Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 7, Issue. 11, November 2018, pg.249 – 260

Dynamic Trust Management Implementation in IoT: A Review Paper

Anup Patnaik[1]; M. Vamsi Krishna[2]

[1]Research Scholar, Department of Computer Science and Engineering, Centurion University of Technology and Management, Paralakhemundi – 761 211, Gajapati, Orissa
[2]HOD, Department of Computer Science and Engineering, Centurion University of Technology and Management, Paralakhemundi – 761 211, Gajapati, Orissa

Abstract: Internet of Things (IoT) is characterized as dynamic distributed network involves provisioning of services, establishing communication protocols among the ubiquitous smart devices to gather the information translated into decision-making process for various automated systems. In this IoT domain, specific challenges are foreseen, unless those are addressed it's hard to connect ubiquitous computing world to betterment of human life. IoT network elements processing inside widely spread random information which spurs up the problems on contextual parameters i.e. privacy, security, trust, integrity for data, confidentiality, authentication, access control, device safety and on other stake holders participated as an entity in the infrastructure. Each contextual parameter is playing prime role on IoT success journey. Hence, we tried to provide the current research status on dynamic trust management schemes pertaining IoT paradigm and subsequently, our analysis brings out indispensable pointers for open issues on which future research work would get precise direction to frame desired trust models to prevent malicious attacks. Higher level of trustworthiness to be achieved through models will steer new revolution to IoT core sectors such as Home automation, Logistics/Transportation, till now cross sectors information sharing is completely undermined in the recent research works, definitely it's an area where more research work could be an option to carry out further.

Keywords: Internet of Things; decision-making process; dynamic trust management schemes

1. Introduction

The Internet of Things (IoT) in ubiquitous computing world is termed as uniquely identifiable things or entities or objects which are seamlessly connected over heterogeneous network for intensive interactions to achieve common benefits through facilitating the services. Basically, evolved wireless communication technology for distributed system in recent past is drastically changing the prospective of internet connectivity limited to tiny devices moving to high-performance smart devices. The real-time objects Sensors, actuators, and Aggregators in IoT paradigm are connected to each other solely to send(receive) data(information) and these accumulated data in middleware triggers data driven decisions for automated systems. This relationship in IoT established by things to things or things to human or human to things communications are largely more complicated than perceptions because of risk and uncertainty.

The increased pervasiveness of whole IoT network setup stays in public domain and modes of communication are also exposed to everyone including intruders, therefore these smart objects/things/entities can be compromised sometime to start unwanted activities to launch attacks on the network and is hard to trace vulnerability using traditional techniques such as cryptography models, OS security models, identity models. Also, current state-of-art models are very much sophisticated and instilling these will consume more processing power, bandwidth, and energy of devices hence resource constrained entities of IoT might not implement to achieve common goals.

Furthermore, before designing whole IoT architecture, keeping in mind its importance in real time the security, trust/reliability, privacy, identity managements which are under threat due to the great challenges must be protected, otherwise it will have significant impact on the performance of the IoT applications. Out of the aforementioned managements, trust management is the important aspect for the secured IoT which can prevent untrustworthy devices performing malicious attacks. The research work here is to do the survey on the existing trust management protocols to get insight of the types of metrics (QoS, Social) considered for trust composition, how trust aggregation techniques selected to get unique convergent value and finally, trust update for neighbor nodes dynamically happening before starting the interaction based on output of trust aggregation technique and later design a dynamic trust management system for IoT devices. Certainly, the challenge to trust management in IoT environments is very stiff subjective of IoT applications, yet the accurate trust assessment could cope with dynamic environments in

the presence of malicious, erroneous, partly trusted, uncertain and incomplete information devices. Our proposed trust management protocol must adapt to the dynamically changing network environment, and to support heterogeneous entities, different communication patters such that the trust assessment for devices are accurate and performance of any IoT application built on top of the trust management protocol is optimized as there is no uncertainty prevailing for IoT elements to initiate interaction leading to reliable distributed trust management system.

