



Context-aware Approach for Trust-based Services Provisioning in the Internet of Things

A thesis submitted to the faculty of the graduate college in partial fulfilment of the requirement for master degree in computer engineering (embedded systems track)

Muhammad Bassam Obeidat

Advisor: Dr. Hisham Almasaeid

Co-Advisor: Dr. Abdallah Alma'aitah

Yarmouk University

Irbid, Jordan

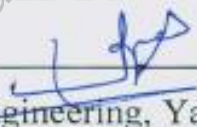
May, 2018


Context-aware Approach for Trust-based Services Provisioning in the Internet of Things

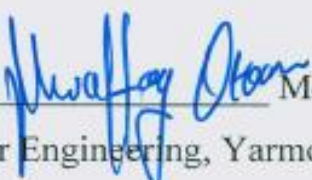
Muhammad Bassam Obeidat


A thesis submitted in partial fulfilment of the requirements for the degree of
Master of Science in the Department of Computer Engineering, Yarmouk
University, Irbid, Jordan

APPROVED BY

Dr. Hisham Almasaeid  Chairman
Assistant Professor, Computer Engineering, Yarmouk University

Dr. Abdallah Alma'aitah  Member
Assistant Professor, Network Engineering & Security, Jordan University of
Science and Technology

Dr. Mwaffaq Otoom,  Member
Associate Professor, Computer Engineering, Yarmouk University

Dr. Muhannad Quwaider,  Member
Associate Professor, Network Engineering & Security, Jordan University of
Science and Technology

May, 2018

ACKNOWLEDGMENT

I would like to thank everybody who tough me, helped me, consulted me, or supported me during the period of achieving this work. In this sense, I want to appreciate my supervisors Dr. Abdallah and Dr. Hisham for their tremendous support and advice in all time of research and planning for our undertaken work.

In addition, I want to acknowledge Dr. Baha” Alsaify who motivated me to choose the Internet of things as the research field of my thesis.

Finally, I would like to express my gratitude to my parents, who have not stopped supporting me throughout my life.

Muhammad Bassam Obeidat

May, 2018

© Arabic Digital Library - Yamouk University

DECLARATION

As a graduate student of the Hijawi Faculty of Engineering Technology at Yarmouk University, I understand what plagiarism is and I am aware of the university's regulations and procedures in this regard. Consequently, I declare that this thesis is my own work and free of any kind of plagiarism.

Muhammad Bassam Obeidat

May, 2018

© Arabic Digital Library-Yarmouk University

TABLE OF CONTENTS

ACKNOWLEDGMENT	2
DECLARATION	4
TABLE OF CONTENTS	5
LIST OF FIGURES.....	7
LIST OF TABLES	8
LIST OF ABBREVIATIONS.....	9
ABSTRACT.....	11
CHAPTER 1: INTRODUCTION	13
1.1 Overview	13
1.1.1 Internet of Things (IoT)	13
1.1.2 Trust management in Internet of Things	16
1.1.3 Fuzzy logic	20
1.2 Motivation and problem definition	21
1.3 Thesis contribution	22
1.4 Scope and objectives	24
1.5 Thesis organization	24
CHAPTER 2: LITERATURE REVIEW	25
2.1 Related work	25
2.2 Summary	31
CHAPTER 3: CATB-IoT TRUST MODEL	32
3.1 Basic architecture and transaction flow	32
3.2 Trust variables.....	36
3.3 Trust factors	38
3.3.1 Social trust for consumer node (ST_c).....	38
3.3.2 Social trust for provider node (ST_p).....	39
3.3.3 Transaction motivation toward service provider (TM_p).....	39
3.3.4 Link quality (LQ)	40
3.3.5 Availability of service provider (AV_p)	40
3.4 Trust calculation.....	41
3.5 Weights adjustment.....	49
CHAPTER 4: EVALUATION AND ANALYSIS.....	50

4.1 Environment setup.....	50
4.2 Evaluation and analysis.....	51
4.3 Case study	57
CHAPTER 5: CONCLUSION AND FUTURE WORK	59
5.1 Conclusion.....	59
5.2 Future work.....	59
REFERENCES	61
ملخص	65

© Arabic Digital Library-Yarmouk University

LIST OF FIGURES

Figure 1: IoT Architecture Layers	16
Figure 2: Fuzzy logic components	21
Figure 3: Architecture of CATB-IoT model	35
Figure 4: Membership function of C	44
Figure 5: Membership function of R	45
Figure 6: Membership function of distance (D)	45
Figure 7: Membership function of provider's availability (AVp)	47
Figure 8: Results of evaluation case 1 ($AV_p=10\%$ after T3 for P1 and P2)	52
Figure 9: Results of evaluation case 1 ($LQ_p=10\%$ after T3 for P1 and P2)	53
Figure 10: Results of evaluation case 2	54
Figure 11: Results of evaluation case 3 (C1 and C2 have good old behavior, & bad recent behavior)	55
Figure 12: Results of evaluation case 3 (C1 and C2 have bad old behavior, & good recent behavior)	56

© Arabic Digital Library - Yamouk University

LIST OF TABLES

Table 1: Trust properties.....	17
Table 2: Summary of reviewed works	30
Table 3: Ranges of provider's capability (C).....	43
Table 4: Ranges of number of instant requests (R)	44
Table 5: Ranges of distance (D).....	44
Table 6: Simulation Parameters.....	51

© Arabic Digital Library-Yarmouk University

LIST OF ABBREVIATIONS

- Auto-ID:** Automatic Identity
- AV:** Availability
- BMA:** Bad Mouthing Attack
- BSA:** Ballot Stuffing Attack
- CATB-IoT:** Context-Aware Trust-Based-Internet of Things
- CATrust:** Context-Aware Trust
- COG:** Center of Gravity
- EPC:** Evolved Packet Core
- ETX:** Expected Transmission Count
- HIP:** Highly Important Person
- ID:** Identity
- IoT:** Internet of Things
- IPV6:** Internet Protocol Version 6
- LQ:** Link Quality
- LTE:** Long Term Evolution
- MIT:** Massachusetts Institute of Technology
- NFC:** Near Field Communication
- OOA:** On-Off Attack
- OSA:** Opportunistic Service Attack
- PCs:** Personal Computers
- PDR:** Packet Delivery Rate
- P2P:** Peer to Peer
- QoS:** Quality of Service
- RFID:** Radio Frequency Identity
- SC:** Service Consumer

SP: Service Provider

SPA: Self Promotion Attack

ST: Social Trust

TF: Trust Factor

TM: Transaction Motivation

TW: Time Weight

VSAT: Very Small Aperture Terminal

WBAN: Wireless Body Area Network

WMA-OWA: Weighted Moving Average-Ordered Weighting Average

WSN: Wireless Sensor Network

© Arabic Digital Library - Yarmouk University

ABSTRACT

Muhammad Bassam Obeidat, Context-aware Approach for Trust-based Services Provisioning in the Internet of Things, Master of Science in Embedded Systems, Department of Computer Engineering, Yarmouk University, 2018, (Advisor: Dr. Hisham Almasaeid)

In the arena of information technology, Internet of Things (IoT) has been leading a significant shift toward seamless interaction between billions of heterogeneous and ubiquitous devices connected over the Internet. Such complicated and pervasive network needs trust management to provide trustworthy relationships, robust decision-making, and reliable collaboration. However, trust in IoT systems is introduced at different levels and perspectives depending on the purpose of the system. Hence, in this work, we introduce trust as a suitability and goodness measure to provision services in IoT paradigm in order to derive robust decisions about potential service-oriented transactions. The main objective of the proposed work is to provide adequate services to eligible service consumers in suitable conditions such that valuable benefits are achieved to the involved IoT entities (service consumer and service provider) and possible risks and undesirable results are avoided. The proposed trust model, named CATB-IoT (Context-Aware-IoT), is context-based and involves multiple factors that are related to service consumer, service provider, and IoT infrastructure. CATB-IoT model presents two main contributions. The first one is considering the social trust of the consumer node in addition to provider node. Whereas, the second contribution is offering recommendation service discovery through which multiple service providers are suggested to provision the requested service. The simulation results show that CATB-IoT offers increased accuracy and improved decision making robustness in estimating the trustworthiness of potential service-oriented IoT transactions.

Moreover, CATB-IoT copes with common trust-related attacks like Bad Mouting Attack (BMA), Ballot Stuffing Attack (BSA), Self-Promoting Attack (SPA), and Opportunistic Service Attack (OSA). The results also show that CATB-IoT provides reliable social trust prediction for both service consumer and service provider by assigning credibility to feedback reports on time basis.

Keywords: IoT, Service-oriented IoT, Trust model, Recommendation service, Decision making, Accuracy, Trust factor, Fuzzy logic, Weight adjustment.

© Arabic Digital Library - Yarmouk University

CHAPTER 1: INTRODUCTION

1.1 Overview

Recently, the concept of IoT has attracted attention due to its valuable contribution to several fields of our life especially social relationships and industry. As per many statistics, the number of connected IoT devices exceeded 20 billion by the end of 2017, and expected to reach 50 billion by 2023, and 125 billion by 2030 [19,20]. However, such pervasive network faces many challenges in terms of security and privacy, trust management, resource limitation, connectivity, standards, and scalability [12,13,15,18]. In this thesis, we focus on the trust management problem for the service-oriented Internet of Things.

1.1.1 Internet of Things (IoT)

In few recent years, IoT has appeared as an advanced internet enabling technology that considers the pervasive deployment of a variety of things connected together ubiquitously and exchanging relevant information to produce innovative services and applications [18]. IoT achieves the convergence of physical world and cyber space resulting in cyber-physical paradigm. Such system model enables humans and systems with numerous embedded computers, sensors, tags, and actuators to inter-communicate. This creates fully smart and automated environments like smart city, smart factories and smart transportation. Hence, some researchers [18] define IoT as “The internet technology that enables things to be connected and communicated anytime, anyplace, with anything and anyone through any communication route/path and any service”.

The evolution of IoT passed gradually through multiple milestones until becoming a trending and prospective Internet technology. Indeed, IoT is a networking platform that connects a wide range of entities together enabling them to exchange essential information. As a result, many glimpses of such platform emerged without explicitly considered as IoT systems. Apparently, the first device connected to the Internet was a toaster that can be controlled remotely, becoming the first IoT device in 1990. In 1998, Mark Weiser made a comparison between virtual reality and ubiquitous computing, resulting in constructing a smart water fountain whose height and flow mimic the price and the volume of stock market respectively [21,22].

In 1999, the Auto-ID Center at MIT in Massachusetts invented the Radio Frequency Identity (RFID) technology that inspired the IoT paradigm by connecting, tracking, and identifying smart objects via attached RFID tags. That event gave birth to the concept of the IoT because significant amount of information on the Internet began to be originated from devices rather than human. Hence, many valuable researches have been published, discussing the remarkable benefits and applications of the Internet of Things. Some of those publications include "When Things Start to Think" by Neil Gershenfeld (1999), "Machine-to-machine technology gears up for growth" by G. Lawton (2004), and "HIP-Tags, a new paradigm for the Internet Of Things" by P. Urien, S. Elrharbi, and D. Nyamy (2008). Also, many IoT-related projects were founded such as LG's Internet refrigerator (2000), Ambient Orb (2002), HP's Cooltown (2003), and Fitbit (2007) [21,22].

