Trust Assessment in Internet of Things Using Blockchain and Machine Learning

Liming Wang
State Grid Jiangsu Electric Power Company
Hongqin Zhu
State Grid Fujian Electric Power Company
Jiawei Sun
State Grid Nanjing Power Supply Company
Ran Dai
State Grid Nanjing Power Supply Company
Qi Ma (maqi@bupt.edu.cn)
Beijing University of Posts and Telecommunications https://orcid.org/0000-0002-6277-3899
Xin Wei
Beijing University of Posts and Telecommunications

Research

Keywords: blockchain, data sharing, deep learning, IoT, trust management

Posted Date: November 19th, 2020

DOI: https://doi.org/10.21203/rs.3.rs-110210/v1

RESEARCH

Trust Assessment in Internet of Things Using Blockchain and Machine Learning

Liming Wang[1], Hongqin Zhu[2], Jiawei Sun[2], Ran Dai[2], Qi Ma[3*] and Xin Wei[3]

[*]Correspondence:
maqi@bupt.edu.cn
[3]School of Computer Science, Beijing University of Posts and Telecommunications, No. 10 Xitucheng Road, Haidian District, 100876, Beijing, China
Full list of author information is available at the end of the article

Abstract

Since IoT devices are strengthened, edge computing with multi-center cooperation becomes a trend. Considering that edge nodes may belong to different center, they have different trust management model, it' s hard to assess trust among edge nodes. In this paper, we take blockchain to coordinate differences among centers, construct a trust environment for transactions in IoT. In detail, we propose a blockchain based identity management for IoT to ensure identity is credible, then design a transaction model to provide certification for IoT transactions. And, we take machine learning methods to analyze IoT transaction log, thus decide trust nodes or not. Experiment results show that our mechanism could effectively identify trustworthy edges in IoT.

Keywords: blockchain; data sharing; deep learning; IoT; trust management

1 Introduction

With development of IoT, more and more devices are involved in network, and ability of devices gets strengthened, which enriches IoT service. Edge computing is a promising technology for current IoT, which could alleviate pressure of cloud by shift tasks to edge. However, deploying lots of edge nodes in wide area would cause enormous costs. Considering that clouds who serve IoT users may have similar needs, edge resource sharing would be a solution for clouds. The solution would not only relieve pressure to cloud and save costs of deploying edge infrastructure, but also improve the experience of IoT users. To achieve this, build trust between edges which belongs to different clouds would be the core issue to solve.

Blockchain is a decentralized ledger technology which can be an ideal solution for multi-center cooperation based trust. In fact, there have been lots of blockchain based IoT trust solution been proposed[1, 2, 3]. However, current blockchain based methods exist lots of problems. First, all data stores on blockchain would cause low efficiency and management challenges, while lack of data sharing would lead to trust difficulties, there is a balance should be considered. Second, research on blockchain based trusted always concentrate on identity authentication and evidence reservation, still lack research for blockchain based trust assessment.

In this paper, we construct a blockchain base cooperation among clouds, design an authenticate mechanism for edge nodes and a transaction data model for IoT service, then propose Machine Learning(ML) based method to assess trust of IoT entity, thus decide trust them or not. Contributions of this paper can be summarized as follows:

1) This paper designs an IoT architecture base blockchain. Clouds endorse their edge nodes, share edge identity by blockchain, nodes propose transaction by smart contract and record results into blockchain, thus a credible environment is constructed.

2) This paper designs a blockchain based authentication method for transactions among edge nodes which belong to different clouds. By design transaction process and model, edge nodes could verify each other easily with blockchain based unified interface. Since transaction result would be recorded into blockchain, the architecture could provide credible data basis for trust assessment.

3) This paper proposes ML based trust assessment algorithm. We compute trust attributes with transaction data in blockchain, then design ML based algorithms to classify trustworthy nodes and un-trustworthy nodes. Evaluations proves that ML can be used to predict trust on the basis of blockchain.

4) This paper compares performance of ML algorithms for trust computation. By taking suitable algorithm, users could classify trustworthy edge nodes precisely. Thus un-trustworthy edge nodes have to behave better to get orders.

This paper is structured as follows: Section 2 describes briefly introduces trend of IoT architecture and ML based trust assessment model. Section 3 describes the IoT architecture base blockchain, whereas Section 4 proposes authentication method and transaction data model. Section 5 details ML based trust assessment algorithm. Numerical results are discussed in Section 6. Finally, concluding remarks are presented in Section 7.

2 Related Work

This part would introduce development of trust management in IoT, and ML based methods for trust assessment.

2.1 IoT and Emerging Technology

With exploding volume of data collected from underlying IoT devices, traditional cloud computing scheme shows a lot of drawbacks. In 2012, fog computing is proposed to extend ability and service of cloud [4, 5]. Soon after, edge computing is proposed to provide more convenient service for IoT users. Then, integration between IoT and edge computing attracts lots of attention. Most of research are proposed to deploy server at edge to reduce delay, while deploy new server is expensive. Then many works tend to operate edge resource: 1) optimizing the resource allocation with information from other entities [6]; 2) offloading tasks by using existed idle resources own to other entity [7]. Both of these solutions have to collaborate with others, then trust become important.

Different with identity authentication in network security, trust management makes services more reliable by ensuring that all communicating devices are trustworthy during service cooperation [8]. Till now, lots of work has been done on trust management in distributed network, such as IoT edge network [9], ad hoc network [10, 11, 12], P2P computing [13], wireless sensor network [14], cloud computing [15] and more [16, 17, 18, 19]. However, these ways always not suitable for the scenario we concerned.

At first, traditional trust computing patterns not concern the assess system' s own reliability, system may get fake data thus make wrong decision. Second, these solutions still rely on centralized management, which is not suitable for wide collaboration in IoT. As a result, blockchain attract lots of attention as a decentralized trusted ledger technology.

To improve reliability of trust system for current IoT, blockchain is introduced to operate edge resource. Cui et al. [7] sets reward for trustworthy edge service and record it into blockchain. Q. Xu and J. Kang et al. designs blockchain based hierarchical identity authentication [20, 21]. Francesco et al. [22] records transactions among IoT into blockchain. J. Kang [23] records data and reputation of car into blockchain. B. Lee et al. [24] check firmware of devices by blockchain for IoT. However, these work take blockchain to authenticate identity of IoT while instead of IoT trust management.

In this paper, we propose a blockchain based trust architecture for IoT transaction, thus enable a reliable trust management method.

2.2 Machine Learning based Trust assessment

ML is an excellent choice to assist in trust evaluation and generate an intelligent model through knowledge learning from the available data. Since blockchain could provide credible data for learning, ML could works better.

Till now, ML based algorithm are always used in trust management especially in crowdsourcing and social networks. Liu et al.[25] proposed a trust framework based on machine learning for large-scale systems to use the previous transactions of agents to infer their trustworthiness. Zhao and Pan et al. [26] applied machine learning approaches into the user trust evaluation scenarios in OSNs, which formalizes trust analysis as a classification problem.

As [27] says, few works have applied ML techniques to solve issues related to IoT security. J. Cañedo et al. [28] proposes a trust assessment mechanism by Artificial Neural Networks to detect anomalies of IoT. M. Miettinen et al. [29] ensure validity of IoT information with neural network.

Since traditional trust assessment methods relies on central management, complex learning method can be deployed. However, decentral cooperation causes lots of data should not be shared and limited IoT devices cannot afford complex computing tasks. Therefore, we try to design ML algorithm which could be easily deployed in limited IoT devices, and analyze their performance by analyzing simplified data.

3 Trusted Architecture

In this part, we propose the blockchain based trust architecture for IoT transaction. The architecture includes three type of roles: cloud, edge, IoT users.

Clouds operate traditional business, perform complex computing tasks. Since different clouds need to construct cooperation to provide more IoT services while cannot trust each other. Clouds can build a blockchain to share information including edge authentication and IoT transaction reserving in a trusted way. And, these data can also help cloud to decide how to arrange edges to serve users.