The rest of this paper is organized as follows: Section 2 analyzes the available research approaches to security, privacy, trust, confidentiality, access control and non-repudiation in IoT to identify key shortcomings of current state-of-art approaches i.e. background and related work. Section 3 provides six layers IoT architecture which would be appropriate to handle requirements of this ecosystem. Open issues are summarized in section 4 after the analysis Trust Management Model and Frameworks. Section 5 describes the comparison study of different trust models discussed in related works. The conclusion of the paper and future work is in section 6.

2. Literature Review

Trust management protocols so far can be classified broadly following types used to evaluate trust levels in dynamically challenging environment of IoT framework to maximize application performance.

1. Dynamic trust management Protocol (DTMP) considering social environment/relationship factors
2. Trust and reputation management protocol considering fuzzy based notions
3. Trust management protocol considering reliability factor (cooperation between IoT nodes)

Unquestionably, trust level upholds desired acceptance level of security which prevents the objects/things from wrong doing initially and prevents compromised nodes (Sfar et al. 2018) to launch any type of attacks such as bad-mouthing attack, selective behavior attack, Ballot stuffing attack, on-off attack Inside.

Ramakrishna (2016) proposed framework of online social IoT system to obtain trust value using social aspects of IoT device owners. Here, social IoT model depends on social connections among people who are proprietors of IoT devices and in this adaptive trust management, each node only updates trust towards others of its interest upon encounter or interaction events. Current work in this paper may not be suitable to diagnose the faulty nodes

and there is no specific procedure to adjust trust parameter properties of social trust application for dynamically changing environment.

Till now, we focused on the robust IoT framework which can overcome problems experiencing for intense interaction among the things. Another research work proposed by Mendoza and Kleinschmidt (2015) which addresses on-off attack to wipe out malicious nodes of a multiservice IoT paradigm and this trust model is not so effectively identifying for other types of attack. This trust model architecture is of three phases distributed trust management schema depends on direct observation between the nodes when requested for the services and number of neighbors with which the node has to communicate. The results from the simulation for the On-Off attack, shows that a factor influencing for the detection of malicious nodes is the number of neighbors and network speed which may create a delay in the assignment of the maximum score of distrust for the malicious nodes.

The fuzzy based novel behaviour trust and reputationmodel for IoT/CPS environment was proposed by Chen et al. (2011) to address security challenges like detection of malicious nodes. This model evaluates both local trust and global trust values between two nodes in WSNs of IoT because nodes in this environment are following dynamic topologies having other characteristics such as bandwidth constraints, energy constraints, and limited physical security. Main advantage of this model which separates from other existing models is that along with fuzzy direct, indirect trust model, it explores all the possible n level indirect trust relationship between two nodes using AOVP routing protocol, therefore trust evaluation is globally available to all member nodes of the WSN community and updated trust vale if any member node issues a new evaluation of a sensor node.

The security issues of IoT involved in three layers architecture are highlighted by Jing et al. (2014) and then proposed different key technologies and solutions to the possible issues of each layers. IoT consists of RFID nodes and WSN nodes following diverse protocols to communicate, hence the heterogeneous data formats and data contents are expected to receive from devices. This architecture model also addresses problems not only related to heterogeneous data of one layer but also focused on the between layers integration issues. In hierarchical IoT structure, single security system may not be applicable to all the applications, and mostly IoT security issues are driven by application, therefore this architecture suggested to develop abstract

security framework having the customizable facility to provide basic security solution to common IoT applications.

Prior to the security issues, addressing of the nodes in network is more important to discourse scalability, performance and latency of system. Mahalle et al. (2013) suggested hierarchical addressing (CCHA) as identifier format for nomadic devices which demonstrates creating different domains as grouping of similar devices/sensors. This approach solves the problem of energy expenditure for storing and communicating data to/from neighbor nodes, end to end delay packet transmission, overall throughput, these are characteristics of stable and organized IoT system, and top of this, some robust abstract model can be applied to take care of security, privacy and other contextual parameters, hence an efficient IDM with context-aware clustering is better strategy than existing flat addressing identification mechanism.

