Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 192 (2021) 1081–1091

Procedia Computer Science

www.elsevier.com/locate/procedia

25th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems

A New Blockchain-Based trust management model

Mariam Masmoudi[a,*], Corinne Amel Zayani[a], Ikram Amous[a], Florence Sèdes[b]

[a]MIRACL Laboratory, Sfax University, Sfax, Tunisia
[b]IRIT Laboratory, Paul Sabatier University, Toulouse, France

Abstract

Nowadays, special attention is directed to trust issues in the Decentralized Online Social Network (DOSN). In a distributed system for social networking, interactions and collaborations can be unreliable because some users resort to malicious behaviors in order to increase their trust values in the network to be chosen later by others, and launch trust-related attacks. In this unreliable situation, users will not be able to estimate the trustworthiness of the received social services' list of recommendations. Hence, a trust management model becomes a necessity in order to overcome its trust-related attacks and to recommend trustworthy social services. In this respect, we propose a new trust management model that helps prevent trust-related attacks in order to ensure a reliable environment. Towards this end, our suggested model implements a new technology, called blockchain. Based on the studied trust-related attacks, we intend to add logical security to blockchain since this technology takes into account only the physical security. Evaluation values show the effectiveness of our model.

Keywords: Trust management model; Trust-related attacks; Blockchain technology; Decentralized Online Social Network (DOSN); Consensus protocol; Classification technique.

1. Introduction

Thanks to its myriad benefits and capabilities, internet has given rise to Online Social Networking (OSN), which has dramatically affected every aspect of human life during the last century by providing users with useful information and social services [20]. The latter is an online platform which users use to build social relationships with others to exchange and share various types of content online [8, 6] such as, similar interests, activities, backgrounds, digital photo or video, real-life connections, etc. However, some social services can be untrustworthy. The recommendation-based trust become a solution. Thus, in our previous research studies achieved by our team, Kalai et al., [12] offered a mechanism called LoTrust (Level of Trust) in a social environment that helps calculate the user's trust degree in the network in order to recommend appropriate and trustworthy services to a given user.

* Corresponding author
E-mail address: mariam.masmoudi19@gmail.com

1877-0509
10.1016/j.procs.2021.08.111

Recently, OSN advances lead to a new level of communication called the Decentralized Online Social Network (DOSN) [8]. This network has emerged to overcome both centralization and security problems encountered in OSN. DOSN is therefore an attractive new trend with various advantages. Despite its multiple strengths, DOSN faces a number of issues that reduce the quality of its performance in recommending trustworthy social services as well [21, 6]. Indeed, interactions pose trust-related issues, since some users resort to malicious behaviors and carry out trust-related attacks in order to be chosen by other users by either promoting their trust values or reducing the trust values of benevolent users in the network. These attacks can cause irreversible damage, disrupt the system and reduce its effectiveness [2]. In addition, its preclude a service requester to estimate the reliability of the received list of recommendations and choose trustworthy users and social services [16]. The absence of a trust management model [2] leads to recommending malicious social services. This is why in our previous works [1, 3, 16], in order to recommend a trustworthy social services, we offered a trust assessment mechanism named the Multi-Dimensional Trust-Model for Dynamic, Scalable and Resources-efficient Trust-Management (DSL-STM) was provided. It can detect trust-related attacks produced by malicious users using the classification technique.

This work aims at improving recommendation approaches based on a new trust management model that helps prevent all types of trust-related attacks to ensure better recommendations of trusted users and social services. Our suggested model implements the new technology, known as blockchain. Based on the studied trust-related attacks, we intend to add logical security to blockchain since this technology takes into account only the physical security, including cryptography, transparency, immutability, etc.

The major contributions of this paper are as follows: i) to propound a motivating scenario in the E-learning field since it is one of the most interesting fields nowadays due to the COVID-19 pandemic and ii) to suggest our trust management model based on blockchain technology which aims to prevent trust-related attacks by using a new consensus protocol named PoTA and implementing our proposition.

The remainder of the paper is organized as follows: In section 2, we review several related works in an attempt to identify the main gaps. In section 3, we propound a motivating scenario in the E-learning field, where the learner wants to find a suitable online course to be able to pass his/her exam with excellence. In this case, a trust management mechanism is required in order to help the student make the right decision and select the most reliable online course. In section 4, we display our solutions based on blockchain for trust-related attacks prevention. We also introduce our consensus protocol named the Proof of Trust-related Attacks (PoTA) based on the classification technique. In section 5, we discussed experimental results. Finally, conclusions and future directions will be drawn in Section 6.

