A study on Trust Management System for Ubiquitous and Pervasive IoT Application

AnupPatnaika[a], BanitamaniMallik[b], and M.VamsiKrishna[c]

[a]
Research Scholar, Department of Computer Science and Engineering, Centurion
University of Technology and Management, Odisha, India.
[b]School of Applied Sciences, Centurion University of Technology and Management, Odisha, India.
[c]Department of Computer Science and Engineering, Chaitanya College of science
and Technology, Madhapatnam, Kakinada, India

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 20 April 2021

Abstract: IoT (Internet of things) is one of prominent technologies for provisioning of services through smart, intelligent and heterogeneous devices connected to each other via internet. With environmental influences, the widely used IoT applications are much prone to security and privacy related problems. In order to address these issues, many solutions were proposed in the recent past but most of these models have not fulfilled yet all the promises of IoT requirements. Furthermore, considering the characteristics of IoT involving heterogeneity, dynamic, mobility of nodes, energy constraint, less computing power devices, then it's challenging to propose dynamic trust management system (TMS). This paper contributes the comparison study of existing trust management approaches applied to various IoT based applications.Further, it highlights open issues, research challenges and provides the future direction to address the current research challenges through research model, holistic trust management.

Keywords: IoT; trust management system; trust model; convergence; environmental influences

1. Introduction

Need of connectivity among devices to share resources, ubiquitous communication and assigning different access levels giving rise to new paradigm, Internet of Things (IoT). This network is envisioned as network of smart objects, namely radio frequency identification (RFID) tags, near frequency communication (NFC), sensors, actuators, PDAs, and smartphones, as well as virtual objects such as data and virtual desktops on the cloud. These devices sense, collect and monitor different types of data from the environment, then further aggregated, processed, analyzed and mined in cloud to enable providing automated service to human life. IoT integration with different technologies starting from sensor devices, IPv6 and Enhanced Communication Protocols, Cloud Computing to business reports are working at different layers of this network layered structure (Table 1).

Owing to growing usage of IoT application in recent years, maintaining trust between various heterogeneous devices is difficult task, so malicious ones may produce erroneous sensing data and impact the performance of the whole network. Main challenges (Access Control, Security, Privacy, Data mining, data integration) issues that a IoT network has to face when unknown devices start interactions without any pre-validation. The motivation behind providing trustworthy and secure IoT network nodes is to develop holistic trust management system which not only verifies the nodes prior, but also grants right access level and make sure the interactions between devices are secure generating trustable data. The concept of trust is to measure the confidence and reliance of aparticular entity on other entities at specific time span which is having multiple properties,

- Direct/Local Observations
- Indirect/Global Observations
- Asymmetric and non-transitive
- Objective and Subjective
- Context dependent
- Time dependent and Dynamic

These trust properties must be considered while defining trust metrics to calculate the trust score. Trust propagation and assessment steps captures these properties value and provide the data to trust evaluation model step to reach the final score for decision making.Also, these trust evaluation model steps are part of Trust management system (TMS) and then it disseminates and updates the trust score to enable secure interactions of devices.Incorporating trust management module with IoT system provides numerous benefits to objects connected in the network and resolves the sensitive issues, such as data privacy & security, issue of uncertainty, scalability, and legitimate governance. TMS schemes are vulnerable to different types of attacks which can happen in one or multiple areas of trust components starting from information gathering to decision making. Trust related attacks disrupting the network function are outlined (Table 2).

The rest of the paper is organized as follows: section 2 surveys four different trust management approaches namely centralized model, distributed model, and blockchain based model and also conducts a comparative study

of current state-of-art trust management mechanisms. Research Open Issues and Scope of future work are discussed corresponding section 3 and Section 4. Section 5 proposes conceptual research model for trust management system followed by the conclusion in section 6.

2. Trust Management Models

2.1. Centralized Trust Mechanism

Secure trust mechanism, Awan et al. [1] also plays critical role in vehicle Ad-hoc network (VANET) and it senses there is risk of spreading misinformation between vehicles and infrastructure due to lack of security aspects, therefore Cluster based trust mechanism in a cluster can identity highest trustworthy node as cluster head (CH) which can eliminate malicious and compromised nodes' active participation inside device to device communication. The achievement of this centralized mechanism is to bring the stability of network by increasing network lifetime and reducing computation overhead, certainly it can't be an ideal approach in case of large volume data and critical application, since it has to consider energy consumption as well.