Hierarchical addressing of devices does not stand by for all types of IoT applications, rather some applications like disaster monitoring where disrupt in communications happens intermittently needs self-reorganization of devices in heterogeneous networks so that the stalled communication could be started among the devices through other available channels which is highly desirable in distress situations to make decisions. The advantages of the self-organization can be extrapolated to other aspects of IoT architecture such as cross layer design for devices as its supporting different protocols, multi-radio communication technology, and use of delay tolerant technologies to connect discrete network system due to communication breakup. Athreya and Tague (2013) identified the key components and their respective challenges to form a Self-adaptive self-organized network.

Gago et al. (2017) proposed framework with four layer architecture where proactive trust approach is introduced in each phases to overcome challenges inherit inside IoT scenarios. This model provides holistic solution to trust management in the IoT considering the interoperability, dynamicity and evolution which means it re-calculates the trust at run time with the change of trust model in accordance with change of position of gadgets/devices. The context definition service initially figures out the different contexts and their specific purpose for the thing, once context is defined then this framework cites the type of model requirement for identity, privacy or trust.

Till now all these above models are concentrating on the nodes capable of performing single function then deriving the trust but aiming in heterogeneity in IoT paradigm it may be

possible that node belongs different context having different function, in this scenario it would be more accurate to find dynamic trust at run time. Saied et al. (2013) suggested context aware and multi service approach trust management system design for the internet of things overcomes the current limitation of the related network system and addresses the new requirements of the IoT. This centralized TMS five phases model can withstand expected attacks more efficiently than other counterparts proposals.

Trust establishment among entities from heterogeneous domains without past interaction or prior agreed policy for RFID applications of IoT is herculean task to achieve so Wu and Li (2017) proposed hierarchical trust management framework which includes a diversity of trust evaluation for diversity of trust requirements of RFID tags, RFID readers and authentication centers in the multi-domain RFID systems. There are two trust layers such as RFID reader trust layer to evaluate the trust of readers leveraging D-S evidence theory based scheme (D-S scheme) and verification of interaction proof based scheme (VIP scheme) and other one is the authentication center trust layer, an administration center is used to manage the trustworthiness of authentication centers in a centralized way. Few areas are still not addressed clearly that involves performance optimization of the trust management system and also not analysed vulnerability of the system to all the threats.

Other than trust management, there are some other paramount requirements i.e. interoperability and Quality of service (QoS) are inevitable to facilitate the smart services within IoT ecosystems. Bello and Zeadally (2017) highlighted the different networking standards used for smart services in the IoT application domains and the focus is not on the device rather to communication network capabilities of Network and transport protocols which supports efficient datatraffic management, resource allocation as needed and is essential for delivering smart IoT services. Each layer input/output are complimenting to other layers. This work is aimed at the mechanism off low of data traffic across various technologies and different application domains provisioning QoS for any smart service.

A new paradigm integrating IoT and Social Networks developed as Social Internet of Things (SIoT) in recent past and Lin and Dong (2018) cited comprehensive trust model to address uncertainty and risk for this paradigm which considers different aspects starting from bilateral evaluation of trustworthiness to decision making then subsequent action and result. This

model is a context/characteristic-based model that can detect malicious nodes effectively based on same characteristic of different tasks.

Instead employing services to calculate trust of sensor nodes, Xua et al. (2013) proposed agent based IoT system where agents will be embedded into sensor nodes and ensures collecting, sharing and processing information in IoT environments. Agent based trust model provides automatic trusted hardware execution platform for agents to act on behalf of sensor nodes whichcould manage resources and regulate actions of node in order to maximize the benefit of the whole IoT system. This model with the features of platform independent, flexibility, compatibility, multi-function, easy to upgrade is able to protects both nodes and agents from different types of attacks. Still, detail work procedure, credibility evaluation of mechanism and collaborative management mechanism are yet to be implemented.

Autonomic trust management for IoT cloud ecosystem is proposed by Namal et al. (2016). Less research work has been carried out on cloud based highly dynamic IoT systems till now. As the proposed system is highly dynamic so it needs self-adaptive decision making and autonomic agents to manage the resources and to evaluate the level of trust in an IoT cloud ecosystem. Cloud integration with IoT can give more benefit to real world applications in much more distributed and dynamic environments as it provides trust as a service(TAAS) and exposed the functionality interfaces to the service providers.MAPE-K feedback loop with autonomic agents finds level of trust much more effective than without feedback.

