Review of “Blockchain-Enabled Trust Management in Service-Oriented Internet of Things: Opportunities and Challenges” by L. Wei [1]

Gagan Chowdary Chatu*,
CS5378 Advanced Computer Security
Texas State University, San Marcos, Texas, USA
Email: *akl103@txstate.edu

In recent years information and computer technology has improved by a significant margin. These improvements lead to growth of the Internet of Things (IoT).To provide high quality services. IoT devices need to be secure, trustworthy,and reliable. Blockchain is considered to be a driving technology used for trust management of service-oriented IoT. This review paper talks about trust issues in service-oriented IoT. It also analyzes and evaluates a blockchain based solution for trust management.

It is estimated that there will be 41.6 billion IoT devices connected by 2025 [2]. With the increase in the number of IoT devices, more diverse and efficient services can be developed. Service oriented IoT devices can request or provide services to other objects. These services include sharing information or computational resources to receive incentives. Trust between IoT devices and service-oriented IoT devices is key for quality of service. Malicious IoT devices could interrupt services and get more benefits which affects the quality of service. To solve the problem of malicious devices we need a trust management solution. Major challenges in the trust management of service-oriented IoT devices are listed below. [3]

- The scale of network refers to the number of devices.
- Limited computing and storage resources of devices.
- The Adaptability of the system to changing devices.
- Attack resistance of the system to malicious devices.

Blockchain is a distributed ledger technology that is popularly used in cryptocurrency. It is known for immutable, timestamped blocks of information. Since blockchain is distributed, there is no need to trust a third party or a cloud server. Blockchain uses hashing so that each block is tamper-resistant. A requester could verify trust of a provider by verifying the historical and behavior data. They could choose to select or reject services based on trustworthiness.

Trust is an abstract and complex topic [1]. Trust in IoT can be defined as reliability, integrity, security, and other characteristics of the object [4]. Trustworthiness of the object can be measured based on identity, behavior data, service records, equipment characteristics. Using classification in [3], author divided trust management into five parts. They are listed below.

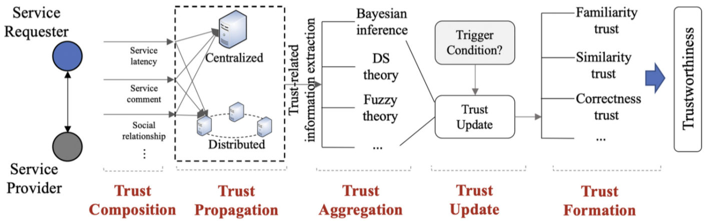

Fig. 1: The key ingredients of trust management in service-oriented IoT [1]

- Trust composition refers to the attributes that will be used to calculate trustworthiness.
- Trust propagation refers to how we can access trust-related information.
- Trust aggregation refers to an algorithm used to calculate trustworthiness.
- Trust update refers to the condition based on which trustworthiness of the object is updated.
- Trust formation refers to property of trust used when calculating trustworthiness.

The author discusses the common forms of attacks that a system could encounter. They are listed below.

- Self promoting attacks (SPA) are attacks in which devices tend to give good recommendations to itself to increase probability of getting a request
- Bad-mouthing attacks (BMA) are attacks in which malicious devices tend to give bad recommendations to others to decrease chances of getting a request.
- Ballot stuffing attacks (BSA) are attacks in which malicious devices tend to give good recommendations to others to increase chances of getting a request.
- Whitewashing attacks (WA) are attacks in which devices leave the network to wash their previous bad behavior.
- Discriminatory attacks (DA) are attacks in which de-

vices prefer to send high quality services to familiar devices and low quality of services for unknown devices.
- Opportunity service attacks (OSA) are attacks in which devices tend to intentionally provide high quality of services when they feel trustworthiness is low.

Blockchain based solution provides attack resistance to SPA, BMA, BSA by providing immutable timestamp information which is traceable. Requester can evaluate trustworthiness of a provider and choose not to use services from malicious devices. WA can be detected by capturing more information like location, task duration and other information. To avoid DA attacks, attributes are gathered from different sources and historical records can be verified for conflicts. An OSA attack can be avoided by frequency of failures from the service information on the blockchain and design a punishment mechanism to lower the trustworthiness of the device.

Current research could solve some of the challenges but there are many other new challenges that needs research. The author, describes future research challenges as Dynamic changes of trust composition, trust related data management, trust qualification, and high performance consensus protocol. Dynamic change of trust composition talks about the need of adaptable data structure that is suitable for the heterogeneous nature of IoT devices. Trust related data management talks about the need for securing of the sensitive information about the service providers and requesters as blockchain stores information more transparently. Trust quantification talks about the specific algorithms and it's effectiveness of calculating trustworthiness. Several consensus protocols are currently in use, but their effectiveness in a high performance context of service-oriented IoT devices requires further research.

The field of service-oriented IoT has grown quickly in recent years, and the problem of trust management has generated a lot of concern. Blockchain already has a lot of potential for improving trust management's efficiency and security. A thorough and in-depth analysis is performed on the unique roles that blockchain plays in improving trust management and combating trust-related threats. It opens up new challenges and topics for future research.

References

[1] L. Wei, J. Wu, and C. Long, "Blockchain-enabled trust management in service-oriented internet of things: Opportunities and challenges," in *2021 The 3rd International Conference on Blockchain Technology*, ser. ICBCT '21. New York, NY, USA: Association for Computing Machinery, 2021, p. 90–95. [Online]. Available: https://doi-org.libproxy.txstate.edu/10.1145/3460537.3460544

[2] "International data corporation (idc)," 2020, retrieved on June 18, 2020. [Online]. Available: https://www.idc.com

[3] J. Guo, I.-R. Chen, and J. J. Tsai, "A survey of trust computation models for service management in internet of things systems," *Computer Communications*, vol. 97, pp. 1–14, 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140366416304959

[4] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for internet of things," *Journal of Network and Computer Applications*, vol. 42, pp. 120–134, 2014. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804514000575