Edge is IoT agent which supply service to user directly, they communicate with clouds and other edges to support their service.

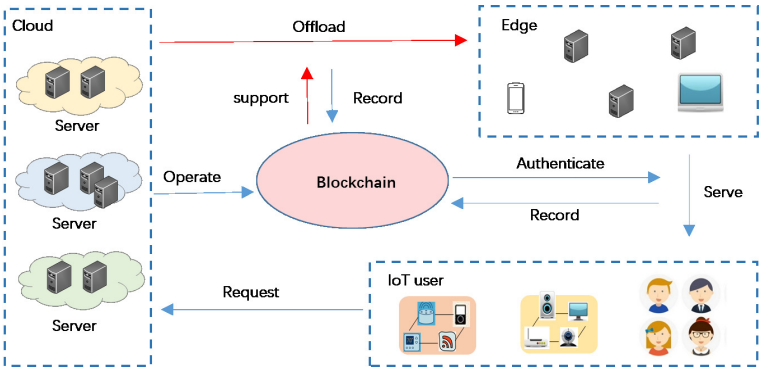


Fig. 1 Architecture

IoT users contains users and devices, they may ask cloud or edge for IoT service, then edge would receive corresponding command. Since most of edge not belong to a common cloud, they need build trust with other edge with help of blockchain.

In our architecture, traditional cloud endorse for the whole system, IoT get legal identity by blockchain, and decide trust others or not by analyzing transaction log in blockchain. Transaction result will be recorded into blockchain to provide credible data basis for future transactions.

Next, we would discuss how to build a trust environment by blockchain at first, then propose trust assessment method on the basis of this architecture.

4 Blockchain Enabled Trust Environment

This part aims to construct a trust environment with blockchain, includes identity authentication process design and transaction model design. Both of them can be encapsulated as smart contracts, edges complete these operations by invoke contracts. We would define operations and design these smart contracts in the following. Identity authentication aims to distribute identity for edges in a unity way, thus different edge can verify each other easily. Identity management include edge register, update, and withdraw.

4.1 Identity Authentication

Table 1 IDENTITY MESSAGE

Parameter	Value
ID	Unique identifier
type	Operation type
Owner	Owner of edge
Pubkey	Public key of the edge
Validity	period of validity
description	Device description
Signature	Signature of who invoke the contract

Each operation includes parameters described as TABLE 1, it is noteworthy that owner field means that the ID will belong it after the transaction has reach consensus, while public key belong to the ID represents, while the message is signed by its current owner. In other word, ID, owner and Signature is related to itself, next owner, and current owner respectively, the three can be different. It is noteworthy

only identity management is verified by its owner, other IoT transaction is verified with its public key.

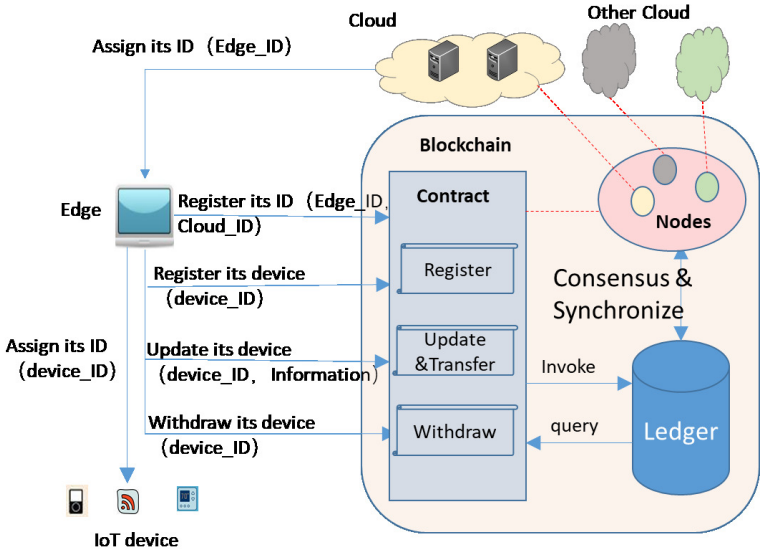


Fig. 2 Identity register process

As Fig.2 shown, traditional cloud assigns legal identity to edge nodes and import this into blockchain. Then, edge nodes manage devices belong to its self and share them by blockchain. Management operations could be divided into three types.

1)identity register

Every entity has identity in blockchain could propose this request to register entity include users and devices it owns. The initial entity is registered in genesis block as basis. In this way, each identity in blockchain is permissioned and has been endorsed by another legal identity.

2)identity update

Identity can be update by its owner. In this way, one can replace devices by update its public key without other complex operation, and transfer device to others by update its owner. In more cases, they need update description to expose information about the device.

3)identity withdraw

In fact, it can be seen as a special update operation. All of information about the device would become invalid. All transactions about this device are recorded into blockchain, including its withdrawn.

4.2 Transaction Model

All transactions among different devices mean that device A ask for help from B. We divide them into two types as following. The first is IoT-A ask IoT-B for data access, while the second is data offloading, IoT-B cache data for IoT-A. We design them as following.

4.2.1 data access control

In this scenario, IoT-A has data collection ability while IoT-B not, this transaction need 3 steps.

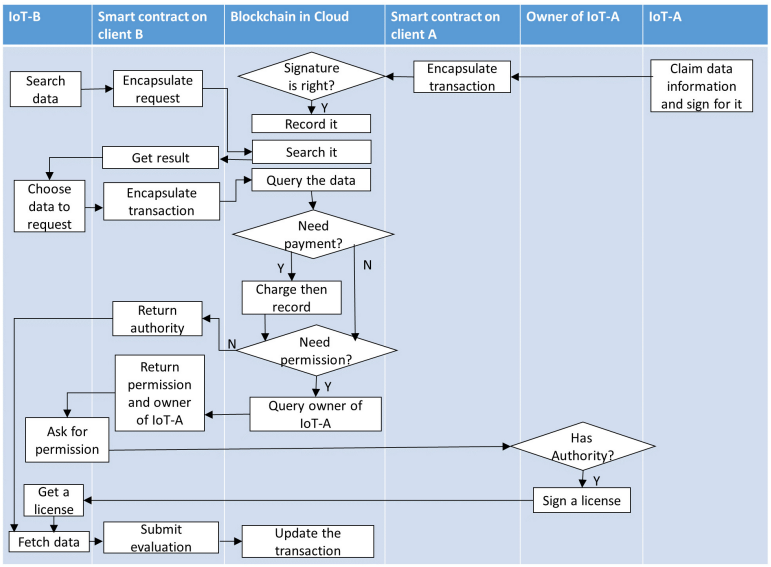


Fig. 3 Data access process

a) IoT-A claims critical message of its data to blockchain by contract.

b) IoT-B queries current data thus find IoT-A' s data. Then it may send an access request to the data. The contract would try to judge whether IoT-B could access the data, then generate a transaction. Both IoT-A and IoT-B would get this result.

c) If IoT-B has the permission, it would fetch data and verify it, then evaluate the transaction.

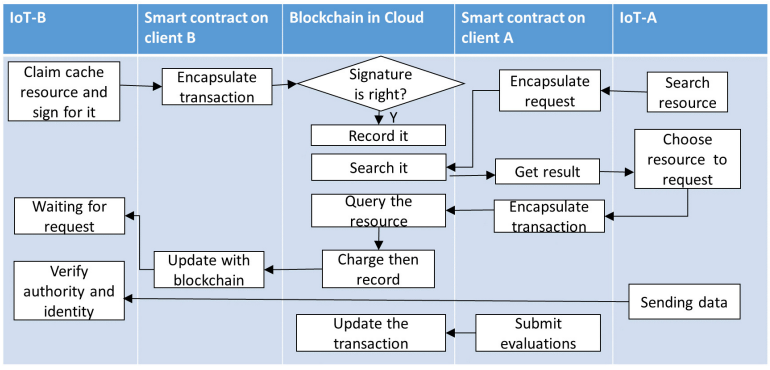


Fig. 4 Data offloading process

4.2.2 data offloading

In this scenario, IoT-B has storage resource while IoT-A lacks. This transaction need 3 steps as Fig.4.

a) IoT-B claims its cache resource by contract.

b) IoT-A sends a request to the resource by a rent smart contract. The contract would charge IoT-A for IoT-B, then generate a transaction. After this, accounts of IoT-A and IoT-B are updated.

c) IoT-A sends data to IoT-B and verify that whether it caches the correct data. Then evaluate the transaction.