2. The state of the art

Recently, special attention is directed to DOSN [8], which is a distributed system for social networking that offers a set of social services to different users. However, some services can be malicious as some users resort to malicious behaviors and launch the so-called “trust-related attacks”. Their main objective is to highlight the recommendation list of trusted users and trustworthy social services. For instance, tutor(s) are users and social services can be a course, video, web services, etc. in the e-learning field. This is why in our previous works achieved by our team, we studied the recommendation-based trust model in a social environment. The study conducted by Kalai et al., [12], offered a mechanism called LoTrust (Level of Trust) which calculates the user’s trust degree in the network to recommend appropriate and trust-worthy services to a particular user. Abdelghani et al., [1, 3] and Masmoudi et al., [16], suggested a trust assessment mechanism called a Multi-Dimensional Trust-Model for Dynamic, Scalable and Resources-efficient Trust-Management (DSL-STM) that can detect trust-related attacks produced by malicious users using the classification technique.

The major purpose of this study is to improve previous recommendation approaches. Since, just detecting such attacks is not an effective solution. In fact, we need other means to mitigate or eliminate these attacks [13] at the transaction generation level i.e. timely detecting and eliminating new attacks. This is called attack prevention. For this reason, [4] put forward a trust management model based on the kalman filter[1] technique. This model allows only to

[1] Is an algorithm that utilizes a series of measurements observed over time, to produce estimates of unknown variables that tend to be more precise than those based on a single measurement

prevent On-Off Attacks (OOA). Recall that some attacks are more dangerous than others in the context in which they have been applied [16]. Therefore, a new trust management model is necessary in order to help prevent all types of trust-related attacks (Bad-Mouthing Attack (BMA), Ballot stuffing Attack (BSA), Self-Promoting Attack (SPA), Discriminatory Attack (DA), Opportunistic service Attack (OSA) and OOA attack) to achieve a better recommendation of trusted users and social services.

The literature based on the trust-related attacks [15, 24, 9, 25, 4] are only related to the precept of the logical security. In order to take into account also the physical security, particularly the blockchain technology has attracted the attention of diverse researchers thanks to its enormous benefits in myriad fields, such as finance, health care, banking [14] and e-learning [17] with its massive use and adoption [11]. it gave satisfactory outcomes on attenuating physical security risks [19] based on these features: i) immutability in which validated transactions cannot be changed or removed, ii) transparency [23] in which all transactions are visible to all the nodes on the network, iii) auditability which refers to the possibility of checking any block at any time for correctness and iv) cryptography in which all transactions are encrypted based on the SHA256 function (hash algorithm) and signed by public and private keys of both transmitters and receivers [2].

Nonetheless, Blockchain does not take into account the logical security grounded in the studied trust-related attacks. In the E-learning field, for example, a learner can make transactions with public and private keys and the transactions are validated. However, in reality these transactions can be seen as attacks. This is why we suggest in this work to add logical security to the blockchain technology to be able to prevent different trust-related attacks, i.e If a malicious transaction is detected it will not be validated.

Before delving into further details of our solution, it is important to define this technology. Blockchain referred to a Distributed Ledger Technology (DLT) that was invented by Satoshi NAKAMOTO in 2008 [18]. It is technically composed of an unlimited number of chained blocks [14]. Each block consists of two components. The first component represents the block header. It includes data related to the block, such as the timestamp, transaction hash, the hash of the previous block, etc. The second component, however, displays the block body. The latter involves the recorded transaction, which can be monetary transactions, users' interactions in a network, etc. The transaction is examined and validated by validation rules that are set by developers from the beginning [3]. These rules are also named a "consensus protocol". The latter is defined in [5] as "a series of steps to approve a proposed state or value by all or most miners".

Several consensus protocols have been employed in the literature. Among these protocols, we can cite Proof of-Work (PoW), Proof-of-Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), etc [4]. Yet, according to [7], the existing consensus protocols are not suitable in a social network context. For this reason, some researchers have offered their own consensus protocols to fulfill their needs and objectives [7, 26, 22, 27]. However, a major challenge is to find a proper consensus protocol that is applicable to the trust-related attack prevention. As a result, a novel consensus protocol for preventing trust-related attacks becomes a necessity.

3. Motivating scenario

To further explain the effect of trust-related attacks on E-learning, we suggest a scenario in the E-learning field since it is one of the most interesting fields nowadays due to the COVID-19 pandemic.