Super node acts as centralized trust manager keeping different trust related modules for trust evaluation and monitoring of devices. It keeps trust values of cluster master nodes and address of cluster nodes in its routing table. Central system supervises the whole TM-IoT network includes communication to master node from IoT application through the REST API calls and sending instructions to CNs to access repository data. This prototype has not been yet implemented through the simulation models to understand its impact on different network parameters to achieve trust convergence, trust rely and resilience against the malicious nodes Alshehri and Hussain [2].

Routing attacks and trust system attacks are also addressed through the trust management system Hajibabaei et al. [3]. Here sink receives the control message from sensor nodes and compute the trust value, then later disseminates the trust values to the nodes for finding the next hop path. This approach is able to transmit the data in secure path with selecting nodes having delivery ratio. Trust based routings finds the path which is possible trustable and optimal.

Most of the trust management system not considered the context which is not suitable to dynamic network, therefore context based trust model is required for this hour Abderrahim et al [4]. This mechanism provides the dynamic trust value of objects depending on different contexts and different services even if there is no previous history of transactions exists for the node. It uses Jaccard Coefficient to establish the social similarity between objects and decision tree technique to predict nodes behaviors.

Intrusion detection mechanism is essential to restrict internal or external attacks to the network which considers geographical localization concept for node identification Maddaret al.[5]. This results show the efficiency of geo-location model and also good at attacks detection rate.

Intrusion detection system (IDS) with hybrid trust architecture having centralized intrusion detection analysis and also, distributed data collection mechanism for securely sending IP flow records to local or remote IDS components is proposed Santos et al. [6] which shows promising results for finding the false positives. This framework hasn't been tried yet with diverse communication technologies and also need a proposal of other threat finding means.

2.2. Distributed Trust Mechanism

Hamdani et al. [7] proposed static/dynamic distributed trust model to compute the trust value of node. Trust computation is calculated based on direct observation and also updated the nodes value at every transaction. It is able to identify and mitigate on off attack (OOA) in IoT domain. Open source simulator provides the provision of saving complete transaction history of the network, later it can be downloaded to CSV file to implement the graphs for analysis.

From a general trust based framework, mature trust model can be realized, which involves trust extraction, trust calculation, transmitting trust value and finally decision making based on trust status. Further, steps trust establishment and computing trust value varies in different trust models. There are many techniques for doing the trust calculation based available trust data. Here it involves layered trust model, where extracting of trust information related to each layer starting from core layer to application layer, and final decision making is of two types either access control policy or self-organizeddecision making based on trust, Wang et al. [8].

Geographic location based intrusion detection model Madder et al. [9] for internet of things is able to eliminate the malicious nodes with help of mathematical model for calculating/update nodes trust value. This model finds the transmitter node localization using the 'TDOA' technique, which makes us able to detect any sybil or identity theft attack. Still it needs to improve lifetime of the network by integrating cloud technology to retain energy consumed and also required to develop the advance detection rule including more criteria and components of IoT.

Ray et al. [10] proposed 3-tier mobile cloud architecture having IoT light weight devices at bottom tier, then in middle tier cloudlet, heavyweight sensor devices and top layer home cloud servers. This cloud hierarchical service management protocol considers friendship, social contact and community interest similarity to calculate the trust value. It also uses intelligent cache management allowing the query regarding the service trustworthiness of a local IoT device to be answered by a local cloudlet without help of the cloud server for query processing which improves the application responsiveness. Here the comparative analysis with other baseline protocols show that it achieves the scalability without any compromise of convergence, accuracy and resilience against attacks.

Context-Based Trust Evaluation System Model Altaf et al. [11] shows its effectiveness in filtering out Sybil attacks, detecting on-off attacks and the malicious nodes causing service-oriented attacks. Trust score is calculated based on direct and indirect experience with assigned adaptive weights to maximize the performance of the protocol that means improvement of trust accuracy. Further context similarity calculations measure is providing additional benefit to remove the bad nodes which are threatening for Sybil attack.

Adaptive trust model Chen et al. [17] uses sliding window and time decay function for direct trust and k-means algorithm for recommendation trust of trust evaluation for synthesis trust. Simulation results are not very impressive when malicious nodes are growing in the network for above 70%, therefore it will impact the accuracy of IoT objects calculation. Further,instead fixing trust third party (TTP) module in advance, dynamic TTP module can be decided based on the trust value of IoT objects, the remaining energy and the computing power.

2.3. BlockChain based Trust Mechanism

Access control system model involves trust and reputation system along with leveraging blockchain technology advantages of distributed processing and storage, transactions transparency and non-repudiation, immutable ledgers Putra et al.[12]. It considered docker container having private ethereum network to set up proof of concept of the proposed protocol. Evaluation of this mechanism feasibility had not been done on basis of energy consumption, trust convergence, and packet delivery ratio parameters.