5 Methods/Experimental

Every user hope its request can be executed truthfully. To choose credible service provider, we propose a machine learning based trust assess algorithm. From transactions in Section 4.2, nodes in the model can get information as TABLE 2. As all these information has been endorsed by blockchain, we take them to construct trust model. To choose suitable features, we have considerations as follows:

Table 2 IDENTITY MESSAGE

Symbol	Parameter	Value
CT	Counting Trust	how many trustworthy transactions occur after the last untrustworthy transaction(belonging to specific context)
CU	Counting Un-trust	how many untrustworthy transactions after the last trustworthy transaction (belonging to specific context)
LT	Last Time	the last experience of a specific context
TC	Transactions Context	type of transaction
TS	Trust Score	Score for this interaction

1. Since there are too many IoT nodes in network, maintain their social relationship would cause heavy overhead. Therefore, we don’ t take social factor into consideration.

2. Since nodes has different ability in different context, we take experience in specific context into consideration.

3. To calculate trust value, historical reputation should be considered. What’ s more, trust behavior would get rewards while un-trust would be punished.

4. All these trust basis should be easily recorded into blockchain while not cause extra data storage. Because blocks always grow, too many data stored in blockchain would cause difficulty in querying data.

5. Since behavior of nodes would change, time should be taken into considered.

The reason why choose these index can be concluded as follows:

1. CT and CU can be easily get. When a transaction ends, it can be easily updated. If the node who supply service get a positive feedback, CT would plus one while CU would be zero. Similarly, after a un-trust service, CU would plus one while CT would be zero. In this way, we could reward and punish behaviors immediately.

2. LT also could be updated easily. The feature represents that the nodes has last experience in the specific.

3. TS is trust decision about the node, it can be divided into trustworthy and untrustworthy.

In this paper, we design machine learning based methods to assess TS according to CT,CU,LT and TC. Since a transaction decision only care logs in the same context, we discuss CT,CU and LT.

Since CT and CU has strong correlation, we combine them together to compute transaction reputation. According to our settings, one of them most be zero, so we get a new parameter to represent the transaction reputation of node.

$$R = CT - CU \tag{1}$$

In the following part, we would try to predict TS according to R and LT with ML based methods. As II.B says, these methods can be divided into KNN based method, Random Forest, SVM based, NN based, and Bayes. As NN based algorithm not suit for low dimension computing, we only try the others.

5.1 KNN based method

KNN is a typical distance based classification algorithm. In this paper ,we define distance as (2) to measure difference of two samples.

$$dist(x_i, \mu_k) = \| x_i, \mu_k \|^2 \tag{2}$$

Since there are only two parameters for us to predict, dimension disaster is impossible. So we could take it directly as Algorithm 1. Generally, size of cluster and central point of each cluster should be defined at beginning. To improve its generalizability, we choose them randomly in the beginning.

Algorithm 1 KNN based trust prediction

Input: $datasetD$
1: $random\ choose\ x_1, x_2 \in D$
2: **for** $k = 1$ to 3 **do**
3: Repeat until convergence
4: **for** $i = 1$ to $D.size()$ **do**
5: $type(x_i) = \arg\min_k dist(x_i, \mu_k)$
6: $\mu_k = average(x \in D_k)$
7: **end for**
8: $J = \arg\min_k \sum_{x \in D_k} dist(x_i, \mu_{type(x_i)})$
9: **end for**
Output: $D_1, ..., D_k$

5.2 Random Forest based method

Random forest is a typical several decision tree based ensemble learning algorithm. Which pick N samples randomly from training dataset to construct several decision tree. Test data would be calculated by each tree, and classification is decided by voting results of trees.

$$H(D) = \sum_i p(TS = i) \log p(TS = i) \tag{3}$$

$$H(D|LT) = -\sum_i \sum_j p(i,j) \log p(TS = i|LT = j) \tag{4}$$

$$H(D|R) = -\sum_i \sum_j p(i,j) \log p(TS - i|R = j) \tag{5}$$

A means attributes in dataset D, which could be LT or R.

$$g(D,A) = H(D) - H(D|A) \tag{6}$$

$$g_r(D,A) = g(D,A)/H(A) \tag{7}$$

Algorithm 2 Random Forest based trust prediction

Input: *dataset* D, *number of trees* N, *sample limit* m
1: *Data discretization*
2: *Repeat* N *times*{
3: *Choose* m *samples randomly from* D
4: *Calculate Information gain ratio* $gr(D,A)$
5: *Variable* $A_1 = \arg\max gr(D,A)$
6: *Splitting into two sub − nodes according* A_1
7: *Splitting into two types according* A_2 *from sub − node*
8: }
Output: N *Tree*

5.3 Bayes based method

Bayes is a probability based algorithm. By computing probability and condition probability, predict whether the node can be trust.

Algorithm 3 Random Forest based trust prediction

Input: *dataset* D
1: *Data discretization*
2: *Calculate* $P(TS = trustworthy)$ *as* P_1, $P(TS = untrustworthy)$ *as* P_2
3: *Calculate* $P(LT|TS)$ *and* $P(R|TS)$

According to features of sample x, the algorithm would choose the most likely TS result as prediction h(x) as (8).

$$h(x) = \arg\max_i P(TS = i)P(x.LT|TS = i)P(x.R|TS = i) \tag{8}$$

5.4 SVM based method

In SVM based method, it try to classify samples by find w with . Since number of attributes is a bit, we take Radial Basis Function Kernel(RBFK) as kernel function $\varphi(x)$.

$$\begin{cases} w^T\varphi(x)+b & > 1-c, x.TS = trustworthy \\ w^T\varphi(x)+b & < -1+c, x.TS = un-trustworthy \end{cases} \tag{9}$$

Algorithm 4 SVM based trust prediction

Input: *dataset* D
1: **for** c, $step = 0.01$ **do**
2: $Model = svm(y, X, RBFK, c, step)$
3: $m, step = \min(diff(Model.fit(X.LT, X.R) - X.TS))$
4: **end for**
Output: c, $step$

In algorithm 4, we try to adjust c with step to find , thus get a most suitable model for training dataset.

6 Results and Discussion

To verify our approach with other methods, we used a synthetic data set obtained by the Java simulator implemented in [30],which include 322 labeled samples [31]. The dataset aims to evaluate the trustworthiness of each user by monitoring the behavior of each other during their interaction in pervasive computing network. In this paper, we take interaction in pervasive computing as transactions in IoT network.

Since some user may give wrong evaluation to transactions, we take some attacks into consideration including Ballot Stuffing (BS), Bad Mouthing(BM), and Random opinion (RO). In BS attack, some user take untrustworthy behavior as trustworthy. In BM attack, some user take trustworthy behavior as untrustworthy. While in RO attack, both BM and BS may happened. In our experiment, attack ratios are set from 10% to 50%. To get results more credible, we execute each test 200 times to get their average value.

To compare our methods with others traditional algorithms including K-Nearest Neighbor(KNN), Support Vector Machine(SVM), Naïve Bayes, and Random forest. To compare these algorithms, we set confusion matrix as TABLE 3.

