International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

# TRUST MANAGEMENT PROTOCOL BASED ON BLOCKCHAIN FOR THE INTERNET OF THINGS

**G. SANTHI KUMARI**

Master of Computer Applications (MCA),

SVKP & Dr.K.S Raju Arts & Science College(A),

Penugonda, W.G.Dt., A. P, India

santhigonnabattula731@gmail.com

**CH. SRINIVAS RAO**

Head of the department in Computer Science,

SVKP & Dr.K.S Raju Arts & Science College(A),

Penugonda, W.G.Dt, A.P, India

chiraparapu@gmail.com

## ABSTRACT:

The Internet of Things (IoT) is a network that connects different nodes such as connected devices (sensors, robots, smart phones, etc.), connected cars, smart homes, and so on. These intelligent objects communicate and collaborate in distributed and dynamic environments that face a number of security challenges. One of the most significant challenges in IoT is trust management. Existing trust management solutions are incapable of meeting the new IoT requirements of heterogeneity, mobility, and scalability. In this paper, we propose a hierarchical and scalable blockchain-based trust management protocol for massively distributed IoT systems with mobility support. Mobile smart objects in our protocol send trust information about service providers to the blockchain. Thus, all the objects will have a global view on each service provider in the architecture, which speeds up the trust evaluation process. In addition, our protocol is resilient against the most known malicious attacks such as bad-mouthing, ballot-stuffing and cooperative attacks. We confirm the efficiency of our proposal through theoretical analysis and extensive simulations. Finally, we show that it outperforms existing solutions especially in terms of scalability, mobility support, communication and computation costs.

**KEYWORDS:** Internet of things (IoT

## I.INTRODUCTION

In recent years, we have witnessed a true revolution of the Internet, which has given rise to the IOT, in which a large number of physical objects have been linked to the Internet. The Gartner Institute predicts that by 2020, there will be more than 50 billion linked objects, which will

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

alter our way of life through a variety of applications [1].

IOT can be viewed as a service centric architecture where each device, can request services from other devices and it may also provide services to other devices (service provider). The service centric based IOT applications are facing several security challenges such as trust management. Indeed, IOT service providers can behave maliciously for the purpose of promoting it-self and defame the honest service providers. Hence, they can trick IOT devices to request services from them instead of the honest ones and monopolize many provided services by performing discriminatory, bad-mouthing and ballot-stuffing attacks. Therefore, it is clear that a trust management protocol which evaluates the trustworthiness of IOT service providers, in a scalable and efficient way, is required.

To date, many trust management protocols have been developed for Wireless Sensor Networks (WSN), Social networks and P2P systems in general (e.g. [3], [6], [8], [9], [14], [20], [27]). In these protocols, trust computation is often based on: 1) the direct observations of each node regarding the others (which is gathered whenever the node encounters the IOT service providers) and 2) the indirect recommendations received from other nodes about the service providers. However, these solutions are still not scalable and not suitable for applications with high mobility as IOT. trust parameters with a large number of IOT devices in order to accurately compute trustworthiness of IOT service providers. Moreover, other questions still arise. For example, how trust information (direct information and indirect recommendations) is shared in a scalable way in order to speed up the process of trust computation and make it more accurate. In addition, each node has to store trust information about every encountered service provider.

Besides, in some cases, an IOT device needs to assess the trust level of a new encountered service provider in a fast way, without necessarily performing a lot of exchanges. Existing trust management solutions do not efficiently deal with these cases. In fact, without any previous exchange, a new encountered service provider is assumed to have a predefined initial trust value, whereas it could be malicious.

Other clustering and centralized based trust management approaches have been investigated in several works (e.g. [12], [26]) in order to enhance the process of trust computation and optimization of IOT resources. Although these approaches allow constrained IOT devices to efficiently assess trustworthiness of each other, these devices only have access to trust data in their own cluster (no global view of Trust worthiness). Furthermore, these protocols usually

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

assume that the cluster heads are pre-trusted nodes. However, such assumption is not practical in most IOT applications.

Hence, this brings us back to an important question: how can we ensure a fully distributed and scalable trust management protocol with mobility support, in which IOT devices can evaluate trustworthiness of any service provider
in the Internet, without the presence of any pre-trusted entity?

IOT can be viewed as a service centric architecture where each device, can request services from other devices and it may also provide services to other devices (service provider). The service centric based IOT applications are facing several security challenges such as trust management. Indeed, IOT service providers can behave maliciously for the purpose of promoting it-self and defame the honest service providers. Hence, they can trick IOT devices to request services from them instead of the honest ones and monopolize many provided services by performing discriminatory, bad-mouthing and ballot-stuffing attacks. Therefore, it is clear that a trust management protocol which evaluates the trustworthiness of IOT service providers, in a scalable and efficient way, is required.