With the appearance and spread of this pandemic all over the world, it has been found that lock-down is the only best option to control and defeat this corona-virus. Yet, this solution has negative impacts on education. In order not to miss the academic year, the ministry of education motivated teachers and students to rely on e-learning as the best solution in these circumstances. Accordingly, in the revision period, a student called "user1" encountered some difficulties in revising her course. For this reason, she looked for an online course to understand her lesson and pass the exam. Since she has no international cards like PayPal, MasterCard or Visa to pay the fees, she prefers to find and have an access to such free courses. To obtain an online course, she will launch a request **Req** depending on her specific preferences **Req = (course name or keywords)** via her device. The latter can be a smartphone, smart-board, tablet, videoconferencing tool, etc. As a result of her query, user1 receives a list of social services according to the request

[2] https://www.ledger.com/academy/blockchain/what-are-public-keys-and-private-keys
[3] https://medium.com/ignation/pulling-the-blockchain-apart-the-transaction-life-cycle-7a1465d75fa3
[4] https://medium.com/coinmonks/implementing-pbft-in-blockchain-12368c6c9548

and her social relations as shown in Figure 1. Among these services, we can mention edx, Udemy, Mooc, a YouTube channel that offers online courses and training sessions, etc. With this diversity of choices, the student will not be able to estimate the reliability of the received services and select the most reliable and relevant service. Considering that some malicious users who want to propagate malicious behavior can be found in this list, this student might make a wrong choice. These malicious users can spread false information and ideas which cause learners' deception. Besides, they don't care about learners. Instead, their unique goal is to make money. In addition, viruses can be also spread for more serious reasons, such as messing up, ruining devices or violating learners or users' personal information, etc. The presence of malicious users among the recommended list to user1 can be attributed to their high trust value in the network. This obtained value is due to dishonest votes, also called trust-related attacks. Indeed, certain users (tutors) can either boost their trust value or reduce the trust value of other users [16] in the network by applying trust-related attacks [3], such as SPA or BMA as shown in Figure 1. Hence, their services will be selected and used by other users. In order to avoid the problem of recommending malicious social services, a trust management mechanism [2] becomes a necessity. In fact, this model aims at preventing attacks. Thanks to this model, we will help user1 to make the right choice.

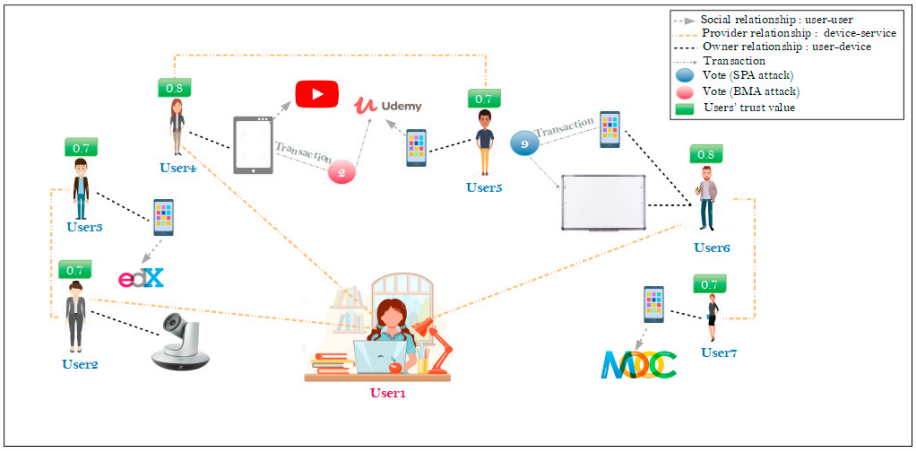

Fig. 1: Example of scenario in the field of E-learning

4. Trust-related attacks prevention blockchain-based

As mentioned above, our major objective is to propose a trust management model based on the blockchain technology in order to prevent trust-related attacks. Our work aims at adapting this technology and its operational steps of validating transactions and adding logical security to be able to prevent these attacks. In what follows, we provide a detailed schema of the two major phases of our architecture. The offline phase defines the rules for classifying transactions. However, the on-line phase predicts the label (attack's type or none-attack) of a new transaction to make the decision of either validating or rejecting this transaction.

4.1. Off-line phase

As shown in Figure 2, we will pick out the transaction components that allow us to predict whether the transaction is an attack or not. Then, a data-set will be generated based on these components and attack types. The aggregation phase consists in applying a learning algorithm on the data-set in order to generate a classification model that permits us to classify transactions. This model will be employed in the next on-line phase in order to predict the new transaction label.