Table 3 CONFUSION MATRIX

Real\classification result	Trustworthy	Un-Trustworthy
Trustworthy	TP	FN
Un-Trustworthy	FP	TN

$$\text{Accuracy} = (\text{TP} + \text{TN})/\text{size of test Data} \tag{10}$$

$$\text{Precision} = \text{TP}/(\text{TP} + \text{FP}) \tag{11}$$

$$\text{Recall} = \text{TP}/(\text{TP} + \text{FN}) \tag{12}$$

$$\text{F1} - \text{score} = 2 * \text{Precision} * \text{Recall}/(\text{Precision} + \text{Recall}) \tag{13}$$

Accuracy is the portion of correctly classified instances. Precision is the portion of trustworthy assessments correctly. Recall is the portion of trustworthy nodes

which are correctly identified. F1-score measures performance of classification by combining precision and recall. To recommend trustworthy edge nodes for users, we mainly care Accuracy and Precision.

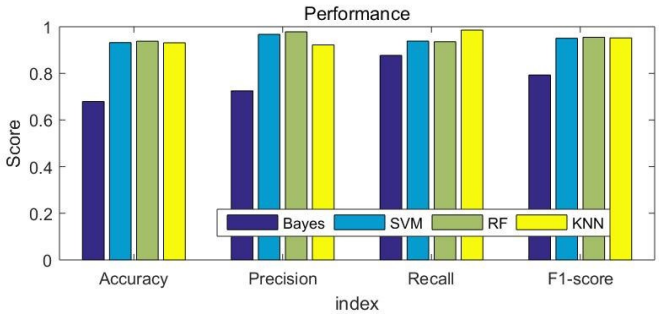
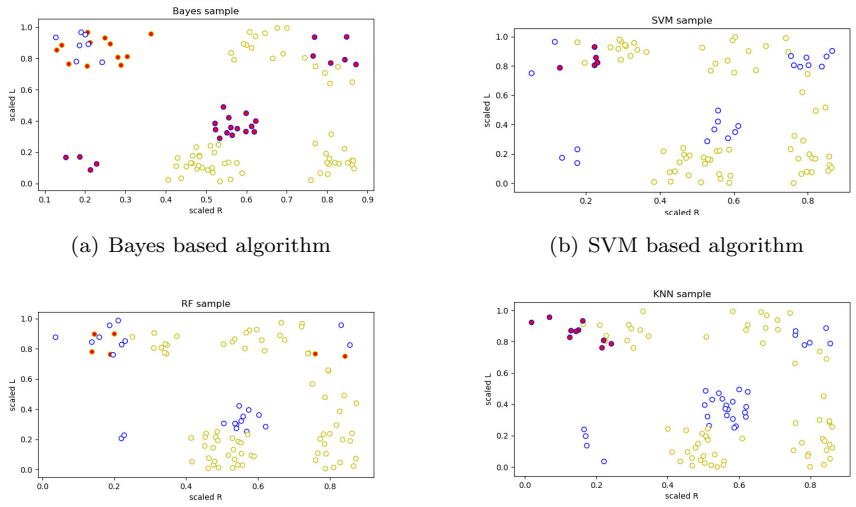


Fig. 5 Performance of different algorithms

Before test performance of ML algorithms, we first test them without attacks as Fig.5 and Fig.6. Fig.5 shows that Naive Bayes based algorithm may not suitable for the dataset. RF based algorithm performs best while SVM could approach it. To identity what happened, we demonstrate classified result as Fig.6. In Fig.6, we use red to identity classified results wrongly. Blue nodes represents untrustworthy nodes and yellow represents trustworthy nodes.



(a) Bayes based algorithm

(b) SVM based algorithm

(c) Random Forest based algorithm

(d) KNN based algorithm

Fig. 6 Performance of different algorithms

From Fig.6 we can get conclusions as follows:

a) Untrustworthy nodes can be divided into four types: A presents nodes whose reputation bad and attend transaction recently, B represents nodes whose reputation bad and no transaction recently, C presents nodes whose no reputation and transaction not long ago, D presents nodes whose reputation well and no transactions recently. The phenomenon coincides with our common sense. Nodes which

don’ t have transactions may have obvious difference with its behavior before, and new nodes may be good or bad.

b) Bayes based algorithm could identity untrustworthy nodes belong to type A. Since it make decision by probability, all nodes behave untrustworthy recently are classified into bad nodes.

c) KNN, SVM, and RF based algorithm could identity almost all nodes correctly. Most of there problem is nodes whose reputation is bad and no transaction recently. SVM and KNN tend to believe them while RF tends to doubt them. In fact, RF performs best, while SVM could get a similar performance.

d) RF is more strictly with nodes who have good reputation and have no transaction recently.

Then we compare the time consumption of each algorithm. From Fig.7 we can see that RF based algorithm would cause larger consumption. Considering results in Fig.6, we can think that SVM is the best solution for our scenario. Next we would compare their performance under different attacks.

6.1 Accuracy

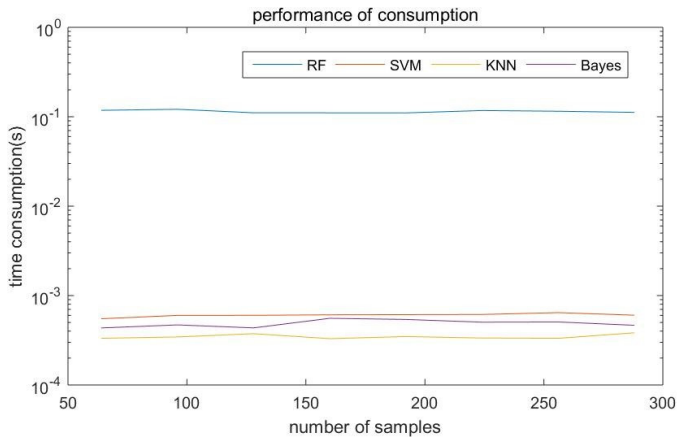


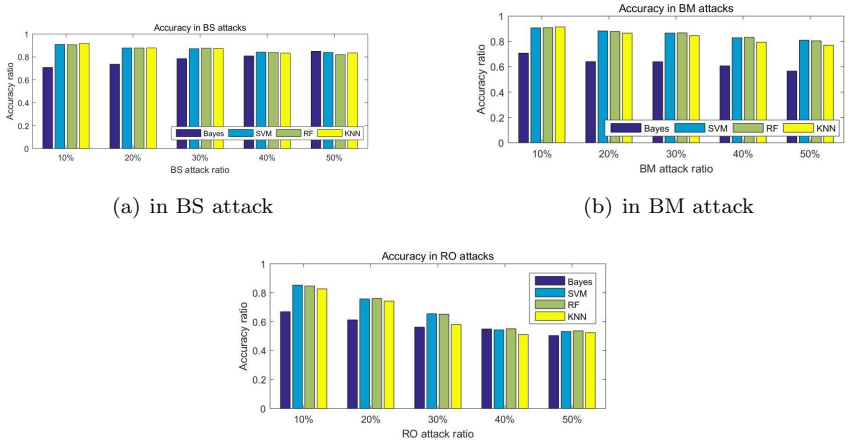
Fig. 7 Accuracy of Algorithms in Different attacks (a)in BS attack (b) in BM attack (c) in RO attack Since

According to Fig.7, BS and BM attacks has similar influence to SVM,KNN,RF algorithm. With the increment of attack ratio, they all show a linear decline. RO attacks is more harmful to trust assessment. If more than 30% of transaction results are evaluated randomly, trust assessment will make no sense.

And, SVM and RF has similar performance in accuracy. KNN is inferior to them obviously while Bayes performs worse.