To date, many trust management protocols have been developed for Wireless Sensor Networks (WSN), Social networks and P2P systems in general (e.g. [3], [6], [8], [9], [14], [20], [27]). In these protocols, trust computation is often based on: 1) the direct observations of each node regarding the others (which is gathered whenever the node encounters the IOT service providers) and 2) the indirect recommendations received from other nodes about the service providers. However, these solutions are still not scalable and not suitable for applications with high mobility as IOT. trust parameters with a large number of IOT devices in order to accurately compute trustworthiness of IOT service providers. Moreover, other questions still arise. For example, how trust information (direct information and indirect recommendations) is shared in a scalable way in order to speed up the process of trust computation and make it more accurate. In addition, each node has to store trust information about every encountered service provider.

Besides, in some cases, an IOT device needs to assess the trust level of a new encountered service provider in a fast way, without necessarily performing a lot of exchanges. Existing trust management solutions do not efficiently deal with these cases. In fact, without any previous exchange, a new encountered service provider is assumed to have

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

a predefined initial trust value, whereas it could be malicious.

Other clustering and centralized based trust management approaches have been investigated in several works (e.g. [12], [26]) in order to enhance the process of trust computation and optimization of IOT resources. Although these approaches allow constrained IOT devices to efficiently assess trustworthiness of each other, these devices only have access to trust data in their own cluster (no global view of Trust worthiness). Furthermore, these protocols usually assume that the cluster heads are pre-trusted nodes. However, such assumption is not practical in most IOT applications.

Hence, this brings us back to an important question: how can we ensure a fully distributed and scalable trust management protocol with mobility support, in which IOT devices can evaluate trustworthiness of any service providerin the Internet, without the presence of any pre-trusted entity?

## II. LITERATURE SURVEY

In this section, we review some trust management protocols for IoT which are closely related to our work. Recently, Guo et al. [13] provided a comprehensive survey about the most recent works in trust management and computational trust models in IoT. They basically focused on service management in IoT dealing with the choice of IoT devices as service providers according to their trustworthiness. They discussed the five fundamental components of each trust management system, namely: trust composition, trust propagation, trust aggregation, trust update and trust formation. Other recent work [23] has investigated and discussed the importance of the feedback in trustworthiness models to build trust management protocols for IoT. Chen et al. [5] proposed a trust management model based on fuzzy reputation concept for IoT. However, they considered only some specific WSN applications where nodes can establish limited trust relationships with other nodes. Compared to WSN nodes, IoT devices are internet enabled and can establish complex relationships with other IoT devices and owners. Saied et al. [25] proposed a multi-service and context aware trust management protocol for IoT systems. Al Hamadi et al. [2] addressed the problem of trust management for service communities in IoT. These protocols deal efficiently with different malicious attacks. However, they are based on centralized trusted cloud servers that collect trustworthiness from IoT devices which is not viable in IoT. Similarly, Guo et al. [12] proposed a 3-tier hierarchical architecture based on cloudlets to disseminate trust information to a central cloud. Their architecture allows IoT devices to report trust information and also query trustworthiness of other devices directly from the local cloudlets. However, the proposed architecture always refers

to the central cloud which is responsible for the dissemination of trustworthiness information gathered from one cloudlet to the other cloudlets which can involve latency issues. Moreover, their trust model is still limited, since the distributed cloudlets are assumed to be honest in the architecture and they maintain only trust data in their geographical area. The concept of social IoT has been developed recently in many works. Through this concept, IoT devices will be able to autonomously establish social relationships between other devices and users. Many works have investigated the trust management problem in the context of social IoT [7], [15], [16], [22]. Chen et al. [7] proposed an adaptive trust management protocol for social and dynamic IoT systems. The main idea consists on distributing the computation of trust information among IoT devices. In their computational model, each device maintains its own trust assessment toward other users and devices. The trust assessment is based on the recommendations of the other devices, the direct observations and also the history of the interactions. The authors considered different classes of trust properties such as QoS, honesty and cooperativeness depending on the social relationships between IoT devices. However, their protocol is not scalable enough since each device must save all the trust pieces of information (that include its history and the recommendations of the other devices, etc.) related to its social friends (IoT devices and owners) in a lookup table. In [22], the authors proposed two trustworthiness computational models. 1) A subjective model which consists on the combination of the local trust parameters (direct observations) and also the received indirect recommendations. And 2) An objective model, where they proposed to disseminate trust assessments in a distributed Hash table maintained by a subset of trusted IoT devices. However, this last assumption is not actually practical in IoT environments. Moreover, their solution is still limited and it is applicable only in social based IoT applications. Recently, blockchain technology has attracted a lot of attention in the IoT and security field. The authors in [17] proposed a data integrity service framework for IoT applications using blockchain and cloud computing. The main aim of this work is to eliminate third-parties (auditors) that are usually essential to ensure data integrity and auditability services. However, due to the high-cost Pow consensus method adopted in this work, it does not scale in constrained IoT applications. Taking into account the limitation of resources in IoT, a lightweight and scalable Blockchain is proposed by Dorri et al. [11] to ensure privacy and security in IoT applications. The main idea of their solution is to establish an overlay network composed of several IoT clusters, where cluster heads are responsible for the management of a public blockchain. Sidra et al. [19] proposed a decentralized and secure blockchain-based trust management framework for supply chains, named Trust Chain. This framework allows each