Trust management is not only prime aspect of internet of things, also required for social internet of things which is nothing but a social network of intelligent objects. Kowshalya and Valarmathi (2017) proposed Trust Management scheme for Social Internet of Things which triggers autonomous communication among the smart objects. Trust model here considers couple of parameters such as direct observations, indirect commendation, centrality, energy and service score of intelligent devices part of IoT loop to get the trust score and exhibits better performance than other existing models, but this model is short of addressing all types attacks in IoT paradigm.

3. IoT Layers Structure

Implementation of correct layered design of IoT has significant impact on performance of IoT applications and also, paves way to address the challenges of IoT trust management such as heterogeneity, scalability, identity, trust and governance. The underneath idea here is to establish distinguished IoT layers before proposing our original trust management mechanism (Table 1).

Table 1: IoT Layers

Layer	**Key Components**	**Service Domain**
Business Process Layer	Business Process Models, Business Ecosystems, Price and Cost Model.	Manages overall IoT system activities Build business models, graphs, flow charts Transformation decision making based on "Things", i.e. big data analysis and App.
Application Layer	Reporting, Analytics and Control Models	E-HealthCare, Retail, Military Transportation, Energy Supply Chain Surveillance
Management Service Layer	Data Abstraction, Aggression, Access Models	Device modeling, configuration management, Trust management, security control
Transmission Layer	Zigbee, Bluetooth,GPS,WIFI,GSM,3G/ 4G,Infrared, ,AMQP,DDS	Data Element Analysis and transformation
Network Layer	Wireless LAN, PAN, IPV6/IP Routing, 6LoWPAN, IEEE802.15.4	Communication and Processing Units
Perception Layer	RFID, Wireless Sensors, acutators, Embedded Devices, Machine to machine(M2M)	Wireless Sensor Networks, Acutator network

Detailed study of above prevalent trust models cited in state-of-art are done to identify how the considered models defend IoT system against all kind of malicious attacks and provide reliable data transmission, finally to highlight the open the issues existing in the IoT ecosystem.

4. Open Issues

1. Lack of Lightweight trust mechanism to support RFID devices and heterogeneous platforms.
2. Current state-of-art doesn't address all types of threats in IoT ecosystem may encounter.

3. No robust framework to support network communications to different application domains and ensure implementation of efficient trust mechanism.
4. Identifying IoT threats and no automated course of actions to address these.
5. Subdue research work on the IoT vision of ‘‘anytime, anywhere, anyway, anything” to access
6. No robust autonomic trust management in cloud based dynamic IoT system.
7. Encouragement to develop more distributed trust management framework than the centralized ones.
8. No hybrid trust framework to support closely related IoT networks WSN, Manet, and VANET.
9. Need to figure out the common trust semantics using ontological representations
10. Identify terms and condition to evaluate the trust of trustor on trustee in case of trustworthiness or vulnerability for cross platforms.

5. State-Of-Art Comparison Study

Referred IoT models in review section for establishing trust mechanism are analyzed on different standpoints. This comparison table (Table 2) draws significant pointers on selecting appropriate approach for different criteria and propels the research community to bring enhancements on the model’s pitfalls.

Table 2.Comparison Study of Existing Algorithms

Algorithms	Cross Layer Heterogeneous Support	Threats Addressed	Scalability Support	Type of Trust Models	Interoperability Support	LightWeight Models	Non-repudiation to Data Formats
Ramakrishna et al. (2016)	No	No	Partially	Reputation	No	Yes	No
Gago et al. (2017)	Yes	No	Partially	Subjective	Yes	No	Yes
Mendoza and Kleinschmidt (2015)	No	Partially		Reputation	No		No
Chen et al. (2011)	No	Yes	Partially	Reputation	No	Yes	No