6.2 Precision

According to Fig.8, attacks has similar influence trend to algorithms despite Bayes. RO attacks is the most serious, BM is the next. Similar to accuracy, if more than 30% of transaction results are evaluated randomly, trust assessment will make no



(a) in BS attack

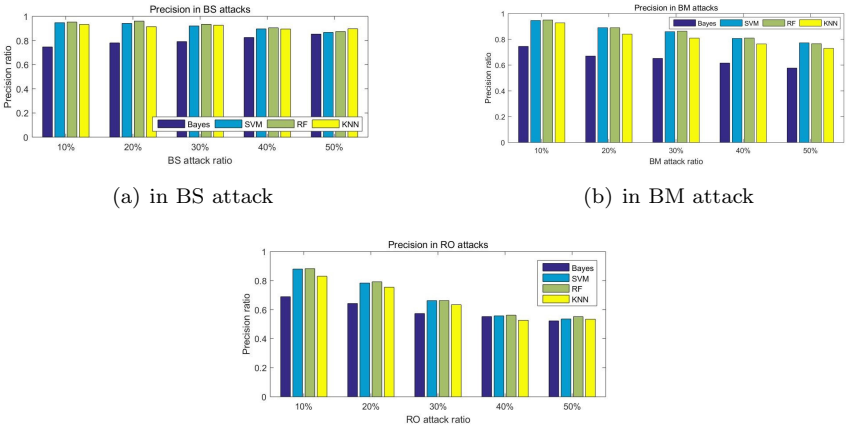
(b) in BM attack

(c) in RO attack

Fig. 8 Accuracy of Algorithms in Different attacks

sense. Compare BS with BM attacks, treat transactions tolerantly would not hurt precision too much.

Under BS attack, KNN is more stable than others. Bayes performs opposite trend under BS and BM attacks, because probability distributions changes. And, SVM and RF has similar performance in precision. KNN is inferior to them obviously while Bayes performs worse.



(a) in BS attack

(b) in BM attack

(c) in RO attack

Fig. 9 Precision of Algorithms in Different attacks

7 Conclusion

In our paper, a blockchain based architecture is proposed for IoT to promote cooperation among different centers. By authenticating identity and executing transactions on blockchain, a credible environment is constructed for IoT service. Then, to help IoT nodes choose trustworthy nodes to supply service, we design ML based trust assessment algorithms to analyze transaction log. To verify our design, we

compare performance of them. Experiment results proves that our mechanism could effectively identify trustworthy nodes in IoT.

Acknowledgements
Not applicable

Funding
This work is supported by Science and Technology Project from Headquarters of State Grid Corporation of China: "基于区块链的电力业务可信服务支撑体系研究及典型场景应用" (5700-201918243A-0-0-00)

Abbreviations
IoT: Internet of Things; ML: Machine Learning; OSNs: Olfactory Sensoryneurons; ID: Identity document; CT: Counting Trust; CU: Counting Un-trust; LT: Last Time; TC: Transactions Context; TS: Trust Score; KNN: K-Nearest Neighbor; SVM: Support Vector Machine; RBFK: Radial Basis F unction Kernel; BS: Ballot Stuffing; BM: Bad Mouthing; RO: Random opinion

Availability of data and materials
Data sharing not applicable to this article as no data sets were generated or analyzed during the current study.

Competing interests
The authors declare that they have no competing interests.

Authors' contributions
The work presented here was carried out in collaboration between all authors. LW, XW and QM designed methods and experiments, carried out the experiments, interpreted the results. HZ co-designed methods and made important revisions. RD and JS co-designed experiments and co-worked on analysis. All authors have read and approved the final manuscript.

Author details
[1]Power dispatching control center, State Grid Jiangsu Electric Power Co., Ltd, 215 Shanghai Road, 210000, Nanjing, China. [2]Power dispatching control center, Nanjing power supply branch of State Grid Jiangsu Electric Power Co., Ltd, No.1 Aoti street, Jianye District, 210019, Nanjing, China. [3]School of Computer Science, Beijing University of Posts and Telecommunications, No. 10 Xitucheng Road, Haidian District, 100876, Beijing, China.

References
1. K. Christidis, M.D.: Blockchains and smart contracts for the internet of things. IEEE Access **4**, 2292–2303 (2016)
2. A. Dorri, R.J.P.G. S. S. Kanhere: Blockchain for iot security and privacy: The case study of a smart home. Proc. IEEE Int. Conf. Pervasive Comput. Commun. (PerCom) Workshops, 618–623 (2017)
3. A. Bahga, V.K.M.: Blockchain platform for industrial internet of things. J. Softw. Eng. Appl. **9**(10), 533 (2016)
4. F. Bonomi, J.Z.S.A. R. Milito: Fog computing and its role in the internet of things. Proc. 1st Ed. MCC Workshop Mobile Cloud Comput. (MCC), 13–16 (2012)
5. M. Chiang, T.Z.: Fog and iot: An overview of research opportunities. IEEE Internet Things **3**(6), 854–864 (2016)
6. T.X.Tran, P.P.D.P. A.Hajisami: Collaborative mobile edge computing in 5g networks: New paradigms, scenarios, and challenges. IEEE Communications Magazine **55**(4), 54–61 (2017)
7. Laizhong Cui, Z.C.Y.P.Z.M.M.X. Shu Yang: A decentralized and trusted edge computing platform for internet of things. IEEE Internet of Things Journal **7**, 3910–3922 (2020)
8. Li, J.Y..X.: A reliable and lightweight trust computing mechanism for iot edge devices based on multi-source feedback information fusion. IEEE Access **6**, 23626–23638 (2018)
9. S. Pinto, J.P.J.C.A.T. T. Gomes: Iioteed: An enhanced trusted execution environment for industrial iot edge devices. IEEE Internet Comput. **21**(1), 40–47 (2017)
10. A. Boukerche, K.E.-K. X. Li: Trust-based security for wireless ad hoc and sensor networks. Comput. Commun. **30**, 2413–2427 (2007)
11. G. Xu, Z.Y.: A survey on trust evaluation in mobile ad hoc networks. Proc. 9th EAI Int. Conf. Mobile Multimedia Commun., 140–148 (2016)
12. X. Li, X.Y. F. Zhou: Scalable feedback aggregating (sfa) overlay for large-scale p2p trust management. IEEE Trans. Parallel Distrib. Syst. **23**(10), 1944–1957 (2012)
13. X. Li, J.D. F. Zhou: Ldts: A lightweight and dependable trust system for clustered wireless sensor networks. IEEE Trans. Inf. Forensics Security **8**(6), 924–935 (2013)
14. F. Azzedin, A.R.: Feedback behavior and its role in trust assessment for peer-to-peer systems. Telecommun. Syst. **44**(3), 253–266 (2010)
15. X. Li, F.Z.X.G. H. Ma: Service operator-aware trust scheme for resource matchmaking across multiple clouds. IEEE Trans. Parallel Distrib. Syst. **26**(5), 429–1419 (2015)
16. G. Theodorakopoulos, J.S.B.: On trust models and trust evaluation metrics for ad hoc networks. IEEE J. Sel. Areas Commun. **24**(2), 318–328 (2006)
17. Y. Sun, K.J.R.L. Z. Han: Defense of trust management vulnerabilities in distributed networks. IEEE Comm. Mag. **46**(2), 112–119 (2009)
18. Z. Yan, A.V.V. P. Zhang: A survey on trust management for internet of things. J. Netw. Comput. Appl. **42**, 120–134 (2014)