component in the supply chain to evaluate the trustworthiness of data generated by the participants in the supply chain. However, the proposed solution has not been evaluated under malicious attacks like bad mouthing and ballot stuffing attacks. Recently, Lu et al. [28] proposed a new blockchain based trust management solution for vehicular networks (VANETs). The idea of their solution is to use the blockchain as a platform to share the reputation scores reported by different vehicles. The blockchain is maintained by the road side units (RSU), which are also the miners. The authors proposed a new consensus algorithm that favors blocks containing a large variation of trust values. However, the proposed consensus method is vulnerable to some kind of collaborative attacks aiming to report high or low trust values to generate priority blocks and then disrupt blockchain trust values. Similarly, Yang et al. [18] proposed a privacy-preserving trust model for VANETs that combines blockchain and public key Infrastructure to deal with tracking attacks while broadcasting forged messages. However, the authors did not discuss the security of their trust management protocol against trust attacks like bad mouthing and ballot stuffing attacks.

**III.PROBLEM STATEMENT**

Recently, Guo et al. [13] provided a comprehensive survey about the most recent works in trust management and computational trust models in IoT. They basically focused on service management in IoT dealing with the choice of IoT devices as service providers according to their trustworthiness. They discussed the five fundamental components of each trust management system, namely: trust composition, trust propagation, trust aggregation, trust update and trust formation. Other recent work [23] has investigated and discussed the importance of the feedback in trustworthiness models to build trust management protocols for IoT.

Chen et al. [5] proposed a trust management model based on fuzzy reputation concept for IoT. However, they considered only some specific WSN applications where nodes can establish limited trust relationships with other nodes. Compared to WSN nodes, IoT devices are internet enabled and can establish complex relationships with other IoT devices and owners.

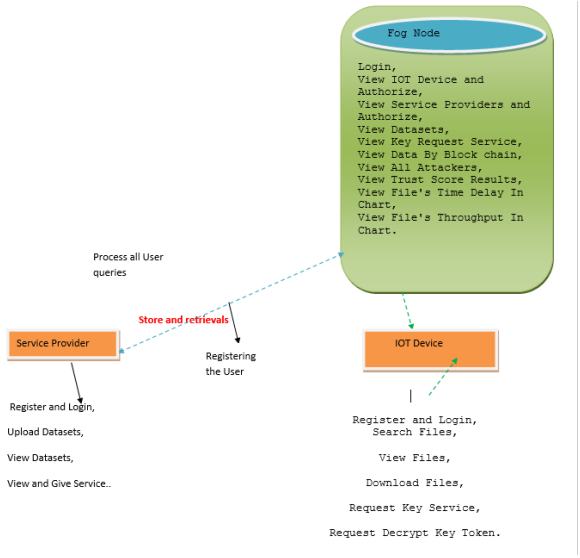
Saied et al. [25] proposed a multi-service and context aware trust management protocol for IoT systems. Al- Hamadi et al. [2] addressed the problem of trust management for service communities in IoT. These protocols deal efficiently with different malicious attacks. However, they are based on centralized trusted cloud servers that collect trustworthiness from IoT devices which is not viable in IoT.

