rights} is the data base that handles the access rights rules as follows:

- Allow N_k to ([r,w,d] in f_i) if { N_k is author of f_i}.

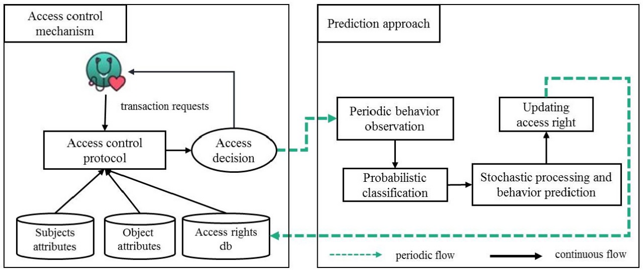


Figure 2: Trust based Authorization process

- Allow N_k to ([r,w,d] in F) if $\{N_k$ is blockchain owner$\}$.
- Allow N_k to ([r,w,d] in C) if $\{N_k$ is blockchain owner$\}$.
- Allow N_k to ([r] in C).

Logical and contextual rules are defined as follow:

- Deployed data have to be non-redundant.
- Deployed data must respect its fixed logical interval.
- Access or alteration requests for the for the same data must respect a minimal fixed time interval.

The nodes use ABAC requests to ask for permissions using: Is Permitted(Subject, Action, Object, Contextual attributes).

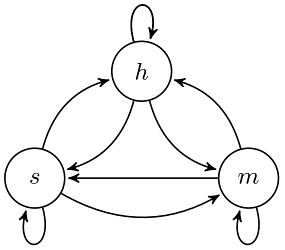
2) Behavioral observation of a node: Periodically, transactions $Tx = \{tx_1, tx_2.., tx_q\}$ of each node are mapped to a set of behavioral vectors $V = \{v_1, v_2.., v_q\}$ where each v_i corresponds to the behavior showed in tx_i. In this proposal, we define: $v_i = (e1, e2)$ where e1 is set to 1 if the transaction owner is authorized to access the data and to 0 otherwise while e2 is set to 1 if the transaction is relevant according to the defined rules and to 0 otherwise. To summarize, each $v_i \in \{(0,0),(1,1),(1,0),(0,1)\}$ and $v_i = (0,0)$ if the transaction is legitimate, $v_i = (1,1)$ if the transaction is malicious and $v_i = (1,0)$ or $(0,1)$ for uncertain transactions.

3) Probabilistic node classification: We classify the nodes according to three classes of trustworthiness: honest (h), suspicious (s) and malicious (m) with: $h \in [0.6, 1]$, $s \in]0.4, 0.6[$, $m \in [0, 0.4[$. We use the Bayesian classifier to compute the probabilities of trustworthiness since it is based on the frequency count of events. For this, we consider the set V as the set of events. Next, we use a membership function that uses the obtained probabilities as input and returns the class of trustworthiness as output.

4) Stochastic processing and behavior prediction: We adopt probabilistic model based on a time homogeneous Markov chain to study the network nodes behavior. We use the classification states: $S = \{h, s, m\}$ defined in the previous section as the space states of all possible states a miner node can reach. Since Markov chain is time independent, the future state of a node N_k a time (t+1) depends only on its current state at (t) and not on its previous states. Thus, if N_k is currently in a state S_i, then is moving to a next state S_j the probability of transition is denoted by $P_{N_{k,ij}}$ and relies only on the current state S_i. To represent the evolution of a node behavior, we use the transaction diagram or the probability transition matrix P as shown in Figure 3. Where $P_{N_{k,i\to j}}$ represents the probability that a miner node N_k makes a transition from a current state s_i to the next state s_j in a single step with $P_{N_{k,i\to j}}$:

$$p_{N_{k,i\to j}} = p(X_{N_{k,t+1}} = j | X_{N_{k,t}} = i) = \frac{\delta_{ij}}{\gamma_i} \qquad (1)$$

Where δ_{ij} is the number of times N_k moved from state i to state j and γ is the number of time N_k visited state i. However, the state m is an absorbing final state. Therefore, if a node reaches the malicious state then returning to another state is proibited and access rights are revoked. Algorithm 1 illustrates how we obtain the first transition matrix using an initial vector V_0 and the observed behavior of a N_k. While Algorithm 2 shows the extensive computation we conducted to reach the limit distribution of the Markov chain which corresponds to the prediction of the node behavior.