Starting from 2008, IoT has been becoming a hot and trending topic in the world of information technology. The number of diverse devices connected to

the Internet had been increasing tremendously ranging from RFID tag, PCs, smart phones, up to airplanes, resulting in about 13 billion devices (exceeds the earth population) in 2010. IPV6 was launched in 2011, letting billions of billions of new devices to join the Internet, hence supporting the IoT. The applications of IoT cover many fields such as self-monitoring healthcare, smart transportation, automated factories, smart buildings, and smart grids. Nowadays, IoT is strongly supported by reasonable number of technologies that combined participate in activating its operations. Such technologies include various Wireless Sensor Network technologies and protocols (like WiFi, Bluetooth, Zigbee, NFC, RFID, Long Term Evolution (LTE), and Very Small Aperture Terminal (VSAT)), machine learning, and embedded systems [22,23].

Conventionally, the architecture of IoT is organized in three layers, named: perception, network and application. Perception layer is responsible for collecting and processing raw data from surrounding environment using different application-based technologies like Wireless Sensor Network (WSN), Wireless Body Area Network (WBAN), RFID and Near Field Communication (NFC). Whereas network layer ensures the network connectivity between the devices of perception layer providing data transmission service using well-known communication protocols. Regarding application layer, it exploits the processing and the analysis of raw data to enable a wide range of intelligent applications in various sectors. Examples of applications include smart vehicle parking (transportation), remote elderly monitoring (healthcare), automated smoke alarm (smart building) and air quality control (smart energy) [12,15,18].

Some researchers and IoT architects add a middleware layer between network layer and application layer [14,18]. This layer acts as an abstraction level between IoT user's application and the rest of IoT architecture such that it copes with the heterogeneity of IoT devices. The key functionalities of the IoT middleware represents performing refinement, analysis, discovery and aggregation on the received information. This might introduce several management and security-related services like trust, reputation, access control, and authentication. Such services make use of meaningful and relevant contextual information to make crucial decisions, and hence providing efficient utilization of device data. Figure 1 summarizes IoT layering stack.

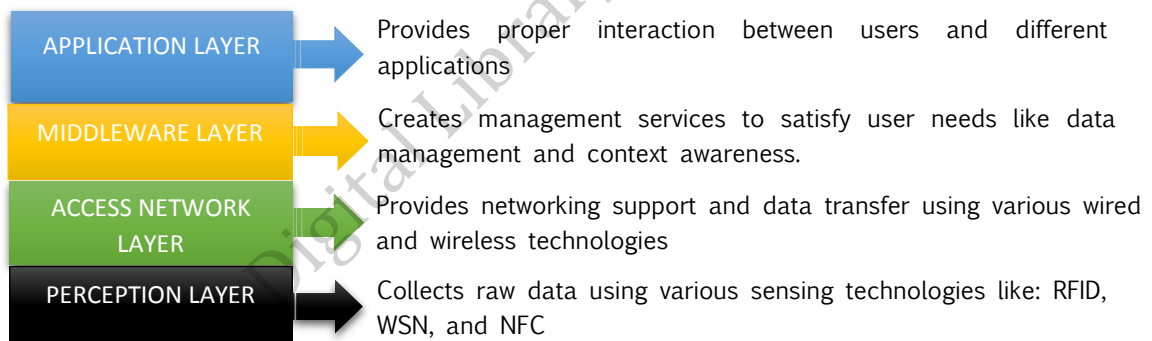


Figure 1: IoT Architecture Layers

1.1.2 Trust management in Internet of Things

The Internet of Things paradigm involves establishing massive communication sessions between diverse and pervasive objects to create innovative ubiquitous services. In such circumstances, significant issues emerge in terms of offering qualified services, collaboration, cooperation, and trustworthy relationships between heterogeneous IoT nodes. Therefore, trust management is essential to address these issues such that it participates in providing trustworthy

relationships, robust decision-making, secure information sharing, reliable service provisioning, and identity trust [12,13,15,23,24,25].

Realizing trust in the IoT is challenging due to its complicated architecture and tremendous diversity. IoT trust does not target security only, in fact, it extends to entity-based characteristics like goodness, reliability, motivation, availability, and robustness [12]. Thus, it is not trivial to define, maintain, and guarantee trust along with security and privacy because it depends on the purpose and the context of using trust. However, many researchers specify the properties that affect trust and hence, used in trust measurement and assessment. These properties are divided into five primary categories which are summarized in Table 1 [12,13].

Table 1: Trust properties

category	Trust properties
Trustee's objective properties	Competence; Ability; Security (confidentiality, integrity, availability); Dependability (reliability, maintainability, usability, safety); Predictability; timeliness; (observed) behaviors; Strength; Privacy preservation.
Trustee's subjective properties	Honesty; Benevolence; Goodness.
Trustor's objective properties	Assessment; a given set of standards; trustor's standards.
Trustor's subjective properties	Confidence; (subjective) expectations or expectancy; subjective probability; willingness; belief; disposition; attitude; feeling; intention; faith; hope; trustor's dependence and reliance.
Context	Situations entailing risk; structural; risk; domain of action; environment (time, place, involved persons), purpose of trust.

Thus, trust management concerns with aggregating relative trust properties that will be used to quantify the target trust value accordingly. Existing trust-based service provisioning models for IoT systems in the literature are discussed and analyzed in terms of certain design criteria. In this sense, [12,13] mention five design criteria:

(1) Trust composition: considers the trust components or properties that are used in trust computation. These components are divided into two primary categories:

- a) Quality of Service (QoS) trust properties: which covers a wide range of attributes that measure the performance of involved IoT-related infrastructure so as to provide quality service in response to service requests. Energy consumption, packet delivery ratio, and computational power are examples of QoS trust properties.
- b) Social trust properties: which covers a wide range of attributes that are associated to social relationships between the owners of connected IoT devices. Community of Interest, centrality, and honesty are examples of social trust properties.

(2) Trust propagation: considers the method by which trust information is disseminated among different IoT devices. Two main methods are adopted:

- a) Distributed propagation: in which every IoT device forwards its observations to other devices autonomously in the absence of any centralized entity. This happens usually in WSN and Mobile Ad-Hoc Networks (MANET).
- b) Centralized propagation: in which a trusted third-party entity is responsible for forwarding trust information in response of incoming requests. The centralized entity may be a physical cloud system or a

virtual trust system implemented in some IoT nodes that stores huge amount of trust information of adjacent IoT nodes.

(3) Trust update: considers the time when trust value is updated. Two main methods are adopted:

- a) Time-driven update: trust information is collected in periodic manner, then trust value is computed accordingly.
- b) Event-driven update: trust information is collected after a certain event like updating self-observed information, or sending a recommendation report by the end of successful trading.

(4) Trust formation: considers how many trust properties are being used to form the overall trust value. Two primary formation methods are adopted:

- a) Single-trust formation: trust computation evaluates only one trust property to form the overall trust value.
- b) Multi-trust formation: trust computation evaluates multiple trust properties to form the overall trust value.

(5) Trust aggregation: considers the adopted technique used in aggregating collected trust properties to evaluate the overall trust value. In this sense, several aggregation methods are used depending on the application and the nature of involved trust properties. Some of most used aggregation methods include weighted sum, regression analysis, fuzzy logic, and Bayesian inference.

Finally, from IoT perspective, trust management is used to satisfy a set of requirements according to [12,24,25]. These requirements are:

- (1) **Data perception:** it ensures data-based trust such as data integrity, data reliability, data collection and data persistency.
- (2) **Trust relationship and decision:** it ensures establishing relationships with only trusted entities, resulting in effective collaboration and well-advised decisions.
- (3) **Privacy preservation:** it ensures protecting user data from being violated.
- (4) **Data fusion and mining:** it ensures inspecting useful data to perform required processing and analysis.
- (5) **Secure data transmission:** it ensures that unauthorized entities cannot access data during communication sessions between involved entities.
- (6) **Quality of IoT Service:** it ensures services are presented only to authorized entities at proper conditions.
- (7) **Security and robustness:** it ensures defeating security threats and possible risks.
- (8) **Generality:** it ensures shared information and services to be deployed broadly.
- (9) **Scalability:** it ensures that the integrating more services and entities will not degrade the overall performance of service-oriented paradigm.
- (10) **Identity management:** it ensures that all integrated entities are identified and trustworthy.

1.1.3 Fuzzy logic

Fuzzy logic is a mathematical model that was introduced by Lotfi Zadeh in 1965. This probabilistic model makes certainty about vague input variables whose values are any values between truth 0 and truth 1 unlike binary logic.

Fuzzy logic concerns with reasoning algorithms to imitate human thinking in dealing with vague and uncertain data used to make decisions.

The fuzzy logic system involves four components to convert the input data into final output as shown in Figure 3 [17]. The fuzzifier takes crisp inputs and converts them into fuzzy input set using pre-defined linguistic variable and proper membership function. Then, fuzzy input is used to obtain fuzzy output by evaluating the programmed rules at the inference engine. Finally, the crisp output is computed using proper de-fuzzification function and the membership function of the output variable at the de-fuzzifier phase [17]. Membership functions takes different shapes such as trapezoidal, triangular, non-linear (bill shaped), and singleton. The common de-fuzzification functions include max-membership, center of gravity, weighted average, and mean-max.

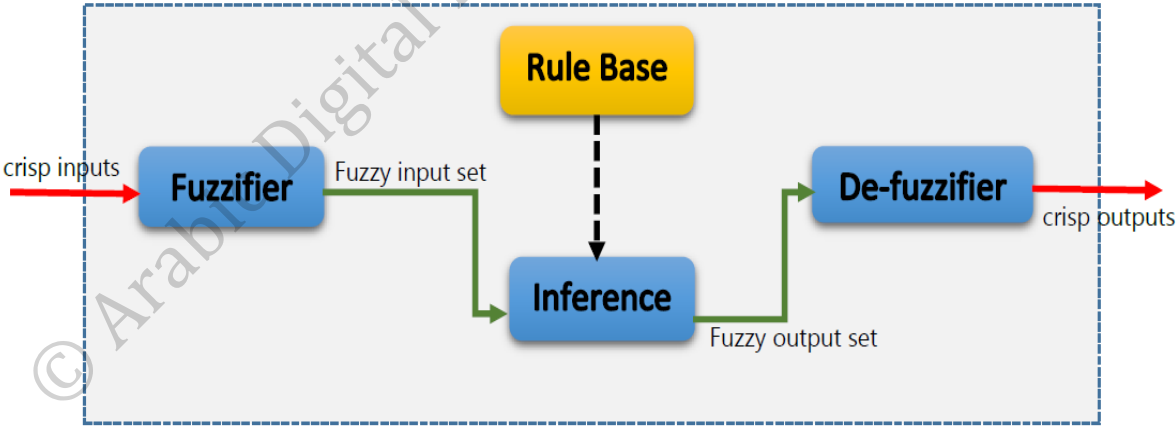


Figure 2: Fuzzy logic components

1.2 Motivation and problem definition

In service-oriented IoT systems, provisioning services and accessing information between heterogeneous IoT devices introduces certain trust-related concerns affecting the collaboration between these devices

[3,12,13,15]. Particularly, the suitability of intended transactions between service consumer's device and service provider's device must be predicted in advance to achieve the goals of that transactions and avoid undesirable events. Usually, this suitability is strongly associated with the dynamic changes in context such that the current situation of service provider, service consumer, and IoT infrastructure combined participate in setting up the appropriate trust level of the intended service-based communication. In this sense, trust management is necessary to estimate how suitable to go ahead in potential transaction between service provider and service consumer [15,16,18]. Hence, the trustworthiness is exploited to anticipate the convenience of potential transactions in attaining benefits and preventing risks. However, figuring out the essential factors (trust metrics) that influence the involved trust is crucial issue, especially when such factors are dominant in trust calculation [12].