19. W. Abdelghani, I.A.F.S. C. A. Zayani: Trust management in social internet of things: A survey. Proc. Conf. e-Bus. e-Services e-Soc, 430–441 (2016)
20. M. Ma, F.L. G. Shi: Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the iot scenario. in IEEE Access (7), 34045–34059 (2019)
21. S. Guo, S.G.X.Q.F.Q. X. Hu: Blockchain meets edge computing: A distributed and trusted authentication system. in IEEE Transactions on Industrial Informatics **16**(3), 1972–1983 (2020)
22. Q. Xu, Q.Y. Z. Su: Blockchain-based trustworthy edge caching scheme for mobile cyber-physical system. in IEEE Internet of Things Journal **7**(2), 1098–1110 (2020)
23. J. Kang, e.a.: Blockchain for secure and efficient data sharing in vehicular edge computing and networks. IEEE Internet of Things Journal **6**(3), 4660–4670 (2019)
24. B. Lee, J.-H.L.: Blockchain-based secure firmware update for embedded devices in an internet of things environment. J. Supercomput. **73**(3), 1152–1167 (2017)
25. X. Liu, A.D. G. Tredan: A generic trust framework for large scale open systems using machine learning,. Comput.Intell. **30**(4), 700–721 (2014)
26. K. Zhao, L.P.: A machine learning based trust evaluation framework for online social networks. Proc. IEEE 13th Int. Conf. Trust, Secur. Privacy Comput. Commun., 69–74 (2014)
27. Francesco Restuccia, T.M. Salvatore D' Oro: Securing the internet of things in the age of machine learning and software-defined networking. IEEE Internet of Things Journal **5**(6), 4829–4842 (2018)
28. J. Cañedo, A.S.: Using machine learning to secure iot systems. Proc. 14th IEEE Annu. Conf. Privacy Security Trust (PST), 219–222 (2016)
29. M. Miettinen, e.a.: Iot sentinel: Automated device-type identification for security enforcement in iot. Proc. IEEE 37th Int. Conf. Distrib. Comput. Syst. (ICDCS), 2177–2184 (2017)
30. G. D'Angelo, S.R. F. Palmieri: Detecting unfair recommendations in trust-based pervasive environments. Information Sciences **486**, 31–51 (2019)
31. D'Angelo, G.: Dishonest Internet users dataset (2018). https://data.world/giannidangelo/dishonest-internet-users-dataset