Similarly, Guo et al. [12] proposed a 3-tier hierarchical architecture based on cloudlets to disseminate trust information to a central cloud. Their architecture allows IoT devices to report

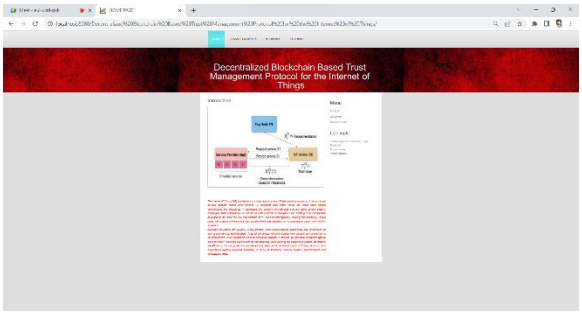
International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

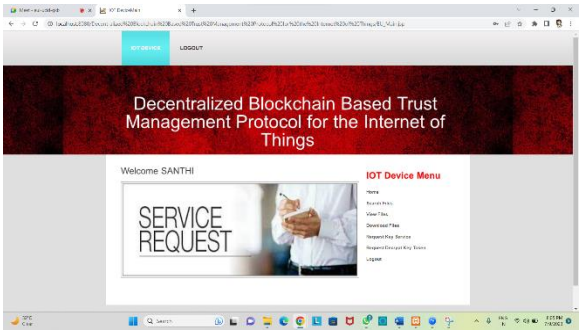
trust information and also query trustworthiness of other devices directly from the local cloudlets. However, the proposed architecture always refers to the central cloud which is responsible for the dissemination of trustworthiness information gathered from one cloudlet to the other cloudlets which can involve latency issues. Moreover, their trust model is still limited, since the distributed cloudlets are assumed to be honest in the architecture and they maintain only trust data in their geographical area.

**ARCHITECHTURE:**




## IV.RESULTS




## V.CONCLUSION

In this paper, we have proposed a private Ethereum blockchain-based solution that manages organ donation and transplantation in a decentralized, accountable, auditable, traceable, secure, and trustworthy manner. We developed smart contracts that ensure the data provenance by recording events automatically. We present six algorithms with their implementation, testing, and validation details. We analyze the security of the proposed solution to guarantee that smart contracts are protected against common attacks and vulnerabilities. We compare our solution to other blockchain-based solutions that are currently available. We discuss how our solution can be customized with minimal effort to meet the needs of other systems experiencing similar problems. In the future, our solution can be improved by developing an end-to end DApp. Furthermore, the smart contracts can be deployed and tested on a real private Ethereum network. Finally, the Quorum platform can provide better confidentiality because transactions among entities can only be viewed by specific participants and nobody else, which is not the case in our solution, where transactions between

two participants are viewed by other actors authorized in the private blockchain.

## VI.REFERENCES

[1] L. A. Dajim, S. A. Al-Farras, B. S. Al-Shahrani, A. A. Al-Zuraib,
and R. Merlin Mathew, ``Organ donation decentralized application using
blockchain technology," in Proc. 2nd Int. Conf. Comput. Appl. Inf. Secur.
(ICCAIS), May 2019, pp. 14, doi: 10.1109/cais.2019.8769459.

[2] A. Powell. (Mar. 18, 2019). A Transplant Makes History. Harvard Gazette.
[Online]. Available: https://news.harvard.edu/gazette/story/2011/09/a transplant-
makes-history.

[3] Organ Donation Facts and Info: Organ Transplants. Accessed:
Apr. 18, 2021. [Online]. Available: https://my.clevelandclinic.org/health/
articles/11750-organ-donation-and-transplantation.

[4] (Mar. 21, 2019). Facts and Myths About Transplant. Accessed:
Apr. 21, 2021. [Online]. Available: https://www.americantransplant foundation.org/about-transplant/facts-and-myths.

[5] Organ Procurement and Transplantation Network. Accessed:
Apr. 18, 2021. [Online]. Available: https://optn.transplant.hrsa.gov/
resources/ethics/ethical-principles-in-the-allocation-of-humanorgans.

[6] How Donation Works. Accessed: Jan. 7, 2022. [Online]. Available:
https://www.organdonor.gov/learn/process.

[7] UFO Themes. (Aug. 1, 2017). Organ Donation and Transplanta-
tion in Germany. Plastic Surgery Key. [Online]. Available: https://
plasticsurgerykey.com/organ-donation-and-transplantation-in-germany/

[8] Harvard Business Review. (Dec. 13, 2021). Electronic Health Records Can
Improve the Organ Donation Process. Accessed: Apr. 8, 2022. [Online].
Available: https://hbr.org/2021/12/electronic-health-records-can-improvethe-
organ-donation-process.

[9] U. Jain, ``Using blockchain technology for the organ procurement and
transplant network," San Jose State Univ., San Jose, CA, USA, Tech. Rep.,
2020, doi: 10.31979/etd.g45p-jtuy.

[10] M. He, A. Corson, J. Russo, and T. Trey, ``Use of forensic
DNA testing to trace unethical organ procurement and organ
trafcking practices in regions that block transparent access to
their transplant data," SSRN Electron. J., 2020, doi: 10.2139/
ssrn.3659428.