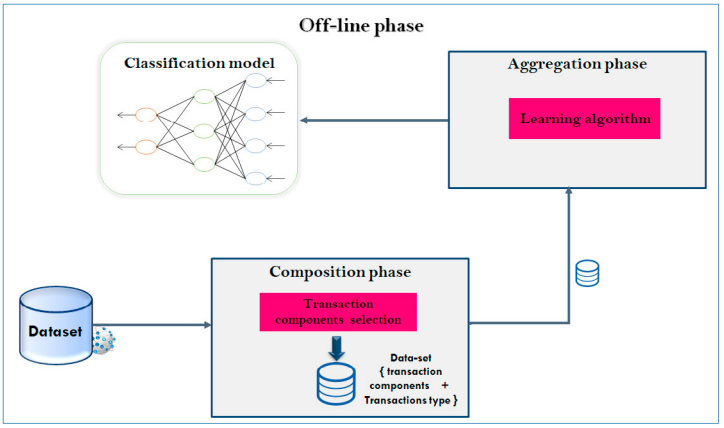

Fig. 2: Off-line phase

4.2. On-line phase

Following the transaction request, in the dialing phase as shown in Figure 3, a new transaction will be created based on the proposed transaction components and added to a new block that will be propagated and examined by our new photo protocol. Thus, based on the classification technique, our online processing-based protocol will be applied in the aggregation phase. In fact, we will exploit the model created in the previous online phase in order to classify the new transaction. If the protocol's result gives a none-attach, the transaction will be either validated and added to the existing blockchain technology or rejected.

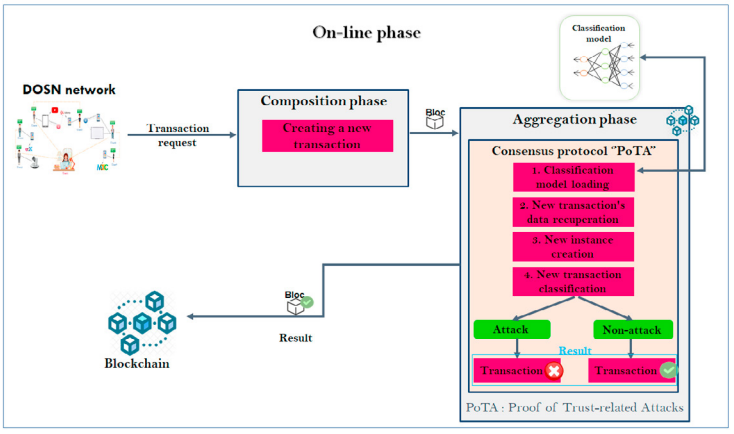

Fig. 3: On-line phase

4.3. Proof of Trust-related Attacks (PoTA)

Building upon the idea of using the consensus protocol as the underlying solution to prevent trust-related attacks, this paper proposes a novel consensus protocol that meets our goal. The new consensus protocol is called Proof of Trust-related Attacks (PoTA).

As we mentioned earlier, our primary goal is to timely predict and prevent a new attack (a malicious transaction). Recall that the classification technique has given very satisfactory results in the attack detection task. In this respect, in our previous studies [3, 16], we approved that the classification technique is capable of analyzing users' behaviors by classifying their interactions into several classes. Thus, we propose to use the classification technique in our consensus

protocol. The latter comprises four different steps as shown in Figure 3. Step 1 consists in loading the classification model, created in the Online phase, that helps us classify new transactions (an attack or a none-attack). Then, once the classification model is loaded, we will restore the transaction data existing in the new block. In the third step, we will create a new instance suitable for not only the instances already used in training phase, but also the classification model designed in the online phase. Finally, we will launch a predicted function to assign a label to the new transaction (either an attack (BMA, BSA, SPA, DA, OSA and OOA) or a none-attack). According to the obtained label, we will take the final decision (either to validate the transaction or to reject it). In the validation case, the transaction will be added to the existing blockchain in the new block. Then, the transaction will be added to a Blacklist and the malicious user will be blocked from the network.

4.4. Transaction components

Transaction components are derived from the description of each attack type. They describe and determine user's behaviors (to predict whether the generated transaction is a trust-related attack or not). In our previous works [3, 16] we set forth seven distinct features. The latter aim to detect attacks (BMA, BSA, SPA and DA) in the online mode leading to satisfactory results with f-measure values equal to 92.8% and 95.03% respectively. However, our purpose is to prevent all types of trust-related attacks (BMA, BSA, SPA, DA, OSA and OOA). Therefore, features will be modified and improved in order to meet our objectives and ameliorate the prediction accuracy of malicious transactions. We present each component as follows:

- **Quality of provider, User Similarity, Rating-Frequency and Rating-trend:** We will reuse these features that were explained in detail in our previous works [3, 16].
- **Vote:** The value of the vote **V(Ui, Sk)** given by the user Ui to the service Sk of the user Uj. We assume that the vote scale ranging from 1 to 10: with a low voting rate (between 1 and 3) and a high voting rate (between 7 and 10).
  To the best of our knowledge, trust-related attacks are dishonest votes [3, 16] that are performed by some users in order to be chosen as service providers by either promoting their trust values in the network or reducing the trust values of benevolent users. Hence, a vote can be considered as a primary component.
- **Trust value:** The overall trust value of the user Ui in the network. It is designated by **TrV (Ui)** and recalculated after each validated transaction (not an attack) according to the following equation:

$$\mathbf{TrV(U}_i) = (TrV0(U_i) + V(U_j, S_k)/10)/2$$

With TrV0(Ui): previous trust value; V(Uj, Sk): vote assigned by user Uj to the Sk service.