Consequently, it is required to implement an efficient trust management system that builds trustworthiness between the two involved entities based on essential trust factors (trust context) such that it ensures that the optimized service, under optimized context, is delivered to qualified service consumer.

1.3 Thesis contribution

This work proposes a multi-factor trust-based service model, named CATB-IoT, that takes into account both historical behavior information and real-time information to establish a trust level. The computed trust is used to provide proper decision on carrying out potential service-oriented communication sessions between involved IoT nodes. Indeed, the target trust level implies two separate but complementary trust sub-levels: the trust level of the consumer

node, and the trust level of the provider node. That is, the aim is to calculate trust as a degree of the suitability and goodness of the essential IoT components based on essential trust factors in such a way the service provider accordingly provides adequate services to eligible service consumer in suitable conditions with low possibility of risks.

CATB-IoT model incorporates five factors which constitute the context we concern with to quantify the target trust level. These factors include ¹social trust of the service consumer, ²social trust of the service provider, ³link quality, ⁴provider's availability, and the ⁵popularity of the service provider. The first factor is used to measure the trust level of the service consumer and will be delivered to the potential providers. Whereas, the last four factors are aggregated using dynamic weighted sum to form the trust level of the potential service provider and will be delivered to the service consumer. Moreover, the weights used in quantifying the trust level of service provider are calculated and assigned by considering the amount of variation of newly calculated values for each trust factor across all available candidate provider nodes that could provide the requested service.

The proposed model adopts centralized approach to calculate the target trust levels by utilizing trusted third-party trust management system that accepts trust queries. Also, with the help of centralized service management system, the model presents a recommendation service by suggesting the nearest service providers that could offer the requested service, letting the service consumer to select the most suitable provider in that given context.

1.4 Scope and objectives

This thesis investigates introducing trust as a measure of the suitability and goodness of the essential IoT components to provision services in the service-oriented IoT paradigm. In this sense, the undertaken work proposes a context-aware trust service model that integrates historical information that measures long-term behavior of involved entities (consumer and provider) with real-time information that measures short-term behavior of involved IoT entities to estimate trustworthiness that derives the decision about potential service-oriented transactions in the IoT environment. The main objective of the proposed model is to achieve valuable benefits for the involved entities and avoid possible risks and undesirable results. Ultimately, we aim at providing reliable and robust decision making regarding offering adequate services and to qualified consumers in suitable conditions. That is, only transactions with high trustworthiness will be made.

1.5 Thesis organization

The undertaken thesis is organized as the following:

Chapter 2: covers the most related works in the literature.

Chapter 3: demonstrates the proposed trust model in details including the architecture, trust factors, and trust calculation.

Chapter 4: presents the results, evaluates the performance, and discusses a case study.

Chapter 5: concludes the thesis and suggests some future directions.

CHAPTER 2: LITERATURE REVIEW

2.1 Related work

Over the last few years, there was a growing interest in establishing trust for the Internet of Things systems and how IoT trust was exploited to provision services accordingly. In this chapter, we made a quick review of the literature on trustworthy IoT. The aim was to recognize adopted approaches in establishing trust, figure out involved trust models, and ultimately identify important research gaps and directions that helped discover the novelty of our undertaken work by contrasting our approach with existing work.

Several authors investigated subjective and objective trust models to evaluate the trustworthiness between IoT nodes. In [1], the authors proposed a trust-based service model that involves three trust metrics: reputation, recommendation, and knowledge to calculate trustworthiness of IoT entities. While In [2], the authors offered a reliable trust model based on various subjective factors like feedback, credibility, number and importance of in-between transactions, and the type of relationship between trustee and trustor that reflects the behavior of IoT nodes.

In [3], the authors presented a distributed trust management technique that considers both direct trust and indirect trust. While the direct trust value is inferred from direct user satisfaction experiences toward trustee node, the indirect trust value is computed by combining three social similarity metrics of the trustee node: friendship, social contact, and community of interest.

In [4], the authors propose a distributed trust and reputation model in which trust is calculated by combining both the direct trust and indirect trust provided by other neighbor nodes. The direct trust is measured by aggregating both uncertainty, and experience toward trustee that is computed using three performance metrics: end-to-end packet forwarding ratio (EPFR), energy consumption (AEC), and packet delivery ratio (PDR). The main addition of [4] is that it enables requesting nodes to select the most trustworthy path toward the service provider, consisting of only good nodes.

In [5], the authors argued the concept of trustworthiness management for the social IoT paradigm by providing two independent models (subjective and objective). Both models rely on feedback messages collected from nodes after each successful transaction. The feedbacks of all nodes are stored in the form of Dynamic Hash Table (DHT) located at centralized node and weighted by the credibility and the relevance of the involved transactions between the trustee and all nodes. The proposed models defeat the trust-related attacks at the expense of the increased network traffic that relates to huge amount of feedback propagations and queries.

The major drawback of the above trust models is that it aggregate subjective and/or objective properties of both the trustee and the trustor to evaluate the trustworthiness without any consideration to the context environment. Relatively, relying on such trust models might introduce undesirable trust biasing, uncertainty, risks, and inaccurate trust computations. Hence, integrating context into trust computation would overcome above challenges and enhance overall performance of the trust model.

In this sense, some efficient works in the literature argued trust computation based on context. In [6], the authors presented a context-based trust management system offering multiple services for a range of heterogeneous IoT nodes. The proposed system uses a central trust manager to receive and response to service requests. The trust manager adaptively filters the selected candidates based on specific contextual information related mainly to current capabilities and the type of service of the assisting candidates. Accordingly, the trust manager calculates the trust value for the most related candidates and sends them to the consumer. Hence, the consumer communicates with the selected assisting node(s) and provides an evaluation feedback to the trust manager stating the quality of service received.

In [7], the authors proposed a novel trust service model which assesses the trustworthiness of the service quality provided by the service provider based on the service behavior patterns of the service provider in response to changes in essential operational and environmental contextual information like channel status, node status, service payoff, and social disposition. The overall service trust value of the service provider relies on both direct self-observation and indirect recommendations of other nodes at given context over a period of time.

In [8], the authors presented an adaptive trust management model that concerns with social disposition and transaction context to evaluate the trustworthiness between IoT nodes such that it involves both social trust and context trust. The model concerns with direct and indirect transactions occurred in specific context so as to improve the robustness and the reliability of the calculated trustworthiness. Moreover, the accuracy of the proposed model offers trust assessments which are close to the trustee node's status.

In [9], the authors proposed a centralized context-based trust measurement model that dynamically assigns trustworthiness levels to candidate service providers. The proposed model depends on service server to determine the candidate nodes that provide the requested service, whereas an authorized trust management server is responsible for calculating the trust level of each candidate using the context-based feedback information sent by service consumers at the end of each service trading. The trust calculation adopts decision tree (built through learning process) to select the most trustworthy candidates. Then the social similarity between the service consumer and every elected candidate is used to compute the credibility of them. Finally, the most trustworthy provider will be the one with the highest trust level.

In [10], the authors introduced a novel fully distributed context-aware trust model that relies on automatic location-based recommendations to discover the nearby interested service providers. The consumer exploits the contextual information in the feedback messages that sent by interested providers to firstly derive weights and secondly calculate the trust values for all interested providers. The trust value is weighted by the number of feedback messages, consumer's preferences weight (uses preference value), time weight (uses feedback time stamp), and the service context weight (uses price and type of the service). Finally, the consumer chooses the provider from all available interested providers based on their trustworthiness values. The main disadvantage of this work is it involves an extreme computational overhead on the resource-constrained consumer node.

In [11], the authors propose a multi-factor trust management system for Peer to Peer (P2P) paradigm. The involved trust computations incorporate five

factors to produce a trust value that will be mapped to equivalent service level. Four factors reflect behavioral information like historical self-experience, reputation, risk possibility, and motivation toward the provider. Whereas, the fifth factor measures the real-time availability of the provider. The weights of trust factors are calculated dynamically using Weighted Moving Average-Ordered Weighting Average (WMA-OWA) algorithm that adaptively assigns suitable weights based on the change in trust factors.

Table 2 below summarizes all reviewed work with regard to the adopted trust computation approach, design dimensions of the trust model, defended attacks, performance measurements, and trustee node.

© Arabic Digital Library - Yamouk University

Table 2: Summary of reviewed works

Reviewed works	Approach used to calculate trust	Design dimensions of the adopted trust model					Defended attacks	Performance measurements	Trustee node
		Trust composition	Trust update	Trust propagation	Trust Formation	Trust aggregation			
Truong et al. [1]	Subjective	Social Trust	Event-driven + Time-driven	Semi-distributed	Single-trust	Dynamic Weighted Sum + Fuzzy Logic	SPA, BMA, BSA, OSA	Resiliency	Service provider
Nitti et al. [2]	Subjective	Social Trust	Event-driven	Distributed	Single-trust	Static Weighted Sum	Collusive attacks	Low error percentage	Service provider
Chen et al. [3]	Subjective	Social Trust + QoS Trust	Event-driven + Time-driven	Distributed	Multi-trust	Dynamic Weighted Sum + Bayesian Inference	SPA, BMA, BSA	Adaptability + Scalability + Resiliency	Service provider
Chen et al. [4]	Subjective + Objective	QoS Trust	Time-driven	Distributed	Single-trust	Static Weighted Sum + Fuzzy Logic	SPA	NA	Service provider
Nitti et al. [5]	Subjective + Objective	Social Trust + QoS Trust	Event-driven	Distributed + Centralized	Multi-trust	Static Weighted Sum	BMA, SPA, BSA, OSA	Adaptability + Scalability + Resiliency	Service provider
Ben Saied et al. [6]	Subjective + Context	QoS Trust	Event-driven	Centralized	Single-trust	Dynamic Weighted Sum	OOA, Selective Behavior, BMA	Adaptability	Service provider
Wang et al. [7]	Subjective + Context	Social Trust + QoS Trust	Event-driven	Distributed	Multi-trust	Regression Analysis	BSA, BMA, Random Attack, Conflicting Behavior Attack	Adaptability + Resiliency	Service provider
Rafey et al. [8]	Subjective + Context	QoS trust + Social Trust	Event-driven	Distributed	Multi-trust	Static Weighted Sum	Malevolent Attacks	Scalability + Adaptability	Service provider
Ben Abderrahim et al. [9]	Subjective + Context	QoS trust + Social Trust	Event-driven	Centralized	Multi-trust	Jaccard Similarity Coefficient + Dirichlet distribution	Misbehaving attacks	Reliable decision making + Scalability	Service provider
Liu et al. [10]	Subjective + Context	QoS trust + Social Trust	Event-driven	Distributed	Multi-trust	Weighted product	Collusion attack, value imbalance attack	High successful trading rate with honest providers	Service provider
Li et al. [11]	Subjective + Context	QoS trust + Social Trust	Event-driven	Distributed + Centralized	Multi-trust	Dynamic weighted sum	Malicious network behavior	accurate and realistic + Adaptability	Service requester