$$P = \begin{pmatrix} p_{N_{k,h\to h}} & p_{N_{k,h\to s}} & p_{N_{k,h\to m}} \\ p_{N_{k,tr\to h}} & p_{N_{k,tr\to s}} & p_{N_{k,tr\to m}} \\ p_{N_{k,s\to h}} & p_{N_{k,s\to s}} & p_{N_{k,s\to m}} \\ 0 & 0 & 1 \end{pmatrix}$$

Figure 3: State transition diagram of a node behavior

Algorithm 1: First Probability Distribution Algorithm

```
Input: Space of states S, Node $N_k$, period of time T
Output: P
for $t=1$ to $T$ do
    for $i=1$ to $|S|$ do
        for $j=1$ to $|S|$ do
            if $(s(N_k)_t = i)$ and $(s(N_k)_{t+1} = j)$ then
                //number of times $N_k$ moved from i to j
                $Counter_{ij}$= $Counter_{ij}$+1
                //number of times $N_k$ visited i
                $Counter_i$ = $Counter_i$ +1
//Complete the transaction probability matrix
for $i=1$ to $|S|$ do
    for $j=1$ to $|S|$ do
        $P_{ij}$ = $Counter_{ij}$ / $Counter_i$
return P
```

5) Updating system access rights: Once the prediction probabilities obtained, permissions are updated using algorithm 3. If the prediction shows the node as honest, it can continue benefiting from his current permissions. While if it is detected as malicious, it will be banned from the system. However, if it is declared suspicious, its permissions are limited to access until the next monitoring. Depending on the discipline, a limited number of suspicious states is allowed before exclusion.

Algorithm 2: System resolution Algorithm

```
Input: Initial state vector $V_0$, P
Output: Stationary state $V_n$
$V_1 = V_0 * P$ //define the first distribution
//increment i until $V_{i+1}$ and $V_i$ are identical
while ($V_{i+1} \neq V_i$) do
    $V_{i+1} = V_i * P$
$Vn = V_{i+1}$ //limit distribution probabilities
return $Vn$
```

Algorithm 3: Access rights update Algorithm

```
Input: $prediction$, $N_k$,$db_{rights}$, $S_{counter}$
Output: $db_{rights}$
if ($prediction$ = 'h') then
    $db_{rights}$= $db_{rights}$ //Do not change permissions
else if ($prediction$ = 's') then
    //Limit permissions to access only MS resources
    $db_{rights}(N_k)$ = Allow [r] to MS
    $S_counter$= $S_{counter}$ +1 //Suspicious state counter
else if ($prediction$ = 'm') or ($S_{counter} > Number_{limit}$) then
    $db_{rights}(N_k)$ = Deny All //Revoke all rights
return ($db_{rights}$)
```

IV. SYSTEM EVALUATION

1) An honest node and a malicious node behavior analysis: We consider two healthcare environments: (1) H1: A trustworthy healthcare institution in which only 10% of the nodes are malicious. This latter represents an honest medical environment. (2) H2: A corrupt healthcare institution in which 40% of the nodes are malicious. We implemented the aforementioned scenario using Ethereum and we deployed the authorization module using Solidity. The main parameters of implementation are defined in Table I. In the next sections, we represent the distribution of honest nodes with blue dots as we use red dots to represent the malicious nodes' distribution.

Table I: Simulation parameters

Parameter	Value
Number of nodes per network	30,50,100,200
Number of transactions	$40pernode$
Maliciousness levels	$H1 : 10\%; H2 : 40\%$
Trustworthiness states	$s \in h, s, m$

Figure 4 represents a periodical observation of a malicious and an honest node initialized under the same conditions without our approach. In the beginning, we consider all the nodes initially suspicious with a trust level equal to 0.5. However, their state of trustworthiness will be defined based on their behavior. As we can see, the honest node trust value remain in constant increase until reaching the maximum value after 11 transactions. However, the second node is a malicious miner conducting an On-Off attack by asking periodically to access unauthorized data. His trust value fluctuates between the minimum value of suspicion 0.4 and high values of honesty such as 0.9 after 20 transactions. With this uncertain behavior, he aims to make conventional security system consider his bad acts as errors.