Jing et al. (2014)	Yes	Partially	Yes	Dynamic	No	Yes	Yes
Mahalle et al. (2013)	No	No	Yes	Dynamic	Yes	No	No
Athreya and Tague (2013)	Yes	No	No	Dynamic	Yes	Yes	Yes
Gago et al. (2017)	No	No	No	Dynamic	Yes	Yes	No
Saied et al. (2013)	Yes	Partially	No	Dynamic	No	Yes	Yes
Wu and Li (2017)	Yes	No	No	Subjective	No	No	Yes
Bello and Zeadally (2017)	Yes	No	No	Dynamic	Yes	No	Yes
Lin and Dong (2018)	No	Yes	No	Dynamic	No	Yes	No
Xua et al. (2013)	Yes	No	Yes	Dynamic	No	No	Yes
Namal et al. (2016)	No	Partially	Yes	subjective	No	No	No

6. Conclusion and Future Work

This paper presented here a survey of different current research papers so far considered on trust management analysis of IoT paradigms and later, highlighted open issues, gaps/draw backs of heterogeneous ubiquitous computing world through comparison study. Further efforts are inevitably needed to improve trustworthiness factor as its paramount important to overcome lack of certainty among intelligent devices. Further, this state-of-art provides the insight and understanding on different trust models, services, applications so far used among the things involved for the IoT applications, also encourages to design one novel trust mechanism which calculates the trust value using fuzzy logic on our future research work.

References

1. Sfar, A.R, Natalizio E, Challal Y, Chtourou Z. (2018). A Roadmap for Security Challenges in Internet of Things. Digital Communications and Networks, 4(2), 118-137.
2. Ramakrishna, M.K. (2016). A Framework of Online Social IoT System and Trust Management Scheme. International Journal of Computer Science, 4(2), 827-835.
3. Mendoza, C.V.L, Kleinschmidt, J.H. (2015). Mitigating On-Off Attacks in the Internet of Things Using a Distributed Trust Management Scheme. International Journal of Distributed Sensor Networks, 11:1-8.
4. Chen D, Chang G, Sun D, Li J, Jia J, Wang X. (2011). TRM-IoT: A Trust Management Model Based on Fuzzy Reputation for Internet of Things. Computer Science and Information Systems, 8(4), 1207-1228.
5. Jing Q, Vasilakos A.V, Wan J, Lu J, Qiu D. (2014). Security of the Internet of Things: perspectives and challenges. Wireless Networks, 20, 2481-2501.
6. Mahalle P.N, Prasad N.R, Prasad R. (2013). Novel context-aware clustering with hierarchical addressing (CCHA)for the internet of things (IoT), Fifth International Conference on Advances in Recent Technologies in Communication and Computing (ARTCom 2013)IET Conference, Bangalore, India, 267-274.
7. Athreya A.P, Tague P. (2013).Network Self-Organization in the Internet of Things. IEEE International Workshop of Internet-of-Things Networking and Control (IoT-NC), DOI: 10.1109/IoT-NC.2013.6694050.
8. Gago C.F, Moyano F, Lopez J. (2017). Modelling Trust Dynamics in the Internet of Things. Information Sciences, 396, 72-82.
9. Saied Y.B, Olivereau A, Zeghlache D, Laurent M. (2013).Trust management system design for the Internet of Things: A context-aware and multiservice Approach. Computers & Security Part B, 39, 351-365.
10. Wu X, Li F. (2017). A multi-domain trust management model for supporting RFID applications of IoT. PLoS ONE 12(7), e0181124.
11. Bello O, Zeadally S. Toward efficient smartification of the Internet of Things (IoT) services. Future Generation Computer Systems, doi.org/10.1016/j.future.2017.09.083

12. Lin Z, Dong L. (2018). Clarifying Trust in Social Internet of Things. IEEE Transactions on Knowledge and Data Engineering, 30(2), 234-248.
13. Xua X, Bessisb N, Caoa J. (2013). An Autonomic Agent Trust Model for IoT systems. Procedia Computer Science, 21, 107-113.
14. Namal S, Gamaarachchi H, Lee G.M, Um T.W. (2016). Autonomic Trust Management in Cloud-Based and Highly Dynamic IOT Applications. Journal of International Business Research and Marketing, 1(5), 26-32.
15. Kowshalya A. M, Valarmathi M. L. (2017). Trust Management in the Social Internet of Things. Wireless Personal Communications, 96(2), 2681-2691.