Trusted consensus fusion scheme is proposed by Wang et al. [13] which provides the trust score based on trust evaluation system along with the X-BFT. It is evaluated according to their historical behaviors in the past consensus process and stored as distributed public ledger of blockchain along with current trust score which is part of new block validation. The trust consensus protocol TXBFT considers four different type of nodes based on the trust value which decides its responsibilities and finally, election of parliament with one leader and many verifiers are decided by election strategy based on trust mechanism.

Main purpose of integrating blockchain with IoT is to take the former technology advantages of reliability, traceability and integrity of information, therefore blockchain based trust management Lahbib et al. [14] gives the features of improved the privacy and security of data during storage, the sharing with other devices, tamper proof data due to immutability, and ensures information integrity changes. There are primarily three components part of this trust architecture, authentication manager doing the device identities, generating authorization token and making authentication decisions, then trust manager calculating trustworthiness degree and finally miners making transactions into blocks after consensus validation of trust data.

Resource constraint IoT nodes not having enough computation power, so mobile edge nodes are heavy weight sensor nodes deciding degree of trustworthiness of sensor nodes. Blockchain-based trust management mechanism can place the smart contracts which will do trust evidence collection, trust score computation and consensus on trust transactions Wu and Liang [15].

Cha et al. [16] proposed cloud architecture based secret sharing algorithm through external cloud services used to protect privacy, security and easy access of data in a distributed system. This blockchain empowered cloud architecture approach uses secret sharing algorithms (SSA1 or SSA2) to protect personal information, also improves its data integrity and security. Mainly collected data from physical layer is distributed using SSA to fog layer and now the same data assigned using SSA can be reconstructed by collecting from CSP data. For the advanced applications of smart city, the distributed sharing algorithm can be further analyzed to benchmark and demonstrate the secure communication, data privacy achieved in real time.

Yavari et al.[17] explained blockchain-based authentication protocol has tested its feasibility against different security attacks, and then addressed its security pitfalls in its improved authentication protocol version. Further, formal and informal security analysis on improved blockchain-based authentication protocol is realized in this approach and formal proofing is done using the Scyther tool. Implementation of IBCbAP is done through nodejs JavaScript language and used as plugin to Ethereum local blockchain network to access the nodes.

Cooperation model, Oualhaj et al.[19] blockchain based decentralized trust management following markov chain model represents the trusted state of node and update of node trust values. Propose proof-of-work is achieved through proof of trust and proof of stake in this approach, where proof of trust is finding valid transactions based on the trust values and proof of stake is finding of new miner, then creating new data block. Through distributed consensus process it identifies the malicious nodes providing either wrong trust values or extreme trust values. This decentralized trust management approach also saves energy and transaction costs integrating with blockchain technology.

Field programmable gate array (FPGA) Xu et al.[20] based blockchain system removes several limitation of IIoT(IndustrialIoT), such as high power consumption, low decentralization and single root trust. It allows the intensive computation/storage to high performance computers and also makes the devices to participate in block creation to have high decentralization. FPGA approach is power efficient trust execution environment, allows blockchain operations for the energy constraint IIoT devices. Based on distribution pattern and exceed the defined threshold, it's able to filter out the malicious nodes which are not following the pattern.

2.4. Comparison Study of Protocols

Comparison study of different trust management approaches based on multiple parameters is analyzed on this table 3.

3. Research Open Issues

1. Lack of comprehensive research work on the IoT vision (anytime, anywhere, and anything), to access device acquiring data transmitting from one point to other with optimal security, privacy of contents.
2. Current state-of-art doesn't address all types of threats happening inside IoT
3. Need of efficient trust management strategy that adaptively adjust with a spontaneous dynamic environment like IoT
4. Trust management strategy should consider device properties (limited storage, low processing capability power, less energy), network properties (throughput, network lifetime, packet delivery ratio, delay, and bandwidth) and network contextual parameters (authentication, authorization, access control, privacy and security)
5. Need of an optimized trust management solution that can stand with scalability IoT network contain huge number of IoT devices.
6. An integrated solution for trust evaluation processes execution through blockchain or fog computing is required
7. Various attacks are expected in IoTenvironment that make maliciousthe reputation/recommendation values, device identity and routing path, therefore aholistic structure of TMS which can show resilience against attacks.
8. Recommendations handling and management strategies are required to deal with falsely recommendation.
9. A trust management system design is required that support cross platforms, i.e. can be implemented on heterogeneous IoT devices.
10. A compatible trust management solution that works with existing security solutions and does not affect their functionality is required.
11. Major point that trust management needs to consider in IoT scenario is context-awareness. A solution is required that takes context-awareness multiservice into consideration.
12. No robust autonomic trust management in cloud based dynamic IoT system, so encouragement to develop more distributed trust management framework for cloud ecosystem.
13. Comprehensive study of hybrid trust framework is required now-a-days.