2.2 Summary

Hence, as shown in above literature, none of the existing works considers evaluating trustworthiness toward the service consumer in addition to service provider. Moreover, no dedicated research has been conducted with full attention to essential social and operational contextual information that is related to IoT infrastructure, consumer device, and provider device. More importantly, no concrete work investigates context-based multiple-dimensional trust as a measure of suitability and convenience level of the upcoming service-oriented transactions in the Internet of Things environment. Consequently, the contribution of our work could be summarized as follows:

- (1) Presenting a reliable behavioral trust evaluation for the IoT consumer node and the IoT provider node by assigning credibility to feedback reports on time basis.
- (2) Introducing trust as a measure of the suitability and goodness of essential IoT components (service consumer, service providers, and IoT infrastructure) in a given context to provision services in the service-oriented IoT paradigm.
- (3) Our model is adaptive because it integrates contextual information into trust computation such that adequate service is offered to qualified consumer node in suitable conditions based on real-time information like end-to-end link quality, number of requesting nodes, node capabilities, time, and service type besides the social trust information.
- (4) Our model introduces an implicit service recommendation feature through which the centralized service management discovers all nearest IoT nodes that could provide the requested service.

CHAPTER 3: CATB-IoT TRUST MODEL

In this chapter, we will demonstrate the proposed trust service model in details showing design dimensions, basic architecture, involved trust factors, trust calculation, and weight adjustment mechanism.

3.1 Basic architecture and transaction flow

CATB-IoT model adopts centralized approach in calculating trust, and relies on authorized third-party entities to cope with the tasks of service discovery and trust computation. Consequently, the model consists of the following components:

- (1) **Service consumer:** represents the IoT node that initiates the whole transactions by requesting a service. Usually, the consumer node implies a smart device owned by human being and assumed to be movable.
- (2) **Service provider:** represents the IoT node that provisions the requested service to service consumer. Likewise, the provider node implies a smart device owned by human being and assumed to be movable.
- (3) **Service management system:** represents an authorized third-party node that is responsible for receiving and answering service requests within its coverage. Also, it provides recommendation service by locating all nearest candidate IoT nodes that could provide the requested service.
- (4) **Trust management system:** represents an authorized third-party node that accepts trust queries from the service management system and calculates

the context-based trust values in response. This system is responsible for gathering all required information used in involved computations.

As a prerequisite, every service provider must register its services with a centralized service management system that will receive the service discovery queries from service consumers. Also, upon joining the network, every service consumer must authenticate the centralized service management system in order to help locate all the nearest candidate nodes which can provide the requested service.

The transaction flow related to service requesting/serving involves the following events:

- (1) Initially, the service consumer (SC_i) sends a service discovery query to the service management system, requesting a specific service.
- (2) The service management system locates all nearest candidate nodes that could provide the requested service. This introduces an implicit service recommendation service.
- (3) The service management system then sends trust calculation queries to the trust management system, requesting trust values for the candidate providers and the service consumer.
- (4) The trust management system collects the required information so as to calculate the requested trust values. After that, it sends the trust values back to the service management system.

- (5) The service management system notifies the service consumer of the candidate provider (SP_j) that has the highest trust value.
- (6) The service management system sends the trust value of the service consumer to candidate provider that has the highest trust value.
- (7) The service consumer initiates a communication session with the selected candidate provider.
- (8) If the trust value of the service consumer exceeds the pre-defined threshold set by the selected candidate provider, the selected provider accepts the communication session and go ahead in providing the requested service to the consumer.
- (9) After successful communication session, the consumer sends a feedback report to the trust management system to rate the quality of received service. The feedback report contains provider ID, time of service, service ID, and evaluation score in the range [0,1].
- (10) After successful communication session, the provider sends a feedback report to the trust management system to evaluate the behavior of the consumer. The feedback report contains consumer ID, time of service, and evaluation score in the range [0,1].

The figure 2 below summarizes the transaction flow of the proposed model.

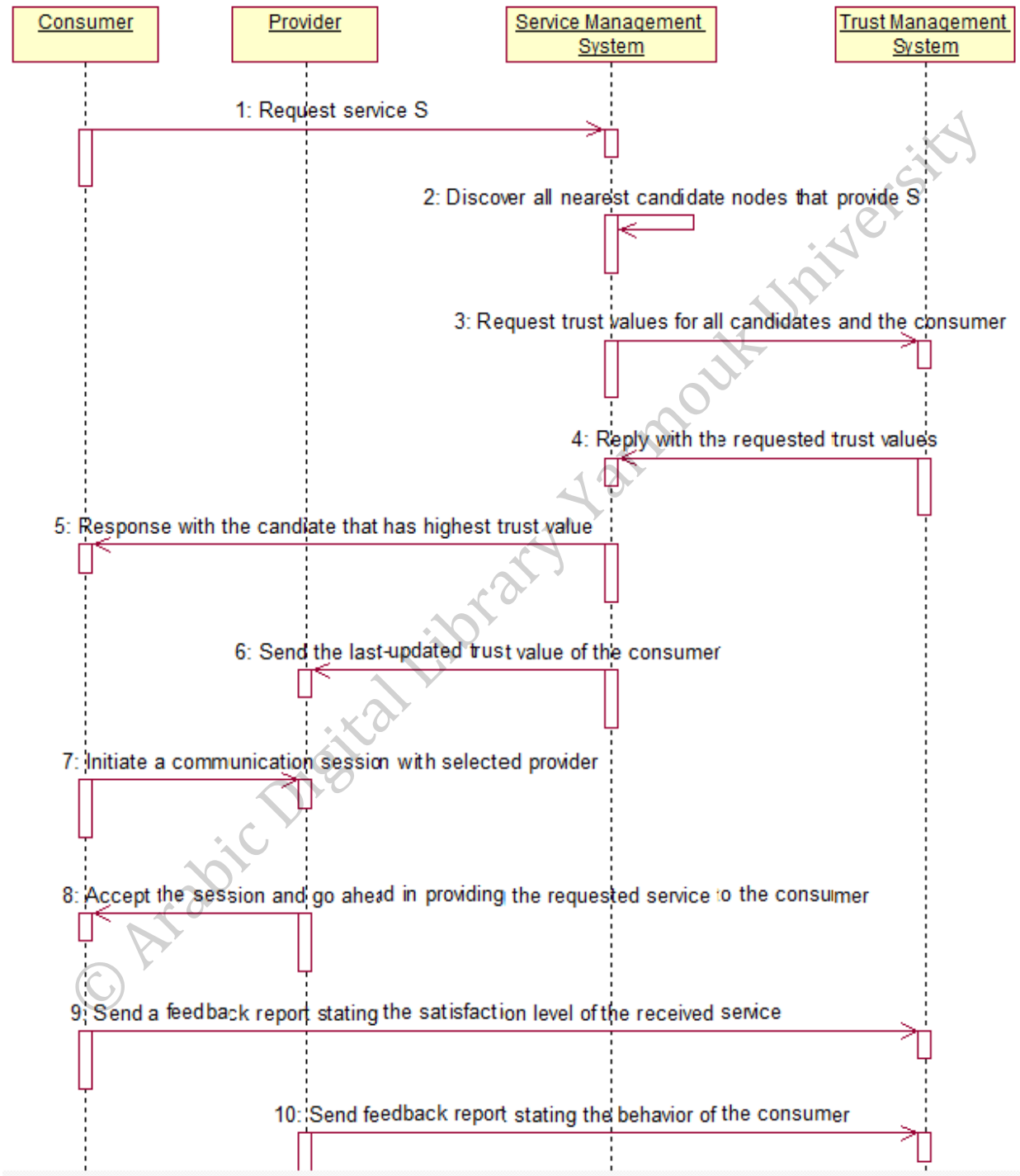


Figure 3: Architecture of CATB-IoT model

3.2 Trust variables

As mentioned in section 1.1.2, the trust is influenced by a range of properties that are associated with trustor, trustee, and the current context. Hence, in this section we investigate the variables that are strongly related to our trust computational model. In this sense, we are interested in capturing the essential information that participates in building robust decision making regarding offering adequate services and information access to qualified (trusted) consumers in suitable conditions. Generally, the trust computation for CATB-IoT model relies on both historical behavior information and real-time information to add a layer of stability to the calculated trust values. With respect to historical information, we are concerned with the following:

- (1) **Direct experience with a potential node:** represents the past evaluations of both the potential provider and consumer toward each other.
- (2) **Indirect recommendation about potential node:** represents the past evaluations of other nodes toward both potential provider and consumer.
- (3) **Transaction volume:** measures the popularity of the provider node in the society over time.
- (4) **Transaction successful rate:** measures the risk possibility associated with undertaken communication.

On the other hand, with respect to the real-time information, we concern with the following:

- (1) **Time:** the timestamps of feedback reports are used in weighting them such that more recent reports are more valid than older ones.

(2) **Provider's capability:** measures how much resources the provider has to accommodate incoming requests including computational power, storage capacity, networking, and energy etc.

(3) **Instantaneous number of requests:** measures how much the potential provider is serving consumers at this time.

(4) **Service type:** is used in filtering both service providers in service recommendation phase, and feedback reports when calculating social reputation for the candidate providers.

(5) **Packet Delivery Rate:** measures the current status of the path to the potential provider. This information is essential in determining the reliability of the route toward the potential provider.

As a result, we can summarize the design dimensions of CATB-IoT model as follows:

- **Trust composition:** the model uses both QoS trust properties and social trust properties in trust computation.
- **Trust update:** the model is event-driven as it may update relevant trust information after successful communication between a consumer and a provider. Accordingly, social reputation of both nodes, successful rate, and transaction volume are updated.
- **Trust propagation:** the model adopts centralized approach through which third-party entities are used to receive and answer service discovery queries and trust calculation queries.
- **Trust formation:** the model uses multi-trust formation because it aggregates both QoS trust properties and social trust properties.
- **Trust aggregation:** the model uses both dynamic weighted sum and fuzzy logic to aggregate the overall trust value.

3.3 Trust factors

As we mentioned previously in section 1.3, CATB-IoT model uses five factors to reflect the complexity of the involved trust for such large-scale pervasive IoT network. These factors cover the social behavior trust of both service consumer and service provider, the current status of in-between link, popularity of the service provider, and the availability of the service provider. The involved trust computations ultimately set up two separate but complementary trust sub-levels to measure the trustworthiness of the service consumer and the candidate providers including IoT infrastructure. Therefore, in this section we demonstrate what properties each factor considers and how each factor affects the trustworthiness in the case of provisioning services in IoT systems.