[11] Livemint. The Illegal Organ Trade Thrives in India-and it isn't
Likely to End Soon. Accessed: Dec. 21, 2021. [Online]. Available:
https://www.livemint.com/Politics/pxj4YasmivrvAhanv6OOCJ/Whyorgan-trafficking-thrives-in-India.html.

[12] D. P. Nair. (2016). Organ is Free, Transplant Cost is Problem.
[Online]. Available:
https://timesondia.indiatimes.com/life-style/healthtness/health-news/Organ-is-free-transplant-cost-isproblem/articleshow/54014378.cms

[13] P. Ranjan, S. Srivastava, V. Gupta, S. Tapaswi, and N. Kumar,
``Decentralised and distributed system for organ/tissue
donation and transplantation," in Proc. IEEE Conf. Inf. Commun. Technol., Dec. 2019, pp. 16, doi: 10.1109/cict48419.
2019.9066225.

[14] V. Puggioni. (Feb. 26, 2022). An Overview of the Blockchain Develop-
ment Lifecycle. Cointelegraph. Accessed: Apr. 8, 2022. [Online]. Available:
https://cointelegraph.com/explained/an-overview-of-the-blockchaindevelopment-lifecycle.

[15] History of Blockchain. Accessed: Apr. 8, 2022. [Online]. Available:
https://www.icaew.com/technical/technology/blockchain-andcryptoassets/
blockchain-articles/what-is-blockchain/history.

[16] M. Hölbl, M. Kompara, A. Kami²ali¢, and L. N. Zlatolas, ``A systematic
review of the use of blockchain in healthcare," Symmetry, vol. 10, no. 10,
p. 470, Oct. 2018, doi: 10.3390/sym10100470.

[17] V. Ferraza, G. Oliveira, P. Viera-Marques, and R. Cruz-Correia, ``Organs
transplantationHow to improve the process ?" Eur. Fed. Med. Inform.,
Cardiff, U.K., Tech. Rep., 2011, doi: 10.3233/978-1-60750-806-9-300.

[18] Organ Procurement and Transplantation Network. Accessed: Nov. 27,

2021. [Online]. Available: https://optn.transplant.hrsa.gov/governance/public-comment/standardize-organ-coding-and-tracking-system.

[19] A. Bougdira, A. Ahaitouf, and I. Akharraz, ``Conceptual framework for general traceability solution: Description and bases," J. Model. Manage., vol. 15, no. 2, pp. 509530, Oct. 2019.

[20] N. Mattei, A. Safdine, and T. Walsh, ``Mechanisms for online organ matching," in Proc. 26th Int. Joint Conf. Artif. Intell., Aug. 2017, pp. 345351, doi: 10.24963/ijcai.2017/49.

[21] S. Zouarhi, ``KidnerA worldwide decentralised matching system for kidney transplants," J. Int. Soc. Telemed. E-Health, vol. 5, Apr. 2017, Art. no. e62. [Online]. Available: https://journals.ukzn.ac.za/index.php/JISfTeH/article/view/287.

[22] Kidner Project. Accessed: Dec. 28, 2021. [Online]. Available: https://www.kidner-project.com.

[23] L. A. Dajim, S. A. Al-Farras, B. S. Al-Shahrani, A. A. Al-Zuraib, and R. M. Mathew, ``Organ donation decentralized application using blockchain technology," in Proc. 2nd Int. Conf. Comput. Appl. Inf. Secur. (ICCAIS), May 2019, pp. 14, doi: 10.1109/cais.2019.8769459.

[24] A. Soni and S. G. Kumar, ``Creating organ donation system with blockchain technology," Eur. J. Mol. Clin. Med., vol. 8, no. 3, pp. 23872395, Apr. 2021.

[25] G. Alandjani, ``Blockchain based auditable medical transaction scheme for organ transplant services," Tech. Rep., 2019, doi: 10.17993/3ctecno.2019.specialissue3.
users-track-themselves

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

**ABOUT AUTHORS:**

**G. SANTHI KUMARI**

currently pursuing MCA in SVKP & Dr.K.S Raju Arts & Science College affiliated to Adikavi Nannaya University, Rajamahendravaram. His research interests include Data Structures, Web Technologies, Operating Systems, Data Science and Artificial Intelligence.

**CH. SRINIVAS RAO**

is working as Associate Professor in SVKP & Dr K S Raju Arts & Science College(A), Penugonda, West Godavari District, A.P. He received Master's Degree in Computer Applications from Andhra University. His research interests include Operational Research, Probability and Statistics, Design and Analysis of Algorithm, Big Data Analytics