4. Scope of future work

1. Future proposed modelsshould be tried for real time very complex applications with short range, tiny devices, and NFC devices with heterogeneous IoT networks.
2. Different mechanisms such as static weighted sum,Bayesian learning, Subjective Logic, Dempster–Shafer theory (DST)to adopt finding the trust score for our proposed protocols to find the difference in trust values of nodes
3. Context-aware multi-service trust management system, where grouping nodes' past experiences segregated into specific trust metrics to address new requirements of the IoTmore appropriately.
4. Enhancement trust management mechanism for public un-permissioned blockchain network
5. Research towards trust evaluation conflicts, where multiple providers having same trust value for a consumer node.
6. Autonomic trust management framework development for IoT cloud ecosystems for network scalability prospective.
7. Develop a trust model which can aggregate different trust models used by various types of nodes in different types of networks.
8. Need to have a mechanism to calculate and integrate multi trust metrics for a trust model as service
9. One of critical research direction is to find solution for trust systemof heterogeneous network platforms deployed devices.
10. Importance to be given to design one holistic conceptual framework first to considerIoT trust models for resilience against various attacks on devices identity, routing path and message communication.

5. Future Research Models

Our self-adaptive and dynamic trust model having following steps, includes pre-state of node as well before considering latter's service/resource request.Mainly the Trust Propagation, Trust Assessment and Trust Evaluation steps are related to finding value of trust metrics which is the trust score of service requester, based on this score the node will be treated either trustworthy or malicious. In our model, dynamic access control policy assigns different access level rights to the node based on this trust score.

General trust metrics is defined for our research model as follows, where apart from direct/indirect interactions; other parameters impacting trust score of node are included.

TV(Y) By(X) = aDI(Y) + bRII(Y)+cEPT(Y)… (1)

- TV(Y) By(X): Trust value of Y evaluated by X, Y: Service Requester and X: Service Provider, $0 \leq$ TV(Y) By(X) ≤ 1.
  - ET(Y) : Environment properties trust
  - SSG(Y): Subscribed Security Groups of Y
  - CEB(Y): Common Elite Buddies of X about Y
  - ACP(XY): Additional Check Points of X and Y
  - DI(Y): Direct Interactions from X to Y

- RII(Y): Reputation Indirect Interactions to Y

The fuzzy set derived from the above trust value equation is defined as below to interpret the node's action as trustable/untrustable.

- FS = { Highly trustable if 0.8 <= TV <=1
  Trustable if 0.5 <= TV <=0.8
  Untrustable if 0.3 <= TV <=0.5
  Very Untrustable if 0 <= TV <=0.3 }

We need multiple dynamic subroutines for this trust metrics to get the score, firstly to find the common elite buddies list of service provider, reputation of service consumer, additional checkpoints of both parties. The proposed trust system workflow is outlined below Figure 1.

6. Conclusions

In this survey, it was emphasized to set future research trends for building up trust management (TM) solution based on self-adaptive, scalability, and context-aware. The current analysis on state of the art of trust management provides the research challenges, open issues and paved the way to propose a new research model for holistic TM. Our research model trust metrics not only considers direct & indirect interactions, but also considers Subscribed Security Groups, Common Elite Buddies, Additional Check Points, and Prioritized Reputation Indirect Interaction of service requester to calculate the trust score for thefinal decision on dynamic access control policy.Finally, we have to analyze the performance mainly on trust convergence, trust accuracy and resiliency against attack properties of trust model. There is always tradeoff between low trust fluctuations with trust convergence that means trust evaluation is approaching to optimal value faster with increase of time.