Figures

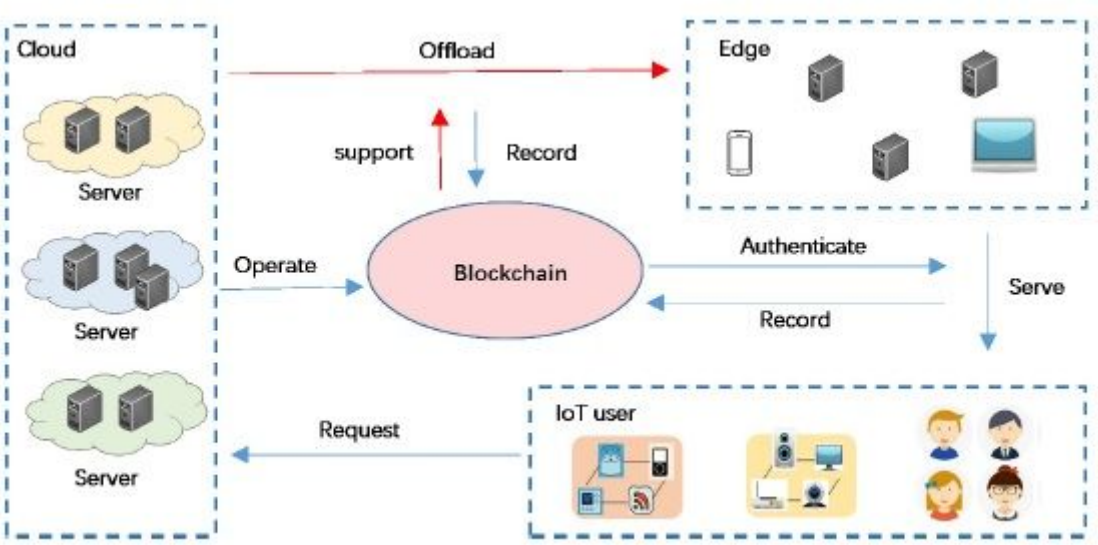


Figure 1

Architecture

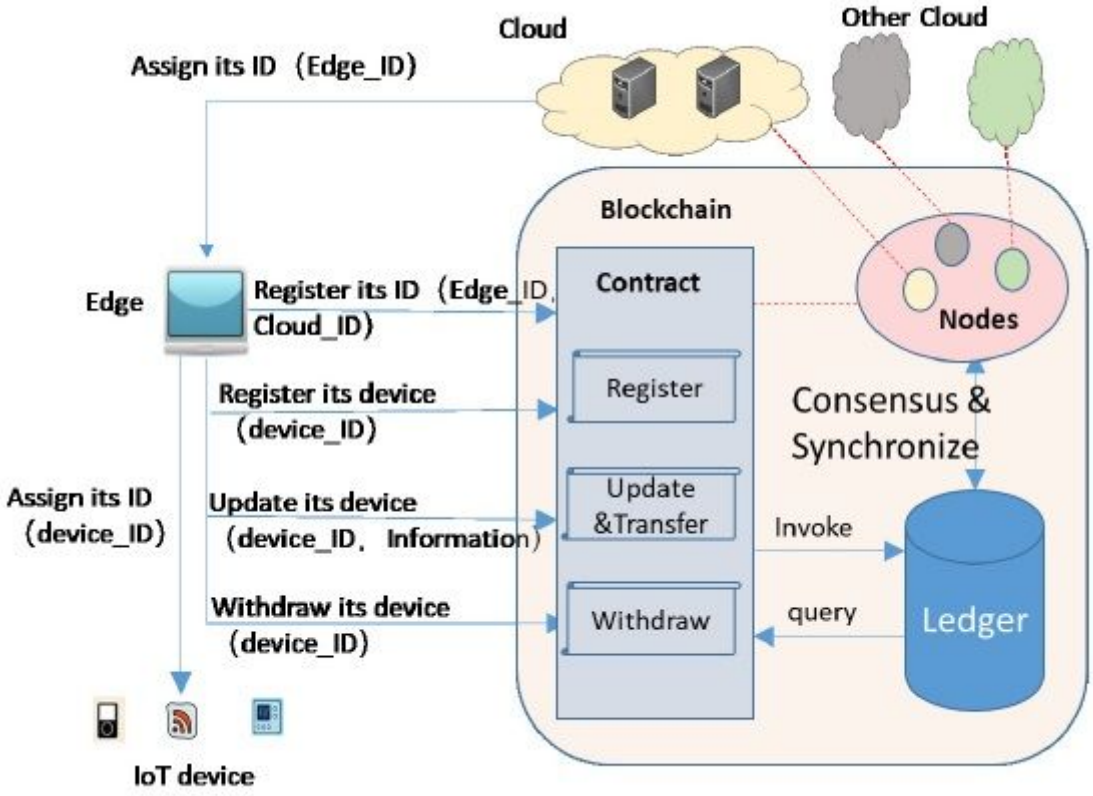


Figure 2

Identity register process

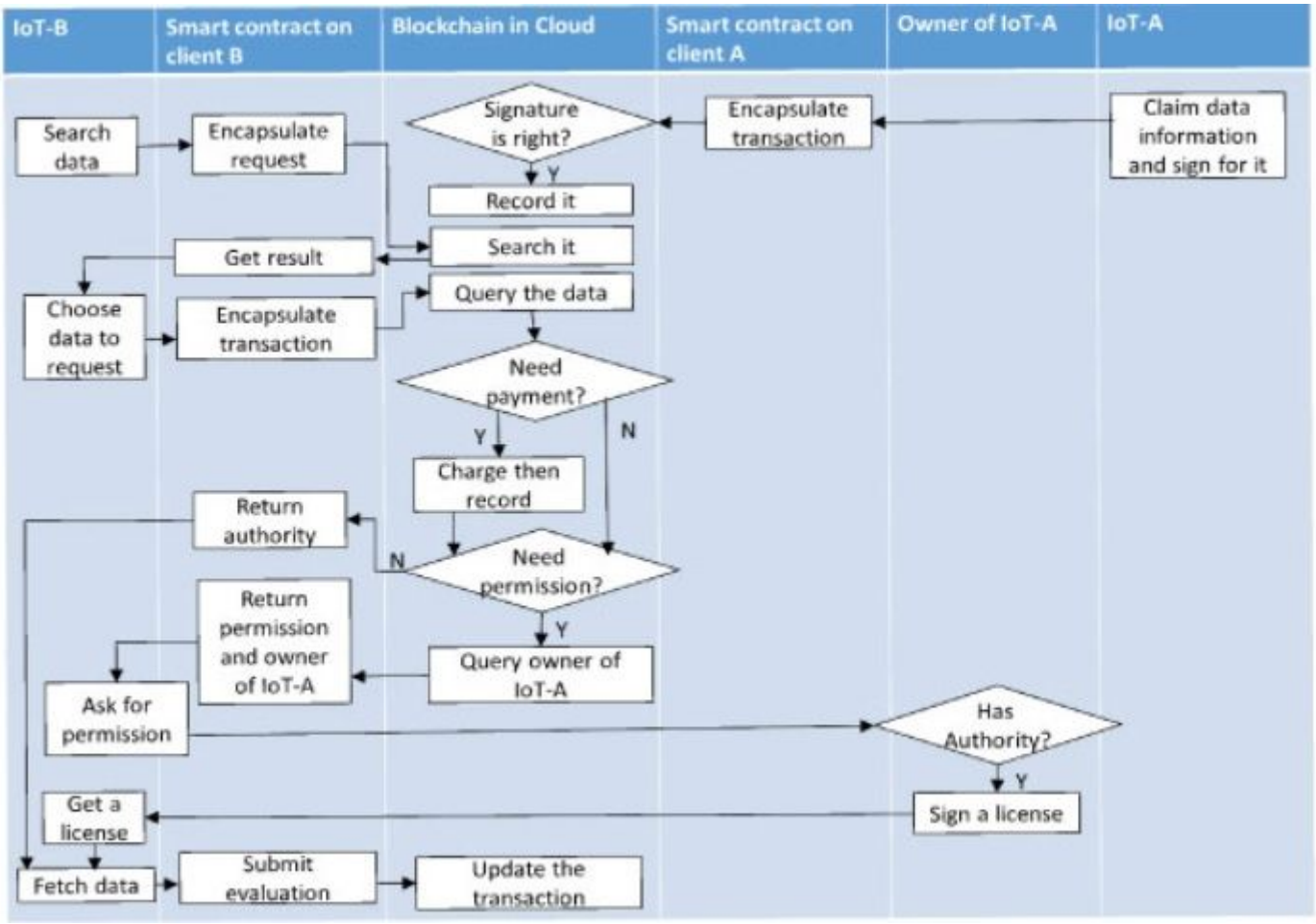


Figure 3

Data access process

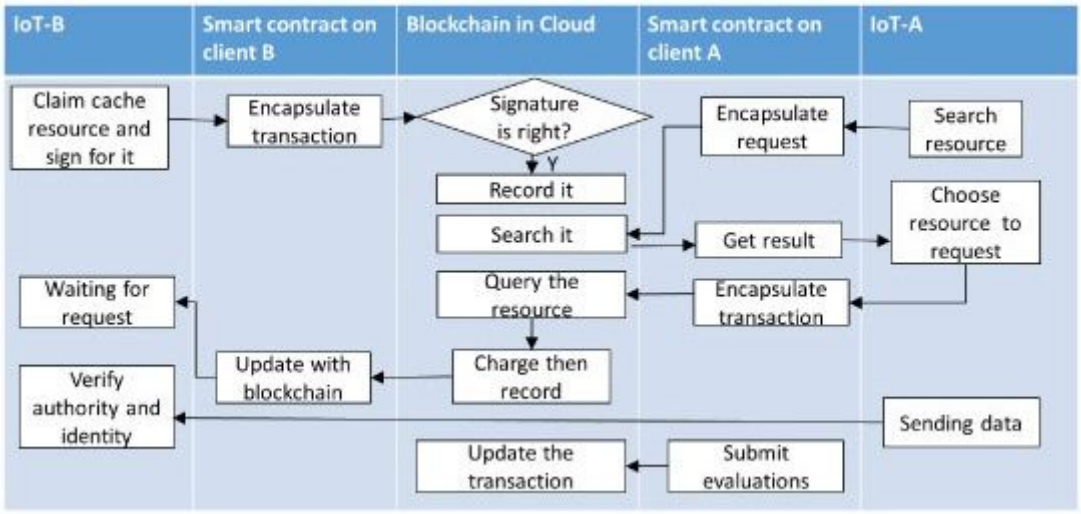


Figure 4

Data offloading process

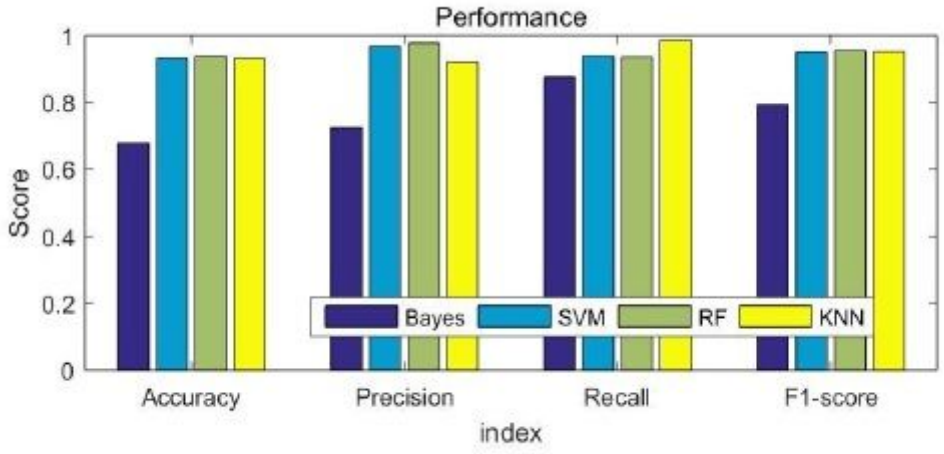
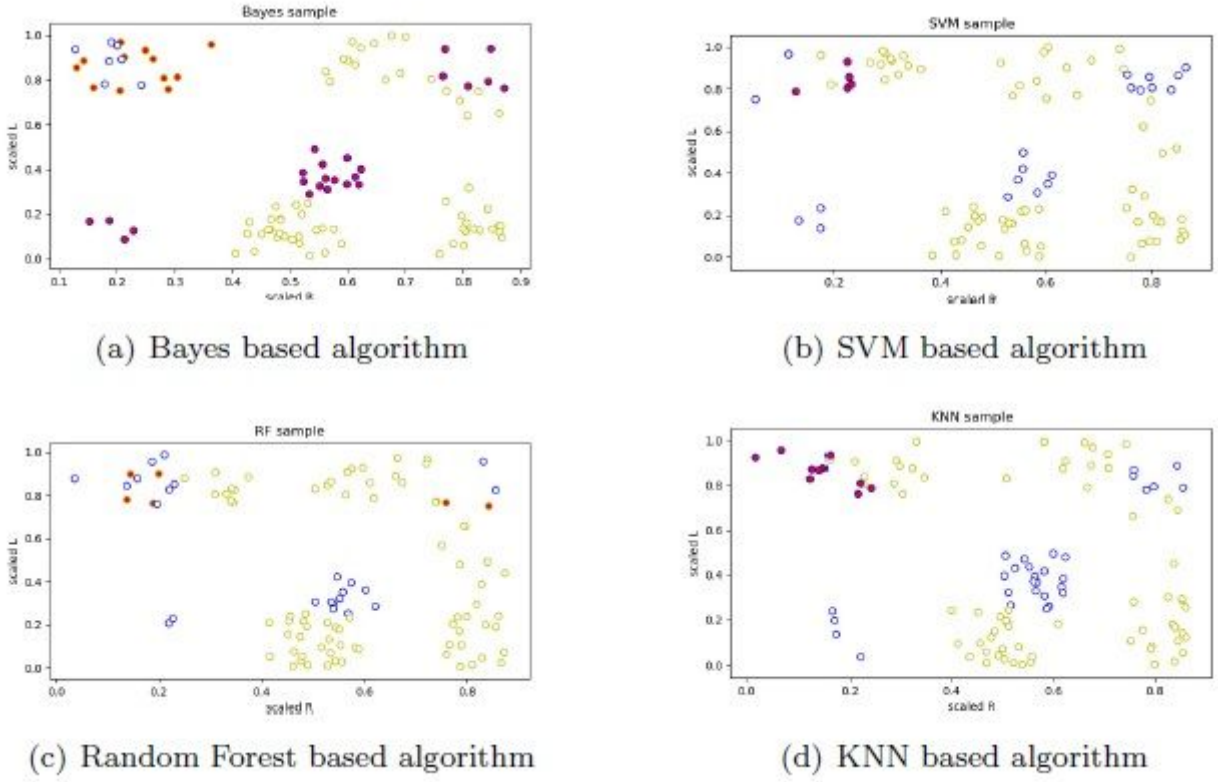