- **Vote's similarity:** The similarity S between the vote V given by the user Ui to the service Sk and the other votes Vl provided by the other users in the network. It is denoted by **VoteSim(V, Vl)** and calculated by the Euclidean distance according to the following equation:

$$\mathbf{VoteSim(V,Vl)=} \sqrt{\sum_{i=1}^{n} (Vl_i - V)^2}$$

With V: the new vote given by the user Ui; Vl: votes given by other users.

According to [10], dishonest votes are usually either lower or higher than the majority of the other votes.
If VoteSim(V, Vl) is near, the vote is at a near distance, the vote will be considered similar. And if VoteSim(V, Vl) is far, the vote will not be considered similar.

5. Implementation and Experimentation

To successfully implement our blockchain and consensus protocol (PoTA) in the on-line phase, we must first apply our classification model in the online phase in order to define the rules for transaction classification (either attacks or none-attacks). In this section, we will present not only our implementation and the classification results obtained, but also our blockchain and protocol PoTA.

5.1. Dataset

Since real data are unavailable, myriad works in the literature offered experiments based on simulations. In our work, we assessed the performance of our classification model based on simulations applied to a real dataset named "Sigcomm[5]". It contains 76 users, their profiles and their lists of interests. Sigcomm also includes social relations between users, the transactions between them and the proximity of each couple of users.

We generate one or more devices for each user. Then, we divide the user's transactions by his devices. The resulting data-set is composed of 76 users, 300 devices, 364 services, 711 users' interests, 531 social relationships between users, 32000 transactions between users and 285788 proximities. Based on this dataset, we performed simulations in order to generate different instances composed of various features and classification classes. These instances are transactions that can be either none-attacks or one of the trust-related attack types. Taking the example of a SPA attack as illustrated in Figure 1, the malicious user 6 who has two different devices a connected white board (D1) and a smartphone (D2). This malicious user will try to boost his own trust value by performing the SPA attack. He will invoke his service provided by D1 and assign good votes such as 9 or 10 using D2.

After performing simulations, we generated a CSV file, which includes 620 transaction instances as shown in table 1. The OOA After performing simulations, we generated a CSV file, which includes 620 transaction instances as shown in table 70% in the learning phase and 30% in the testing phase.

Table 1: Our data-set

Attack type	Number of instances
BMA	85
BSA	80
SPA	145
DA	110
OSA	310
OOA	165
non-attack	200

5.2. Learning Method

In the first step, we utilized the weka tool to try different supervised algorithms, such as the decision table, SVM, the perceptron, etc. Based on the obtained results, we chose the SVM algorithm which performed the best results. Then, we implemented the SVM algorithm using the PyCharm tool based on Python in order to build our classification model. We also employed the Anaconda navigator to manage the required libraries, such as pandas, sklearn, pickle, etc. Once this algorithm is trained, the model will be created and saved using the '.sav' extension.

5.3. Experimental Model for blockchain

This part shows the main outcome of the simulation experiment in order to check whether blockchain can prevent trust-related attacks or not.

1. **Initial setting**
   As senders, we generate a public address called a "public key" (the equivalent of a RIB). The latter is a sequence of about 34 characters comprising numbers and letters in upper and lower case forms, such as 040e981d2C283a4e90045d945A00978g56. We also create another sequence named a "private key" (the equivalent of a bank card code, that you should neither give nor lose it), to be able to sign and authorize the sending of the transaction. For a receiver, a public key must be generated to receive the transaction.

[5] https://crawdad.org/thlab/sigcomm2009/20120715/

2. **Sending transaction**
   We should enter the necessary transaction data, such as the vote value, trust values, vote similarity, and other features detailed in the previous sections. Then, the transaction is written.
3. **Assembling transactions into a new block**
   Once the transaction is written, it will be entered in a new block that contains transactions not yet validated. A simple block will not be suitable for the trust issue discussed in this study. Hence, an improvised block structure is proposed as a solution for preventing trust-related attacks. Each block is made up of a cryptographic summary of the previous blocks and transactions. This summary, known as hash, is obtained by applying the function SHA256 (a hashing algorithm) [6] and transactions.
4. **Transactions validation**
   A block is transmitted to the new consensus protocol called Proof of Trust-related Attacks (PoTA). It will examine the transaction and check the veracity and trustworthiness of the generated transaction [7]. i.e., is the sent vote honest or not? is it an attack or not? which type of attack? Based on the obtained results of each transaction, the protocol will take the decision (either to validate the transaction or to reject it).
5. **Block addition** Once the block is validated, it will be added to the existing blockchain [8]. But, if the transactions are considered as attacks, they will be rejected and not stored on the blockchain.