3.3.1 Social trust for consumer node (ST_c)

As known, self-observations and reputation are important trust metrics used widely in trust assessment in social environment [3,5,26]. As a result, one of the additions our work present is considering the social disposition toward consumer node. Normally, the behavior of the owner of consumer node affects deeply building trust with the provider node since it could misbehave and collude with malicious nodes to perform attacks [11].

In this work, we form the social trust of consumer node by aggregating long-term behavior of the potential consumer node which includes the direct experience with the potential provider node besides the indirect recommendations coming from other IoT provider nodes who have past interaction with the potential consumer node. Moreover, this trust factor assigns time-based importance to every feedback report such that old reports

have a small impact on the overall factor value than recent ones. However, more weight is given to direct experience than indirect recommendation to reduce the effect of malicious and collusive behaviors.

3.3.2 Social trust for provider node (ST_p)

Without doubt, the level of the service quality offered by the service provider over time plays an important role in building trust in service-oriented paradigm because it relates to the satisfaction of the potential consumers [13,25,26].

Like the social trust of the consumer, we form the social trust of the provider node by aggregating long-term behavior of the potential provider node which includes the direct experience with the potential consumer node besides the indirect recommendations coming from other IoT consumer nodes who received the requested service from the potential provider node. Like ST_c , this trust factor assigns time-based importance to every feedback report such that old reports have a small impact on the overall factor value than recent ones.

Also, we will give more weight to direct experience than indirect recommendation to reduce malicious and collusive attacks.

3.3.3 Transaction motivation toward service provider (TM_p)

In such service-oriented environment, it is so important to consider the transaction trend (popularity) toward the potential service providers as an encouraging factor in trust assessment. Thus, the provider who provided successfully the requested service to so many consumers is most likely to be selected in potential transactions. Therefore, the more popular the service provider, the higher the provider's trust level will be.

In this work, we form the motivation factor based on both transaction volume and transaction successful rate properties.

3.3.4 Link quality (LQ)

Determining the quality of the channel that connects the consumer and the potential provider is a critical issue in evaluating the involved trust since it acts as indication about possible congestion, packet loss, throughput, and end-to-end delay [27]. As a result, the better the link quality, the higher the provider's trust value will be.

In this work, we form link quality factor by considering the packet delivery rate property over the communication link in both directions. As a result, we use the expected transmission count (ETX) metric to measure the packet delivery rate in both directions.

3.3.5 Availability of service provider (AV_p)

From the perspective of the service provider, service behavior depends mainly on its current situation so as to fulfill the service requirements [6,8]. Hence, this factor measures the short-term behavior of the provider node that determines how ready the provider is to serve the upcoming requests without the possibility of disconnection. As a result, the more available the service provider, the higher the provider's trust value will be.

In this work, we form the availability of the service provider by considering the current capability of the provider node (computational power, storage, network resources, energy, etc.), the instantaneous number of incoming requests, and the distance between the consumer and the potential provider.

3.4 Trust calculation

After realizing the involved trust factors, we are to demonstrate the computational approach of CATB-IoT model in order to obtain the target trust values to reflect the goodness and convenience level between the consumer and provider nodes.

With regard to trust level of the provider node, we adopt dynamic weighted sum to calculate the trust value TL_j of every potential provider node SP_j . This aggregation method helps in obtaining a measure or interpretation of multiple relative quantitative data that are weighted based on their importance. TL_j is calculated according to the following equation:

$$TL_j = w_1 \cdot ST_p + w_2 \cdot TM_p + w_3 \cdot AV_p + w_4 \cdot LQ, \sum_{i=1}^4 w_i = 1 \quad (1)$$

Starting with the social trust for the provider node ST_p , we concern with the weighted average value of all past evaluations sent by the service consumer node SC_i , evaluating the service quality provided by SP_j besides the weighted average value of all past recommendations coming from different consumers who received the requested service from SP_j . The following equation calculates the overall value of the social trust for the provider node SP_j :

$$ST_p = \alpha_1 \left[\frac{\sum_{l=1}^m TW_l \cdot DScore_l}{m} \right] + \beta_1 \left[NW_c \cdot \frac{\sum_{k=1}^n TW_k \cdot RScore_k}{n} \right], 0 \leq ST_p \leq 1 \text{ \& } \alpha_1 + \beta_1 = 1 \quad (2)$$

Where α_1 is the direct experience weight, and β_1 is the indirect recommendation weight. $DScore_l$ indicates the l^{th} value of direct evaluation score sent by SC_i , and $RScore_k$ indicates the evaluation score value sent by the k^{th} recommender. Also, TW_k and TW_l are time-based weights used to weight

the impact of each evaluation score based on its time-stamp such that recent ones have more impact. The time-based weights are formulated using the following piecewise function that is used in [10]:

$$TW = \begin{cases} 0, & \text{if } Eva_{age} > \psi \\ e^{-(Eva_{age}/\gamma)}, & \text{otherwise} \end{cases} \quad (3)$$

Where ψ represents the time window that specifies the validity of the feedback report, γ is a time constant that specifies the speed of time decay, and Eva_{age} is the difference between the current time-stamp and the time-stamp of the evaluation (direct experience or indirect recommendation). [10]

NW_c represents the number weight used to measure the credibility of the recommendations such that they will be considered only if the number of recommendations exceeds a pre-defined system threshold N_{thr1} , hence, $NW_c=1$ if $n > N_{thr1}$, otherwise $NW_c=0$.

The transaction motivation factor TM_p is calculated by finding the weighted sum of two elements. The first element represents the number of times SP_j has been selected for the requested service. The second element represents the successful rate of transactions made with SP_j . The following equation captures the two elements:

$$TM_p = \alpha_2 \frac{N_{xj}}{N_x} + \beta_2 \frac{N_{succ}}{N_{tot}}, \quad 0 \leq TM_p \leq 1 \ \& \ \alpha_2 + \beta_2 = 1 \quad (4)$$

- α_2 is transaction volume weight, and β_2 is transaction successfulness weight.
- N_{xj} is the number of times SP_j has been selected to provide the requested service.
- N_x is the total number of times all providers including SP_j has been selected to provide the requested service.
- N_{succ} is number of successful transactions with SP_j
- N_{tot} is the total number of transactions with SP_j

We calculate the availability factor AV_p using fuzzy logic due to its flexibility to integrate multiple irrelevant vague components that have different scales to produce one accurate crisp output value. In our work, fuzzy-based approach helps determine the certainty about the current situation of the provider node based on its current capability (C), instant requesting rate (R), and the current distance between the provider node and the consumer node (D) so as to judge the availability of the provider.

First of all, we divide the possible values of each input into membership classes in form of linguistic variables as shown in following tables:

Table 3: Ranges of provider's capability (C)

Linguistic variable	Assigned values
Low	0-0.4
Average	0.2-0.7
High	0.6-1.0

Table 4: Ranges of number of instant requests (R)

Linguistic variable	Assigned values
Low	0-110
High	80-200

Table 5: Ranges of distance (D)

Linguistic variable	Assigned values
Near	0-250
Far	200-500

It is worth mentioning that the value ranges above vary depending on the application and system requirements. The membership functions of the three input variables are plotted using the values in the above tables and following trapezoidal curve. Then we obtain the fuzzy input sets (membership degrees) of the three inputs by finding the value of the membership functions at the current values of the inputs. Figure 4 shows the membership function (FUZ_C) for provider's capability C.

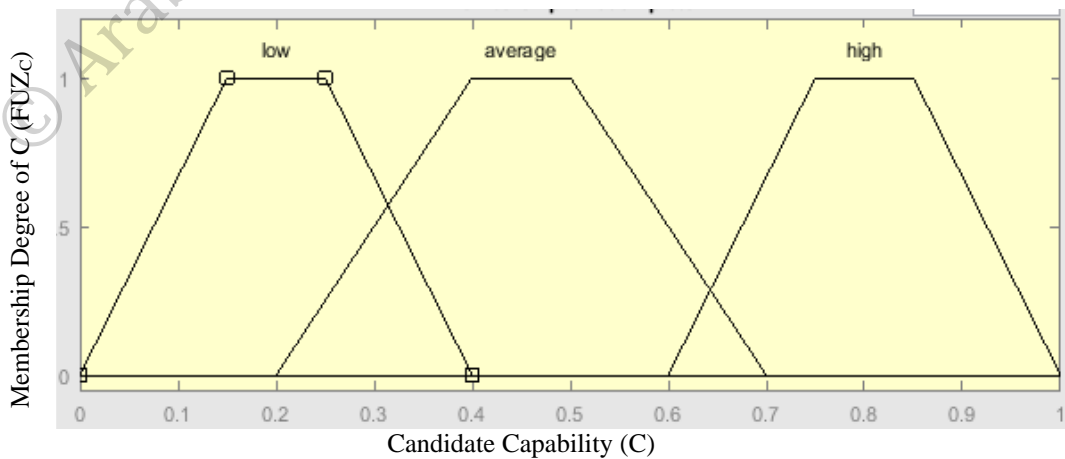


Figure 4: Membership function of C

Figure 5 shows the membership function (FUZ_R) for the number of instantaneous requests R . Figure 6 shows the membership function (FUZ_D) for the distance between consumer and provider D .