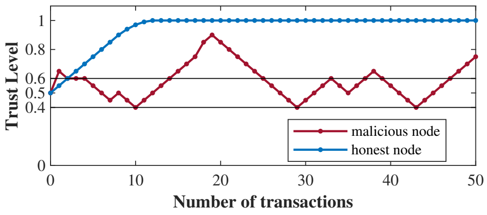
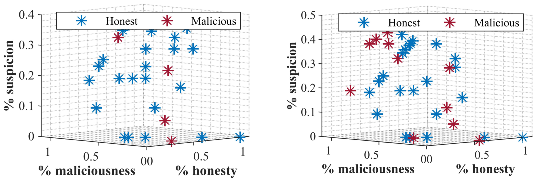
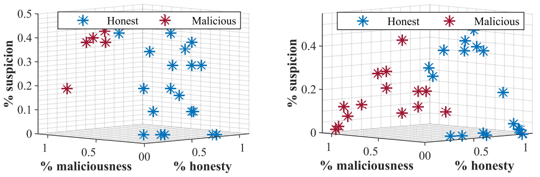


Figure 4: Honest and malicious nodes behavior comparison



(a) H1: Initial distribution (b) H2: Initial distribution



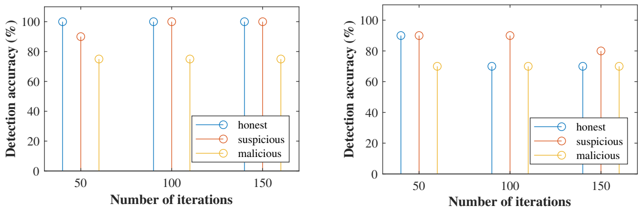
(c) H1: Prediction results (d) H2: Prediction results

Figure 5: Impact of varying the number of malicious nodes

2) Impact of increasing the number of nodes on the prediction performances of the system: Figure 5 shows the execution of the Markov process in H1 and H2 environment with 30 nodes. Figure 5a and Figure 5b represent the initial distributions. In H1, all the malicious nodes are detected and only one honest node is classified as malicious. In fact, we can observe an honest class with almost all the honest nodes grouped into a clear linear shape as shown in Figure 5c. However, in Figure 5d, we remark that over 20% of the nodes are misclassified. To identify the cause of the misclassified nodes, we study one of the potential reasons. Figure 6 shows the impact of varying the initial vector in the Markov chain on the accuracy of the results during the several calculated probability distributions. To this aim, we calculate the True Positive Rate as follows:

$$Accuracy = \frac{\varphi + \rho}{\varphi + \rho + \overline{\rho} + \overline{\varphi}} \tag{2}$$

Where φ and ρ represent honest and malicious nodes correctly classified (true positives and true negatives) and $\overline{\varphi}$ and $\overline{\rho}$ represent honest and malicious nodes wrongly classified (false positives and false negatives). First, we remark that in average, if suspicious is the initial vector of probabilities, the detection rate is high in both environments. We note that in Figure 6a the accuracy rate with suspicious as initial vector of probabilities is 90%, however this rate increases to reach 100% in its limit distribution. Thus, in Figure 6b we note that for the same input configuration the rate decreases from 90% to 80%, yet, it is the highest rate obtained in a dishonest environment.



(a) H1: Accuracy evaluation (b) H2: Accuracy evaluation

Figure 6: Prediction accuracy in H1 and H2 environments

To conclude, varying the value of the initial vector has no effect on the prediction results in honest environments. However, declaring the initialization vector as suspicious is the most accurate when ignoring the nature of the environment.

3) Scalability of the prediction algorithm: We study the accuracy of our predictions in three dishonest environments of 100 nodes, 200 nodes and 300 nodes respectively as shown in Figure 7. Figure 7a, Figure 7b and Figure 7c represent the initial distributions of the networks. All of the initial distributions show a remarkable overlap between honest and malicious nodes with an average 40% of misclassified nodes. Figure 7d, Figure 7e and Figure 7f are the limit distributions in which most of the malicious nodes misclassified in the initial distribution are correctly classified in the predictions. We increase the number of nodes and classify them into correctly classified and misclassified nodes to quantify the scalability of the approach. In Figure 8, we use an incomplete version of our solution (without the prediction phase) denoted "No-sec approach" to show the efficiency of our approach in terms of correct classification despite the increase of nodes number. On average, we manage to correctly classify more than 75% of the nodes. Thus, we consider that our approach is efficient for the early detection of dishonest nodes. However, increasing the number of nodes may have a slight impact on the prediction results for the nodes with suspicious behavior.