Figure 5

Performance of different algorithms



(a) Bayes based algorithm

(b) SVM based algorithm

(c) Random Forest based algorithm

(d) KNN based algorithm

Figure 6

Performance of different algorithms

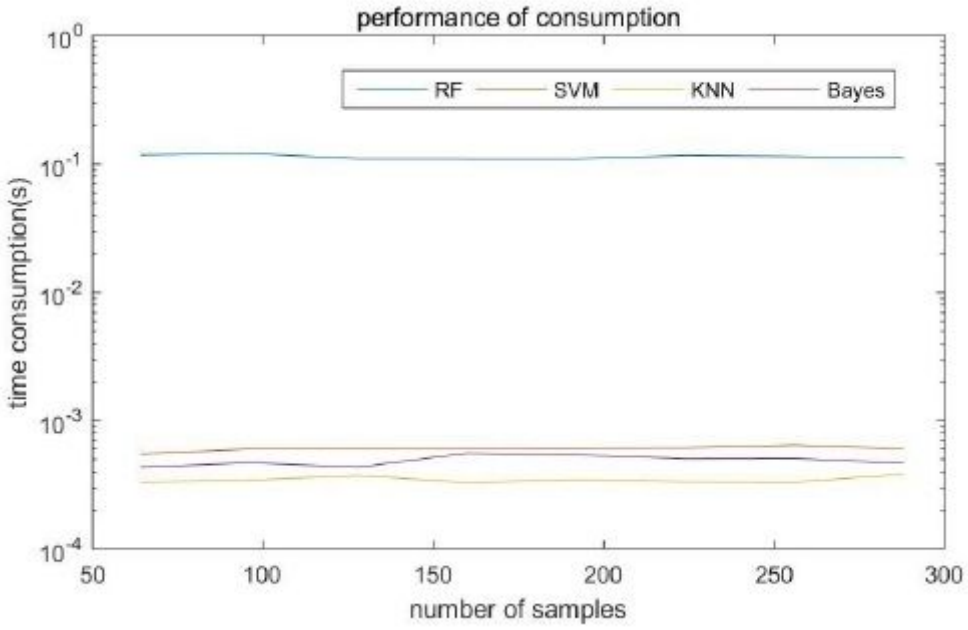
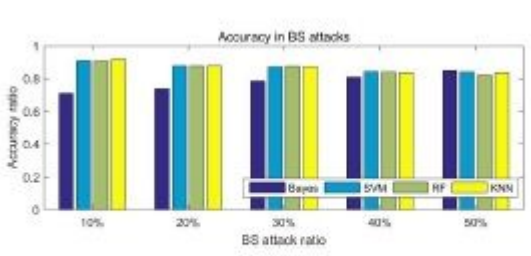
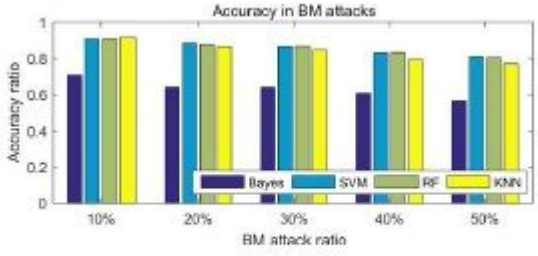


Figure 7

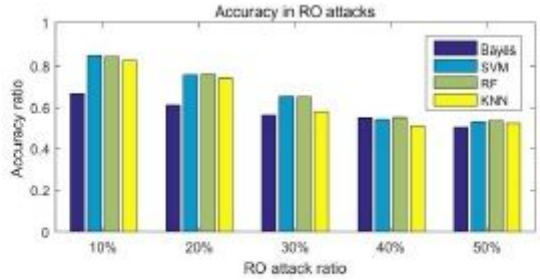
Accuracy of Algorithms in Different attacks (a)in BS attack (b) in BM attack (c) in RO attack Since



(a) in BS attack



(b) in BM attack



(c) in RO attack

Figure 8

Accuracy of Algorithms in Different attacks

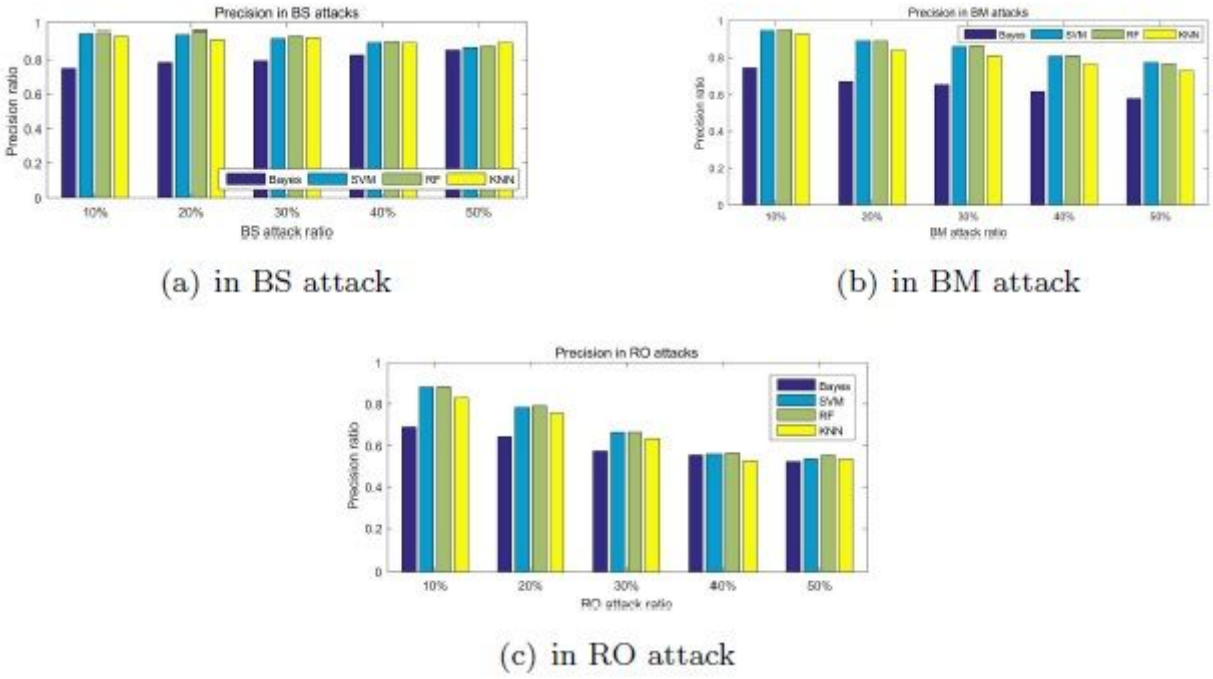


Figure 9

Precision of Algorithms in Different attacks