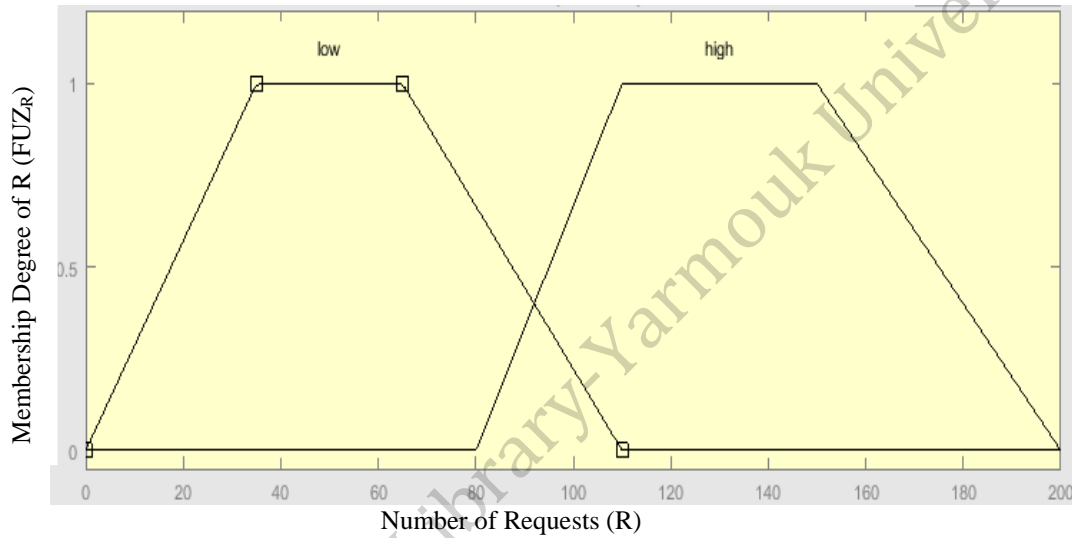


Figure 5: Membership function of R

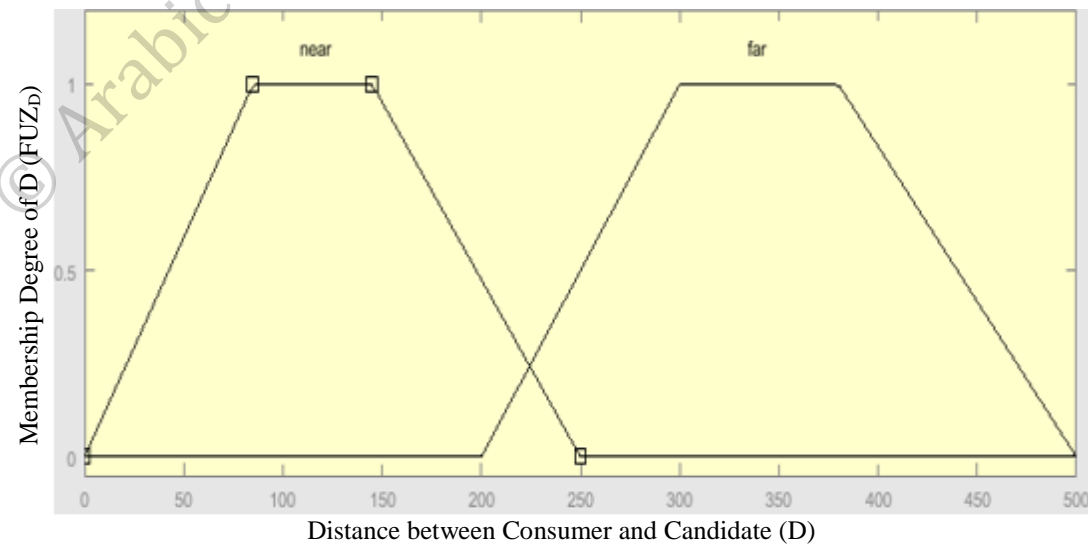


Figure 6: Membership function of distance (D)

The next step is to produce fuzzy output set by applying the fuzzy rules on fuzzy input set. These rules provide reasoning process in form of a series of IF...THEN statements that decide actions based on the fuzzified inputs [17]. The rule base of CATB-IoT model contains the following reasoning rules:

IF C is low AND R is low AND D is near THEN

AV_p is medium

IF C is low AND R is low AND D is far THEN

AV_p is low

IF C is low AND R is high AND D is near THEN

AV_p is low

IF C is low AND R is high AND D is far THEN

AV_p is low

IF C is medium AND R is low AND D is near THEN

AV_p is medium

IF C is medium AND R is low AND D is far THEN

AV_p is medium

IF C is medium AND R is high AND D is near THEN

AV_p is medium

IF C is medium AND R is high AND D is far THEN

AV_p is low

IF C is high AND R is low AND D is near THEN

AV_p is high

IF C is high AND R is low AND D is far THEN

AV_p is high

IF C is high AND R is high AND D is near THEN

AV_p is medium

IF C is high AND R is high AND D is far THEN

AV_p is medium

We use $\min(\mathbf{FUZ}_C, \mathbf{FUZ}_R, \mathbf{FUZ}_D)$ operation to evaluate AND operators in each of the above fuzzy rule. Finally, the crisp output that represents the value of availability factor is calculated using one of the de-fuzzification algorithms with the help of the membership function of the output AV_p as shown in Figure 7. Here we decide to use Center of Gravity for Singletons (COG) algorithm as de-fuzzification algorithm to find the crisp value of the availability factor [17]:

$$AV_p = COG = \frac{\sum_{n=1}^k Res_n * Cen}{\sum_{n=1}^k Res_n}, \quad 0 \leq AV_p \leq 1 \quad (5)$$

Res_n is the result of n^{th} rule

Cen is the center of the gravity of the area bounded by the membership function.

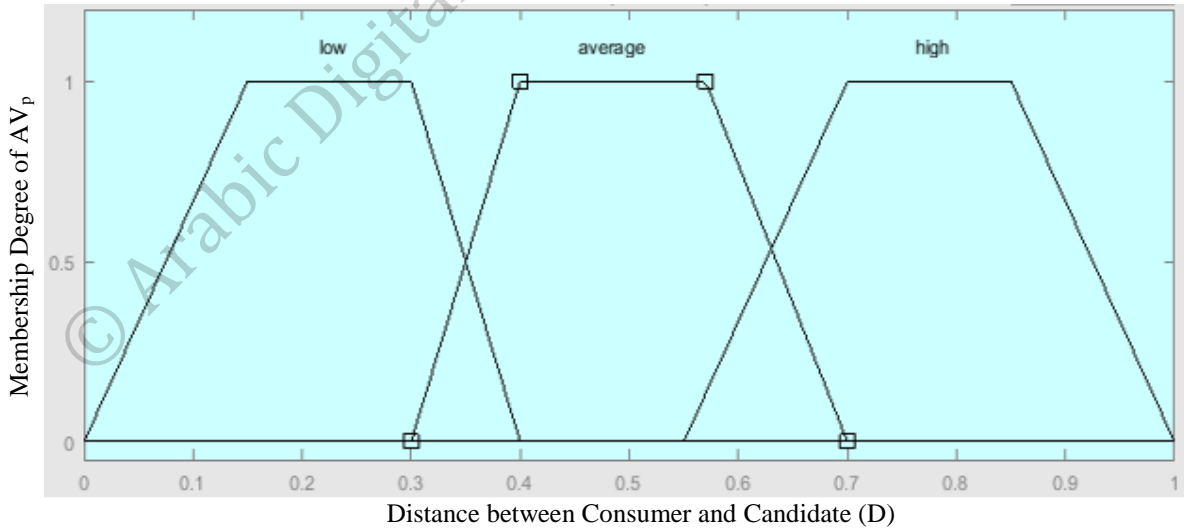


Figure 7: Membership function of provider's availability (AV_p)

With respect to link quality factor, we use an effective link quality estimation metric used widely in wireless networks, named expected transmission count

(ETX) [27]. Simply, ETX is formulated as a function of both the forward packet delivery rate PDR_f , and reverse packet delivery rate PDR_r as follows:

$$LQ_p = PDR_f . PDR_r , 0 \leq LQ_p \leq 1 \quad (6)$$

Finally, the social trust for the consumer node (ST_c) concerns with calculating the weighted average value of all past evaluations sent by the potential provider SP_j evaluating the behavior of SC_i besides the weighted average value of all past recommendations coming from different providers who provided any service to SC_i . The following equation calculates the overall value of the social trust for the consumer node:

$$ST_c = \alpha_3 \left[\frac{\sum_{l=1}^m TW_l . DScore_l}{m} \right] + \beta_3 \left[NW_p . \frac{\sum_{k=1}^n TW_k . RScore_k}{n} \right] , 0 \leq ST_c \leq 1 \ \& \ \alpha_3 + \beta_3 = 1 \quad (7)$$

Where α_3 is the direct experience weight, and β_3 is the indirect recommendation weight. $DScore_l$ indicates the l^{th} value of direct evaluation score sent by SP_j , and $RScore_k$ indicates the evaluation score value sent by the k^{th} recommender. Also, TW_k and TW_l are time-based weights used to weight the impact of each evaluation score based on its time-stamp such that recent ones have more impact. The time-based weights are calculated using equation 3.

NW_p represents the number weight used to measure the credibility of the recommendations such that they will be considered only if the number of recommendations exceeds a pre-defined system threshold N_{thr2} , hence, $NW_p=1$ if $n > N_{thr2}$, otherwise $NW_p=0$.

3.5 Weights adjustment

CATB-IoT model follows a dynamic condition-based approach to adaptively assign new values to the weights of the trust factors in equation 1 each time a new trust calculation query is issued by the in-charge service management system. In this sense, we aim at changing trust factor's weights based on the amount of variation of newly calculated values for each trust factor across all candidate provider nodes selected in service recommendation phase. As a result, the trust factor with high dispersive values will be assigned higher weight than the factor with lower dispersive values. Deciding such approach in adjusting weights is suitable because it contributes to determining the importance of each trust factor based on the current situation of all candidate provider nodes. Mathematically, we use the standard deviation to measure the variance of the values of each trust factor (TF_i) across n candidate provider nodes selected by the service management system:

$$SD_i = \sqrt{\frac{\sum_{k=1}^n (TF_{ik} - \overline{TF_i})^2}{n-1}}, i=1,2,3,4 \quad (8)$$

Consequently, the calculated standard deviation of each trust factor contributes to the ranking of involved trust factors based on their importance such away the most important factor has the highest standard deviation, hence, will have the highest weight. Next, the actual weights are simply calculated by finding the relative ratio as follows:

$$w_i (\text{percentage}) = \frac{SD_i}{\sum_{k=1}^n SD_k}, i=1,2,3,4 \quad (9)$$

CHAPTER 4: EVALUATION AND ANALYSIS

In this chapter, we are to develop some test cases and scenarios so as to analyze and evaluate the performance of CATB-IoT model regarding its accuracy, condition adaptability, defending common trust-related attacks, and robustness in decision making about potential service-based interactions between various IoT nodes. Following the evaluations, we present a case study where CATB-IoT could be applied effectively.

4.1 Environment setup

Indeed, there is no real database to test our model, nevertheless, we developed C# application to simulate the operations of CATB-IoT based on random data. Hence, we rely on data generated at simulation time to calculate all trust factors that form our trust values. The simulator program generates 600 feedback reports for each provider and consumer node filled with random values of evaluation scores, consumer id, provider id, and service id. Also, the values of PDR_f (equation 6), PDR_r (equation 6), N_{xj} (equation 4), N_x (equation 4), N_{succ} (equation 4), N_{tot} (equation 4), and the provider's availability attributes (capability, instantaneous number of requests, and distance between consumer and provider) all are generated randomly. Table 6 contains the default simulation parameters that will be used to initialize some constants and variables used in trust computation [10].

Table 6: Simulation Parameters

Total number of IoT nodes	200
Number of provider nodes	50
Number of consumer nodes	150
Number threshold for consumers as recommenders (N_{the1})	30
Number threshold for providers as recommenders (N_{the2})	10
Time window (ψ)	300 (hours)
Time decay constant (γ)	200 (hours)
direct experience weight (α_1) in equation 2	0.6
indirect recommendation weight (β_1) in equation 2	0.4
Transaction volume weight (α_2) in equation 4	0.3
Successfulness weight (β_2) in equation 4	0.7
direct experience weight (α_3) in equation 7	0.6
indirect recommendation weight (β_3) in equation 7	0.4

4.2 Evaluation and analysis

In this section, we elaborate a set of evaluation cases through which the efficiency of the proposed model is recognized. The evaluation cases are applied based on the transaction flow illustrated in Figure 2. Consequently, we always assume that multiple IoT nodes could provide the requested service. Also, we assume that candidate providers vary in their capabilities, locations, popularity, and service behavior. Consumers vary in their behaviors as well.