At the implementation stage, we used PyCharm tool based on Python and anaconda navigator to manage the required libraries, such as Crypto, SHA, etc. Besides, we used Flask to interact with blockchain via GET and POST requests. First, we implemented the consensus protocol PoW and blockchain. Then, we made another version with our proposed protocol PoTA to compare between them.

5.4. Evaluation Metrics

To evaluate the relevance of our model, we will apply the most commonly used measures in the classification problems, namely F-measure, Recall and Precision. In contrast, for our Blockchain, will use the prediction rates of malicious transaction metrics and Transactions Per Second (TPS)[9].

5.5. Experimental Results for our classification model

These experiments are done to chose the best algorithm to predict all types of trust-related attacks. Indeed, we exploited different supervised algorithms, such as the decision table, SVM, perceptron etc. Based on the obtained results, we chose the SVM and decision table algorithms since the other algorithms did not give us satisfactory results. Figure 4 shows that the SVM algorithm has the best results in predicting each type of trust-related attacks relative to the decision table algorithm and especially for the three types of BMA, BSA and DA attacks with an f-measure value of 99.7%. Likewise Figure 5 proves that the SVM algorithm has the best performance in terms of f-measures, precision and recall in predicting all types of trust-related attacks.

For a technical evaluation, we will compare the results obtained by our classification model with our previous work in [16]. Our choice of [16] is justified by the fact that we treated the same attacks types (BMA, BSA, SPA, DA and OSA) and we used the same dataset (Sigcomm). However, our Classification model and the model of [16] utilized different features in order to predict the attacks types as mentioned in section 4.4 since we do not have the same work objectives. The Figure 6 delineates in details this comparison. Compared to [16], our classification model was able to obtain a better values in terms of recall, precision and f-measure where respectively 99,6%, 99,7% and 99,6%. Yet, for [16], the recall, the precision and f-measure are respectively 94,4%, 95,6% and 94,3%. According to these outcomes, we can notice that this new classification model improves our previous work [16] with 5,22% in term of F-measures. Therefore, we can conclude that our classification model will improve the prediction accuracy of the launched attacks

[6] https://www.ledger.com/academy/blockchain/what-are-public-keys-and-private-keys
[7] https://www.ledger.com/academy/blockchain/what-is-proof-of-work
[8] https://medium.com/futurs-io/comprendre-la-blockchain-1-3-les-concepts-clés-d2de94e06112
[9] Transactions per second (TPS) is a measurement that represents the number of transactions completed in one second by an information system.

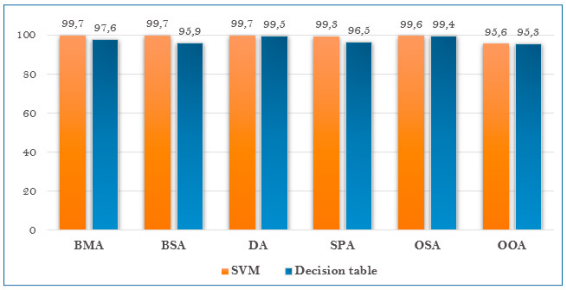

Fig. 4: Prediction of each trust-related attack's type

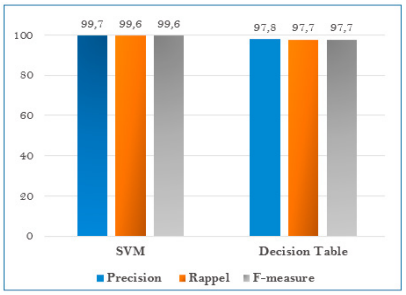

Fig. 5: Prediction of all trust-related attacks' types

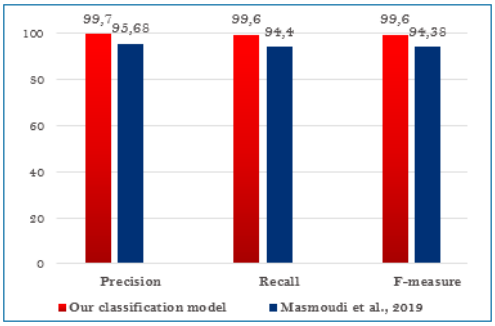

Fig. 6: Comparison of our classification model and Masmoudi et al., [16]