4) Evaluation of the energy consumption and the time execution cost : Figure 9a illustrates the required time to execute several types of transactions in our approach. In Ethereum, a new block of transactions is created approximately every 15 seconds. However, we calculated the total execution time including the time to check the rights and display the response and conclude that in all cases our approach is slightly slower. Figure 9b illustrates the energy consumption evalution of our approach. In this figure blue bars represent the necessary energy cost to execute different types of transactions in our approach. While orange bars represent the same transactions' execution of our approach with only static authorization mechanism we denoted “no-sec approach”. To provide a comprehensive evaluation, we performed the same transactions we used for the time execution analysis. Next, we analyzed their related computational consumption. Transactions in Ethereum are measured using the Gas metric and estimated in Ether or Wei. As expected, our approach shows to be consuming more gas compared to the" no-sec approach". The additional computational effort introduced by our method is in average 0.04 MilliEther per storage and 0.1 MilliEther per retrieving transaction. Even though the retrieving transaction cost is higher than the storage transaction, it is still considered small, since 0.1 MilliEther is equivalent to 0.052 dollars. However, the consumption rise is due to the fact that the security functions execution are considerably changing the state of the smart contracts updating the access control permissions, and the miners states. Consequently, the energy computing cost in our operations are proportional to the changes in the states of the smart contracts. In the same figure is illustrated the authorization smart contract deployment costs in our approach and in the "no-sec approach". The results show that we consume in average between 30% and 40% more than the "no-sec approach" deploying a smart contract.To conclude, high fees and additional time execution are considered insignificant compared to the security we guarantee, especially considering that smart contracts are often deployed only once.

5) Comparison with other trust based approaches: Figure 10 illustrates a comparison of malicious nodes' detection between our proposal and the works of Duma *et al.* [9] and Meng *et al.* [10] we mentioned earlier. We remark that the trust values decreased under all the propositions to reach the minimum threshold of each approach. However, we notice that the curve in Meng et al. proposal goes down faster than ours, this shift is due to the difference of the adopted trust models. Overall, under the same conditions, our approach can achieve better performance detecting first the malicious behavior.

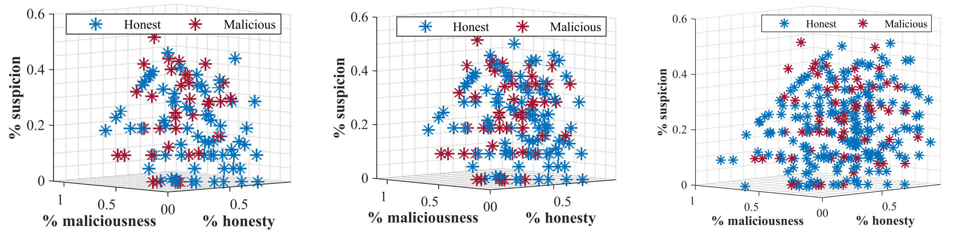
6) Security evaluation: Table II summarizes the security requirements to which our approach responds.

Table II: Security requirements evaluation

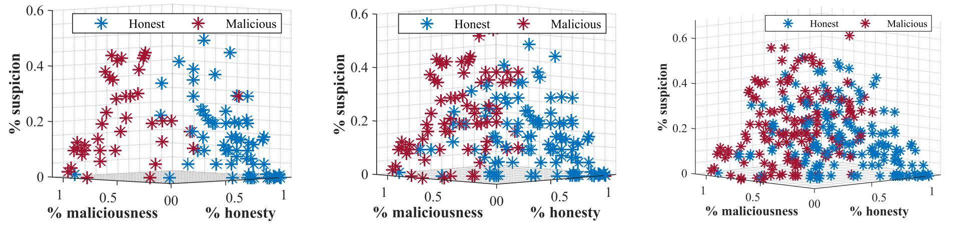
Security requirement	Employed safeguard
Integrity	- Cryptography and hash mechanisms. - Defined contextual and logic rules.
Availability	- Blockchain decentralized topology.
Non-repudiation	- Blockchain signature and time stamp.
Authorization	- Probabilistic detection of malicious nodes. - Stochastic prediction of malicious nodes.

V. CONCLUSION AND FUTURE WORKS

Attackers arer only external entities, they are now hiding among the medical teams. In this paper, we proposed a distributed trust management architecture based on a dynamic authorization mechanism combining probabilistic classification and stochastic modelling to manage the nodes access rights in a fully decentralized way and limit efficiently insider attacks. To evaluate the performance of our proposal, we simulated the behavior of both honest and dishonest healthcare institutions. Results showed that our approach can efficiently detect the malicious nodes. In addition, compared to other trust based models, our approach proves to be more reliable in classification and faster in detection. In the future, we are considering several directions: the first is to include a method that determine dynamically appropriate trust intervals according to the behavior of the group to avoid overlaps between the states; the second is to consider integrating external parameters in the evaluation process such as feedback.