- **Evaluation case 1: Influence of decreasing one trust factor on the choice of a service provider**

To prove the accuracy of our model in estimating the trust level of the potential service-oriented IoT transactions, it is proper to show how CATB-IoT responses to sudden drop in one trust factor and how this will affect the consequent decision about selection of a service provider for potential

requests. Given that successful trade between consumer and provider nodes implies that each node must trust each other, Figure 8 below plots the total number of successful trades for each candidate provider based on requesting a certain service initiated by various consumers over a period of time. Assuming that out of available 50 providers, only 5 service providers (P1, P2, P3, P4, & P5) could provide the requested service out of available 50 providers. Provider P1 is selected randomly, i.e.: not on CATB-IoT basis. Whereas, providers P2 through P5 are selected based on CATB-IoT approach. Also, P1 and P2 will have a sudden drop in their AV_p (only 10%) starting from time T3. Given that 1000 requests are initiated per time unit (5 hours), the results show that starting from time T3, P1 is still selected normally apart from the significant decrease in AV_p , however, P2 selection approaches to zero. On the other hand, the selection of the providers P3 through P5 increases significantly. Figure 9 shows the results of the former scenario but with regard to LQ_p (i.e.: $LQ_p=10\%$).

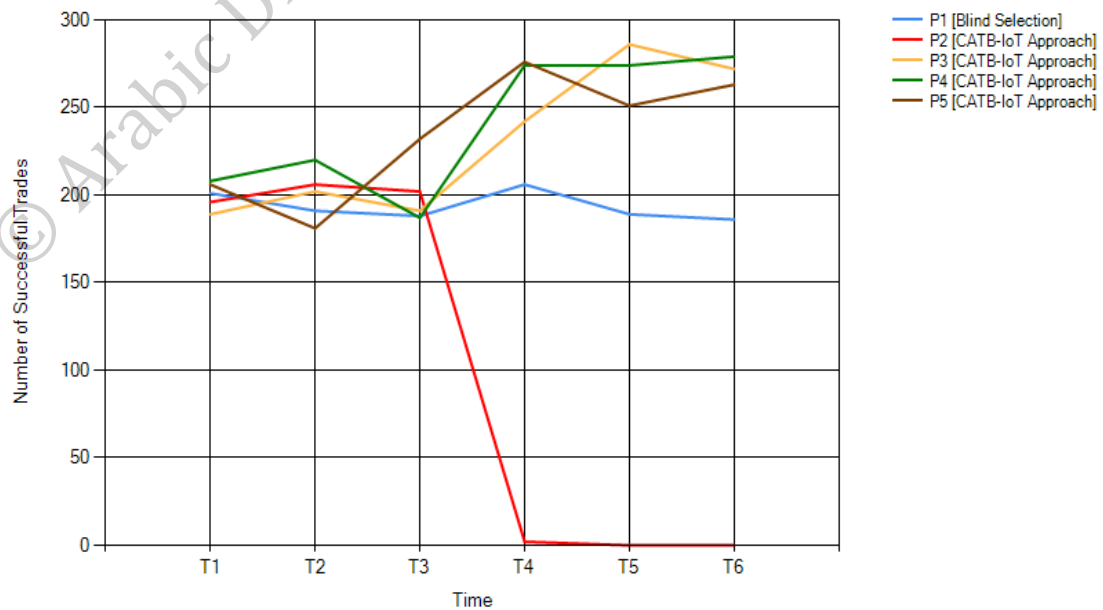


Figure 8: Results of evaluation case 1 ($AV_p=10\%$ after T3 for P1 and P2)

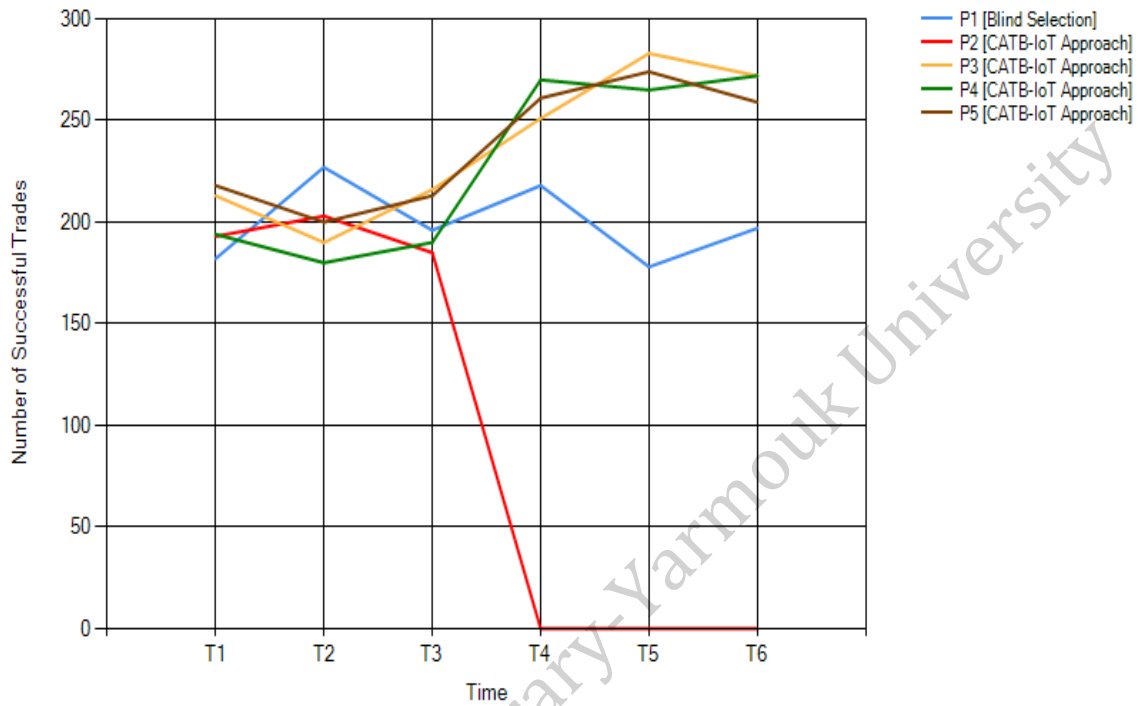


Figure 9: Results of evaluation case 1 (LQp=10% after T3 for P1 and P2)

▪ **Evaluation case 2: Relationship between the number of successful trades and the average trust value for a service provider**

One way to show the strength of our proposed model is to plot the relationship between the number of successful trades and the average trust value for each provider over time. Hence, Figure 10 shows the consistency in relationship between the number of successful trades and the average trust value for each of the five service providers (P1, P2, P3, P4, & P5) over 5 days. Given that 100 requests are initiated over the simulation time, the results show that the normalized trust value (TV_{avg} which represents the average of all trust values calculated in response to the 100 requests) reflects the corresponding normalized successful trades (Succ which represents the

ratio of the number of successful trades over 100) over the whole simulation time.

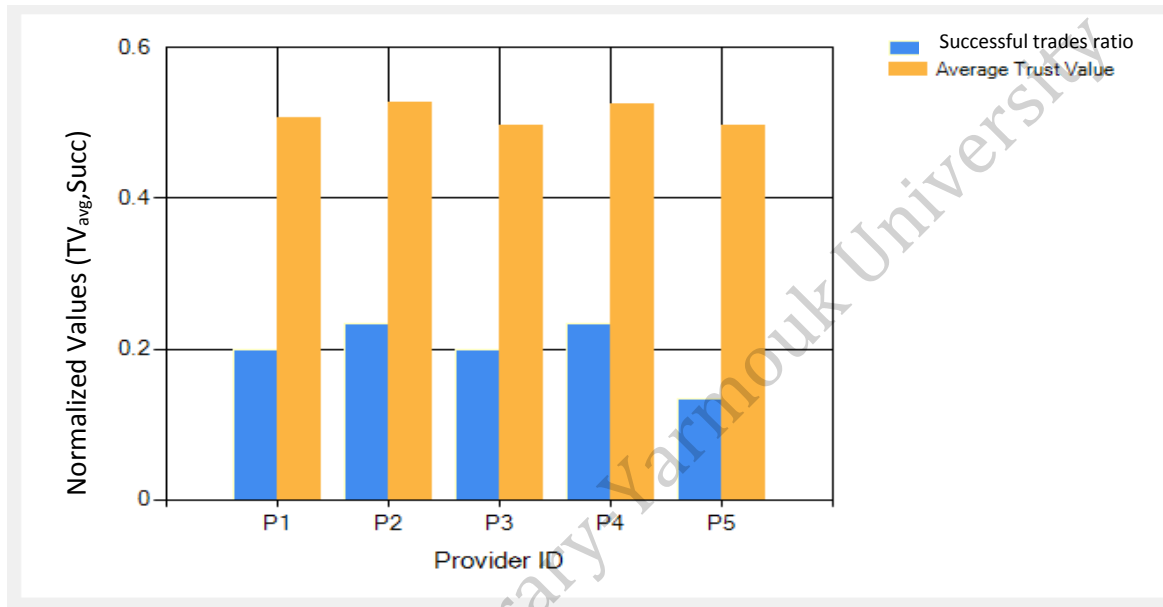


Figure 10: Results of evaluation case 2

- **Evaluation case 3: Reliable behavioral trust estimation for consumer node**

CATB-IoT is distinguished in estimating long-term behavioral trust of the communicating nodes (consumer and provider) in such a way it gives more credibility to recent feedback reports, imposes a restriction on the number of valid recommendations, and discards feedback reports whose ages exceed a pre-defined time window. This will participate in providing a reliable evaluation of the behavior of these nodes when they intend to communicate. Therefore, Figure 11 plots the total number of successful trades for five consumers (C1, C2, C3, C4, & C5) over five days. Assuming that all providers set randomly predefined thresholds for the consumers' social trust (ST_c) in the range [0.6, 0.7]. Particularly, consumer C1 is not undergone to

CATB-IoT approach, whereas, the behavior of the consumers C2 through C5 is determined based on CATB-IoT approach. Moreover, both C1 and C2 have good evaluation scores (above 0.7) in the first 40 hours and bad evaluation scores (only 0.3) in the rest of the simulation time (last 80 hours). Given that one request is initiated from each consumer every 4 hours (5 requests per 20 hours), the results show that consumer C1 is involved normally for future communications with different potential providers apart from the sudden changes in its evaluation scores. Whereas, consumer C2 will have a gradual decline in the number of successful trades with candidate providers starting from the 40th hour of simulation time. On the other hand, consumers C3 through C5 have made reasonable number of successful trades with various providers over the whole simulation time.