References

1. Awan, Kamran Ahmad, IkramUd Din, Ahmad Almogren, Mohsen Guizani, and Sonia Khan. "StabTrust—A stable and centralized trust-based clustering mechanism for IoT enabled vehicular ad-hoc networks." Ieee Access 8 (2020): 21159-21177.
2. Alshehri, Mohammad Dahman, and FarookhKhadeer Hussain. "A centralized trust management mechanism for the internet of things (CTM-IoT)." In International Conference on Broadband and Wireless Computing, Communication and Applications, pp. 533-543. Springer, Cham, 2017.
3. Hajibabaei, Fatemeh, and Mohammad HossinYaghmaeMoghaddam. "Proposing a centralized trust management system to detect compromised node in WSN." In ICCKE 2013, pp. 315-320. IEEE, 2013.
4. Abderrahim, Oumaima Ben, Mohamed HoucineElhedhili, and Leila Saidane. "CTMS-SIOT: A context-based trust management system for the social Internet of Things." In 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 1903-1908. IEEE, 2017.
5. Maddar, Hela, WafaKammoun, and Habib Youssef. "Effective Centralized Trust Management Model for Internet of Things." In International Conference on Intelligent Data Engineering and Automated Learning, pp. 46-57. Springer, Cham, 2018.
6. Santos, Leonel, Ramiro Gonçalves, Carlos Rabadao, and José Martins. "A flow-based intrusion detection framework for internet of things networks." Cluster Computing (2021): 1-21.
7. Hamdani, Syed Wasif Abbas, Abdul Waheed Khan, Naima Iltaf, and Waseem Iqbal. "DTMSim-IoT: A Distributed Trust Management Simulator for IoT Networks." In 2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), pp. 491-498. IEEE, 2020.
8. Wang, Jing Pei, Sun Bin, Yang Yu, and Xin XinNiu. "Distributed trust management mechanism for the internet of things." In Applied Mechanics and Materials, vol. 347, pp. 2463-2467. Trans Tech Publications Ltd, 2013.
9. Maddar, Hela, WafaKammoun, and Habib Youssef. "Effective distributed trust management model for Internet of Things." Procedia Computer Science 126 (2018): 321-334.
10. Chen, Ray, JiaGuo, Ding-Chau Wang, Jeffrey JP Tsai, Hamid Al-Hamadi, and Ilsun You. "Trust-based service management for mobile cloud IoT systems." IEEE transactions on network and service management 16, no. 1 (2018): 246-263.
11. Altaf, Ayesha, Haider Abbas, Faiza Iqbal, Malik Muhammad ZakiMurtaza Khan, Abdul Rauf, and TehsinKanwal. "Mitigating service-oriented attacks using context-based trust for smart cities in IoT networks." Journal of Systems Architecture 115 (2021): 102028.
12. Dharma Putra, Guntur, VolkanDedeoglu, Salil S. Kanhere, and Raja Jurdak. "Trust Management in Decentralized IoT Access Control System." arXiv e-prints (2019): arXiv-1912.

13. Wang, Ke, Chien-Ming Chen, Zuodong Liang, Mohammad Mehedi Hassan, Giuseppe ML Sarne, Lidia Fotia, and Giancarlo Fortino. "A trusted consensus fusion scheme for decentralized collaborative learning in massive IoT domain." Information Fusion (2021).
14. Lahbib, Asma, KhalifaToumi, AnisLaouiti, Alexandre Laube, and Steven Martin. "Blockchain based trust management mechanism for IoT." In 2019 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1-8. IEEE, 2019.
15. Wu, Xu, and Junbin Liang. "A blockchain-based trust management method for Internet of Things." Pervasive and Mobile Computing 72 (2021): 101330.
16. Cha, Jeonghun, Sushil Kumar Singh, Tae Woo Kim, and Jong Hyuk Park. "Blockchain-empowered cloud architecture based on secret sharing for smart city." Journal of Information Security and Applications 57 (2021): 102686.
17. Yavari, Mostafa, Masoumeh Safkhani, SaruKumari, Sachin Kumar, and Chien-Ming Chen. "An Improved Blockchain-Based Authentication Protocol for IoT Network Management." Security and Communication Networks 2020 (2020).
18. Chen, Guozhu, Fanping Zeng, Jian Zhang, Tingting Lu, Jingfei Shen, and Wenjuan Shu. "An adaptive trust model based on recommendation filtering algorithm for the Internet of Things systems." Computer Networks 190 (2021): 107952.
19. Oualhaj, Omar Ait, Amr Mohamed, Mohsen Guizani, and AimanErbad. "Blockchain Based Decentralized Trust Management framework." In 2020 International Wireless Communications and Mobile Computing (IWCMC), pp. 2210-2215. IEEE, 2020.
20. Xu, Lei, Lin Chen, Zhimin Gao, Hanyee Kim, Taeweon Suh, and Weidong Shi. "FPGA based Blockchain System for Industrial IoT." In 19th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom 2020). 2020.
21. Zhaofeng, Ma, Wang Lingyun, and Zhao Weizhe. "Blockchain-Driven Trusted Data Sharing with Privacy-Protection in IoT Sensor Network." IEEE Sensors Journal (2020).