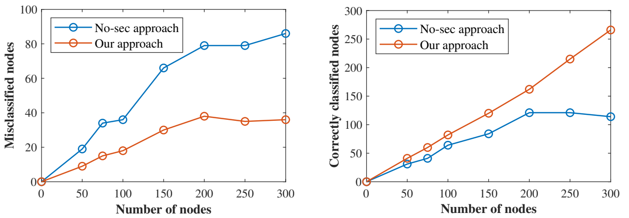


(a) Initial distribution: 100 nodes (b) Initial distribution: 200 nodes (c) Initial distribution: 300 nodes



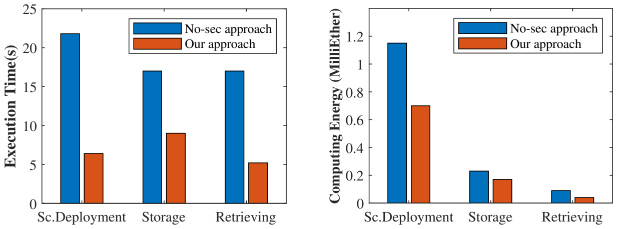
(d) Limit distribution: 100 nodes (e) Limit distribution: 200 nodes (f) Limit distribution: 300 nodes

Figure 7: Impact of varying the number of nodes on the behavior prediction results in a dishonest environment



(a) Misclassified nodes (b) Correctly Classified nodes

Figure 8: Scalability evaluation in a dishonest environment



(a) Execution time evaluation (b) Energy computing evaluation

Figure 9: Computation power and time cost evaluation

ACKNOWLEDGMENT

This work is partly supported by grants from the Troyes University of Technology and financed by CD10 and by the research RETRO project, which is financed by the European Union FEDER.

REFERENCES

[1] SUN, Wencheng, CAI, Zhiping, LI, Yangyang, et al. Security and privacy in the medical internet of things: a review. Security and Communication Networks, 2018, vol. 2018.

[2] EVANS, Mark, HE, Ying, LUO, Cunjin, et al. Employee perspective on information security related human error in healthcare: Proactive use of IS-CHEC in questionnaire form. IEEE Access, 2019, vol. 7, p. 102087-102101.

[3] NAKAMOTO, Satoshi et BITCOIN, A. A peer-to-peer electronic cash system. Bitcoin.–URL:https:bitcoin. org/bitcoin. pdf, 2008.

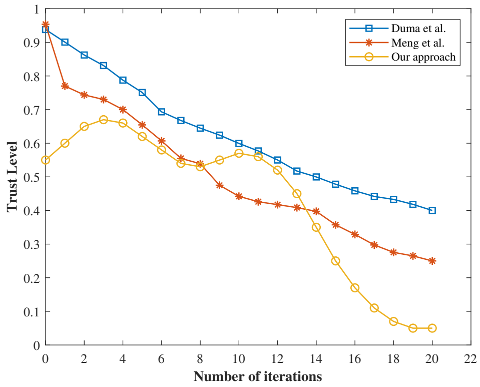


Figure 10: Average detection results comparison

[4] GUO, Shaoyong, HU, Xing, GUO, Song, et al. Blockchain meets edge computing: A distributed and trusted authentication system. IEEE Transactions on Industrial Informatics, 2019.

[5] DUKKIPATI, Chethana, ZHANG, Yunpeng, et CHENG, Liang Chieh. Decentralized, blockchain based access control framework for the heterogeneous internet of things. In : Proceedings of the Third ACM Workshop on Attribute-Based Access Control. 2018. p. 61-69.

[6] LIN, Iuon-Chang et LIAO, Tzu-Chun.A survey of blockchain security issues and challenges.IJ Network Security,2017,vol.19, no5, p.653-659.

[7] NOVO, Oscar. Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE Internet of Things Journal, 2018, vol. 5, no 2, p. 1184-1195.

[8] DORRI, Ali, KANHERE, Salil S., JURDAK, Raja, et al. Blockchain for IoT security and privacy: The case study of a smart home. In : 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops). IEEE, 2017. p. 618-623.

[9] DUMA, Claudiu, KARRESAND, Martin, SHAHMEHRI, Nahid, et al. A trust-aware, p2p-based overlay for intrusion detection. In : 17th International Workshop on Database and Expert Systems Applications (DEXA'06). IEEE, 2006. p. 692-697.

[10] MENG, Weizhi, LI, Wenjuan, et ZHU, Liqiu. Enhancing Medical Smartphone Networks via Blockchain-Based Trust Management Against Insider Attacks. IEEE Transactions on Engineering Management, 2019.

[11] LU, Zhaojun, LIU, Wenchao, WANG, Qian, et al. A privacy-preserving trust model based on blockchain for VANETs. IEEE Access, 2018, vol. 6, p. 45655-45664.