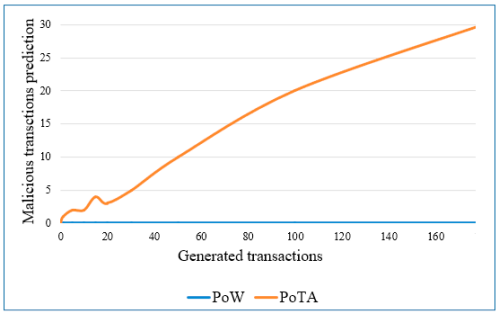

Fig. 7: The prediction rate of malicious transactions

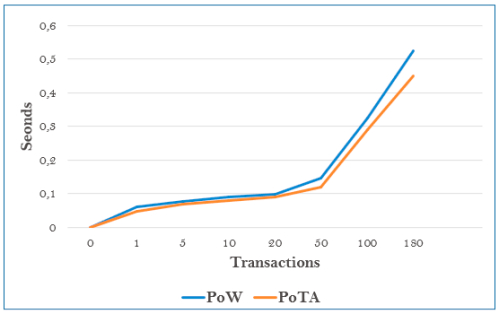

Fig. 8: Transactions validation per second

to prevent malicious transactions. And can confirm the good choice and performance of our model in predicting the attacks types.

5.6. Experimental Results for our consensus protocol PoTA

Remember that our suggested new consensus protocol PoTA based on the classification model presented in the subsection 5.5.

To proves the ability of our Protocol PoTA, a comparison will be performed between this protocol and the benchmark protocol (PoW). Figure 7 proves that PoW is not capable of predicting the studied attacks and all the generated transactions will be validated and added to the existing blockchain. On the contrary, our protocol PoTA has the best performance in terms of predicting malicious transactions which will not be added to the blockchain. Since our classification model did well in predicting attacks this is why our protocol is capable of not validating malicious transactions. Therefore, we can conclude that our protocol will improve trust-related attacks prevention i.e to ensure the logical security of the blockchain technology.

Besides, to demonstrate the ability of our protocol (PoTA) in completing transactions as soon as possible i.e the transaction number per second, a comparison will be performed between this protocol and the benchmark protocol (PoW). Figure 8 shows the obtained results. Thus, we can notice that PoTA is able to complete more transactions compared to PoW in less time.

After this comparison, we can conclude that the innovation of our work can be summarized as follows: To the best of our knowledge, this is the first work that deals with the prevention of all types of trust-related attacks (BMA, BSA, SPA, DA, OSA and OOA. Besides, we have taken into account the logical security to the blockchain technology to be able to prevent different trust-related attacks.

6. Conclusion and perspectives

In this paper, to ensure a trustworthy DOSN environment, we suggested a new trust management model based on the blockchain technology. To the best of our knowledge, this is the first work that deals with the prevention of all types of trust-related attacks (BMA, BSA, SPA, DA, OSA and OOA). Besides, we have taken into account the logical security to the blockchain technology to be able to prevent these attacks. This prevention is done by a novel consensus protocol named PoTA. This protocol is based on the classification technique to figure out if the performed transaction is an attack or not and to make the decision of either validating or rejecting the transaction. According to the experimental results, we showed the performance of our classification model in predicting malicious transactions with an f-measure value of 99,6% comparing to our previous work [16] (94,3%).According to these results, we can notice that this new model improves our previous work [16] with 5,22% in term of F-measures. Moreover, we notices that our protocol PoTA has the best performance in terms of predicting malicious transactions which will not be added to the blockchain and will improve trust-related attacks prevention i.e to ensure the logical security of the blockchain technology. Besides, our new protocol is able to complete more transactions compared to PoW in less time. Nevertheless, in this work we have discussed the implementation and experimentation of our PoTA in preventing trust-related attacks. Likewise, we tried our proposed model based on simulations applied to a real dataset. In our future work, our attention will be directed to increasing the number of our database instances obtained after simulations and implementing a real scenario that will permit us to evaluate our protocol.

Acknowledgements

This work was financially supported by the PHC Utique program of the French Ministry of Foreign Affairs and Ministry of higher education and research and the Tunisian Ministry of higher education and scientific research in the CMCU project number 18G1431.

References

[1] Abdelghani, W., 2020. A multi-dimensional trust-model for dynamic, scalable and resources-efficient trust-management in social internet of things. Ph.D. thesis. Université de Toulouse, Université Toulouse III-Paul Sabatier.
[2] Abdelghani, W., Zayani, C.A., Amous, I., Sèdes, F., 2016. Trust management in social internet of things: a survey, in: Conference on e-Business, e-Services and e-Society, Springer. pp. 430–441.
[3] Abdelghani, W., Zayani, C.A., Amous, I., Sèdes, F., 2018. Trust evaluation model for attack detection in social internet of things, in: International Conference on Risks and Security of Internet and Systems, Springer. pp. 48–64.
[4] Abderrahim, O.B., Elhdhili, M.H., Saidane, L., 2017. Tmcoi-siot: A trust management system based on communities of interest for the social internet of things, in: 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), IEEE. pp. 747–752.
[5] Bashir, I., 2017. Mastering blockchain. Packt Publishing Ltd.
[6] Bok, K., Kim, Y., Choi, D., Yoo, J., 2021. User recommendation for data sharing in social internet of things. Sensors 21, 462.
[7] Chen, Y., Xie, H., Lv, K., Wei, S., Hu, C., 2019. Deplest: A blockchain-based privacy-preserving distributed database toward user behaviors in social networks, Elsevier. pp. 100–117.
[8] Datta, A., Buchegger, S., Vu, L.H., Strufe, T., Rzadca, K., 2010. Decentralized online social networks, in: Handbook of social network technologies and applications. Springer, pp. 349–378.
[9] Ekbatanifard, G., Yousefi, O., 2019. A novel trust management model in the social internet of things, Science and Research Branch, Islamic Azad University. pp. 57–70.
[10] Filali, F.Z., Yagoubi, B., 2015. Global trust: A trust model for cloud service selection.

[11] Iqbal, R., Butt, T.A., Afzaal, M., Salah, K., 2019. Trust management in social internet of vehicles: Factors, challenges, blockchain, and fog solutions, SAGE Publications Sage UK: London, England. pp. 155–177.
[12] Kalaï, A., Zayani, C.A., Amous, I., Abdelghani, W., Sèdes, F., 2018. Social collaborative service recommendation approach based on user's trust and domain-specific expertise. Future Generation Computer Systems 80, 355–367.
[13] Kenkre, P.S., Pai, A., Colaco, L., 2015. Real time intrusion detection and prevention system, in: Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014, Springer. pp. 405–411.
[14] Khan, A.S., Balan, K., Javed, Y., Tarmizi, S., Abdullah, J., 2019. Secure trust-based blockchain architecture to prevent attacks in vanet, Multidisciplinary Digital Publishing Institute. pp. 49–54.
[15] Kumar, J.S., Sivasankar, G., Nidhyananthan, S.S., 2020. An artificial intelligence approach for enhancing trust between social iot devices in a network, in: Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications, Springer. pp. 183–196.
[16] Masmoudi, M., Abdelghani, W., Amous, I., Sèdes, F., 2019. Deep learning for trust-related attacks detection in social internet of things, in: International Conference on e-Business Engineering, Springer. pp. 389–404.
[17] Mikroyannidis, A., Third, A., Domingue, J., Bachler, M., Quick, K.A., 2020. Blockchain applications in lifelong learning and the role of the semantic blockchain, in: Blockchain Technology Applications in Education. IGI Global, pp. 16–41.
[18] Nakamoto, S., Bitcoin, A., 2008. A peer-to-peer electronic cash system, pp. 8–9.
[19] Panarello, A., Tapas, N., Merlino, G., Longo, F., Puliafito, A., 2018. Blockchain and iot integration: A systematic survey, Multidisciplinary Digital Publishing Institute. pp. 25–75.
[20] Ramanathan, A., 2015. A multi-level trust management scheme for the Internet of Things. Ph.D. thesis.
[21] Roopa, M., Pattar, S., Buyya, R., Venugopal, K.R., Iyengar, S., Patnaik, L., 2019. Social internet of things (siot): Foundations, thrust areas, systematic review and future directions. Computer Communications , 32–57.
[22] Shala, B., Trick, U., Lehmann, A., Ghita, B., Shiaeles, S., 2019. Novel trust consensus protocol and blockchain-based trust evaluation system for m2m application services, Elsevier. pp. 39–58.
[23] Smik, B.B., 2018. Blockchain technologies adapted for data manipulation in IoT. Ph.D. thesis. Masaryk University Faculty of Informatics.
[24] Talbi, S., Bouabdallah, A., 2020. Interest-based trust management scheme for social internet of things, Springer. pp. 1129–1140.
[25] Xia, H., Xiao, F., Zhang, S.s., Hu, C.q., Cheng, X.z., 2019. Trustworthiness inference framework in the social internet of things: A context-aware approach, in: IEEE INFOCOM 2019-IEEE Conference on Computer Communications, IEEE. pp. 838–846.
[26] Yahia, Y.O., 2019. A proposal for a security model for the protection of personal data in systems based on the internet of things. Ph.D. thesis.
[27] Zou, J., Ye, B., Qu, L., Wang, Y., Orgun, M.A., Li, L., 2018. A proof-of-trust consensus protocol for enhancing accountability in crowdsourcing services, IEEE. pp. 429–445.