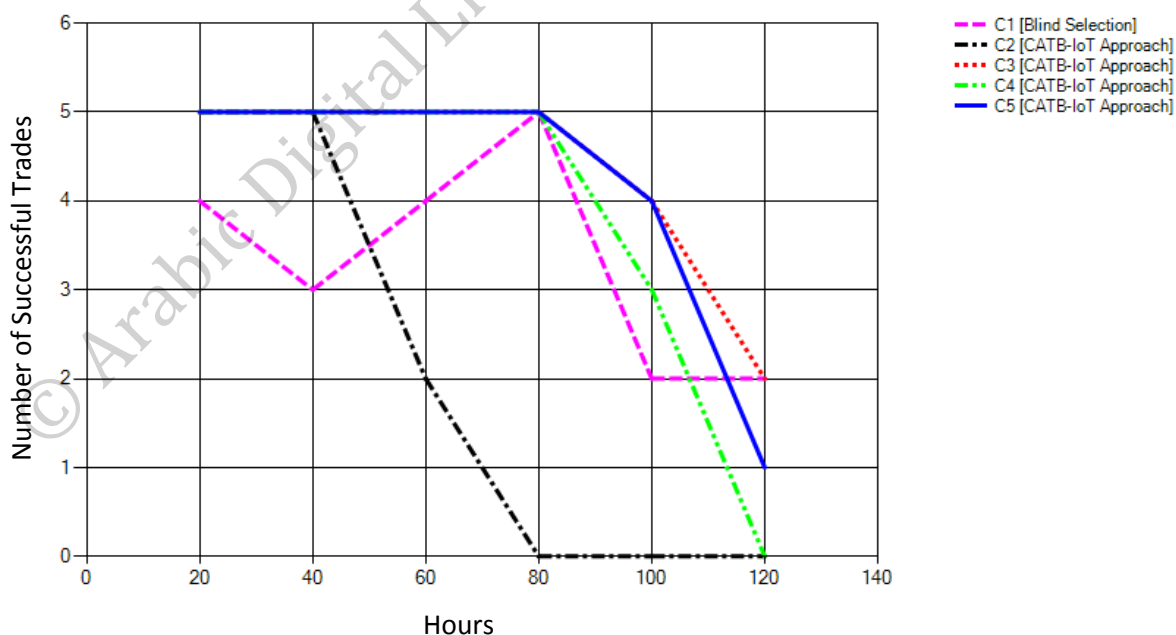


Figure 11: Results of evaluation case 3 (C1 and C2 have good old behavior, & bad recent behavior)

Figure 12 depicts the above scenario, but in this case both C1 and C2 have bad evaluation scores (only 0.3) in the first 40 hours and good evaluation scores (above 0.7) in the rest of the simulation time (last 80 hours). The results show that consumer C1 is involved normally for future communications with different potential providers apart from the sudden changes in its evaluation scores. Whereas, there is a significant increase in the number of successful trades that C2 made starting from the 60th hour of the simulation time. On the other hand, consumers C3 through C5 have made reasonable number of successful trades with various providers over the whole simulation time.

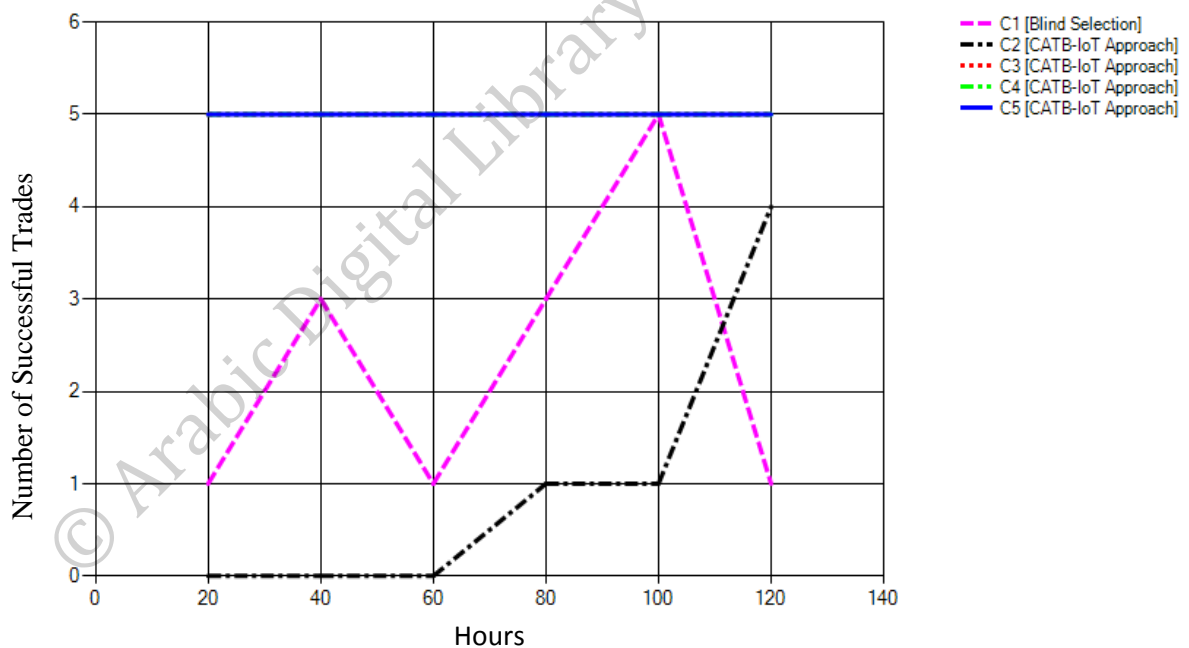


Figure 12: Results of evaluation case 3 (C1 and C2 have bad old behavior, & good recent behavior)

▪ **Evaluation case 4: Protection against trust-related attacks**

In malicious environment, malevolent nodes perform recommendation attacks like SPA, BMA, and BSA and malicious behavior attacks like OSA.

In such situations, trust management systems must cope with these attacks to offer secure environment and avoid possible risks as much as possible. In this sense, CATB-IoT handles these attacks as follows:

SPA: in CATB-IoT model, nodes do not provide recommendations about themselves, so it is impossible to perform such attacks.

BMA and BSA: CATB-IoT assigns more importance to direct experience than indirect recommendations besides that recommendations themselves are received from different recommenders. Therefore, the impact of false recommendations is decreased to minimum levels.

OSA: Since CATB-IoT model takes into consideration long-term behavior of involved nodes, it can record past misbehaving. As a result, it is not easy to regain the reputation of the involved nodes.

4.3 Case study

Here we are to exemplify a case where CATB-IoT model could be applied such that the benefits of our proposed model are efficiently utilized to enhance the overall performance of the target applications. Thus, we choose on-demand taxi service as a case study in which both the client and the service provider needs to evaluate each other prior going ahead in service provisioning.

In such circumstances, the client concerns with finding a service provider that will offer reasonable service quality. Similarly, the service provider interests in attracting qualified clients that will behave well. Consequently, there must be a trust management mechanism by which each entity could contact with eligible counterpart that meets its pre-defined trust level. In this sense, CATB-IoT model

comes to play such role in deciding the trustiness of the involved entity. CATB-IoT efficiently will evaluate the trustiness of the client based on the historical behavior which reflects the eligibility of him. On the other hand, CATB-IoT will evaluate the trustiness of the provider based on the historical service behavior patterns in addition to the essential real-time information which predicts the quality of the service it will offer. Moreover, the taxi service will be enhanced by the service recommendation feature of the proposed model through which the client will find multiple alternatives in case of failing interactions or interesting in finding providers that meet its preferences.

© Arabic Digital Library - Yarmouk University

CHAPTER 5: CONCLUSION AND FUTURE WORK

5.1 Conclusion

CATB-IoT is a multi-factor information fusion trust model that presents trust as a convenience and goodness degree to judge the suitability of the potential service-oriented transactions in IoT systems. CATB-IoT invests trustworthiness to ensure providing adequate services to qualified consumer in suitable conditions. We introduce a centralized recommendation service through which multiple providers are suggested to the consumer upon requesting a service. Unlike most trust models, CATB-IoT takes into consideration the trustworthiness of the service consumer in addition to service provider which improves the collaboration and trust between the two entities.

The simulation results show that CATB-IoT exhibits increased accuracy and improved decision making robustness in estimating the trustworthiness of potential service-oriented IoT transactions. Moreover, CATB-IoT withstands common trust-related attacks like BMA, BSA, SPA, and OSA. The results also show that CATB-IoT provides reliable trust measurement toward service consumer by assigning credibility to feedback reports on time basis.

5.2 Future work

At the end of the day, it is important to explore some critical issues, innovative ideas, and shortcomings that might fix problems and enhance the overall performance of our trust system. In this sense, we suggest the following future research directions and recommendations:

- Introducing a proactive service management system through which it automatically suggests a list of all available service providers that could provide common services with high request rates depending on the current context of the service consumer.
- To decrease the effects of single-point failure, we suggest to modify CATB-IoT model such that it adopts hybrid approach. By this way, we rely on central database system to receive social trust of both provider and consumer nodes in timely manner. However, the essential trust computations are performed at the potential nodes (consumer and provider).
- To produce more meaningful and reliable results, we aim to use a network simulator like OPNET or NS2 to simulate and verify the operations of our model.

© Arabic Digital Library - Yamouk University

REFERENCES

- [1] Nguyen B.Truong, Tai-Won Um, and Gyu Myoung Lee, “*A Reputation and Knowledge Based Trust Service Platform for Trustworthy Social Internet of Things*”, 19th International ICIN Conference - Innovations in Clouds, Internet and Networks, 2016.
- [2] Michele Nitti, Roberto Girau, Luigi Atzori, Antonio Iera, and Giacomo Morabito, “*A Subjective Model for Trustworthiness Evaluation in the Social Internet of Things*”, 23rd Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, 2012.
- [3] Ing-Ray Chen, Member, Fenyue Bao, and Jia Guo, “*Trust-Based Service Management for Social Internet of Things Systems*”, IEEE Transactions on Dependable and Secure Computing, 2016.
- [4] Dong Chen, Guiran Chang, Dawei Sun, Jiajia Li, Jie Jia, and Xingwei Wang, “*TRM-IoT: A Trust Management Model Based on Fuzzy Reputation for Internet of Things*”, Computer Science and Information Systems Journal, 2011.
- [5] Michele Nitti, Roberto Girau, and Luigi Atzori, “*Trustworthiness Management in the Social Internet of Things*”, IEEE Transactions on Knowledge and Data Engineering, 2014.
- [6] Yosra Ben Saied, Alexis Olivereau , Djamal Zeghlache , and Maryline Laurent, “*Trust management system design for the Internet of Things: A context-aware and multi- service approach*”, computers & security, Volume 39, SciVerse ScienceDirect, 2013.
- [7] Yating Wang et al., “*CATrust: Context-Aware Trust Management for Service-Oriented Ad Hoc Networks*”, IEEE Transactions on Services Computing, 2016.

- [8] Sherif Emad Abdel Rafeey, Ayman Abdel-Hamid, and Mohamad Abou El-Nasr, “*CBSTM-IoT: Context-based Social Trust Model for The Internet of Things*”, International Workshop on Scalable Internet of Things, 2016.
- [9] Oumaima Ben Abderrahim, Mohamed Houcine Elhedhili, and Leila Saidane, “*CTMS-SIOT: A Context-based Trust Management System for the Social Internet of Things*”, 13th International Wireless Communications and Mobile Computing Conference (IWCMC), 2017.
- [10] Zhiquan LIU, Jianfeng MA, Zhongyuan JIANG, and Yinbin MIAO, “*FCT: a fully-distributed context-aware trust model for location based service recommendation*”, Science China Information Sciences, Journal no. 11432, volume 60, 2017.
- [11] Xiaoyong Li, Feng Zhou, and Xudong Yang, “*A multi-dimensional trust evaluation model for large-scale P2P computing*”, Journal of Parallel and Distributed Computing, Volume 61, 2011.
- [12] Zheng Yan, PengZhang, and AthanasiosV.Vasilakos, “*A survey on trust management for Internet of Things*”, Journal of Network and Computer Applications, Volume 42, 2014.
- [13] Jia Guo, Ing-Ray Chen, and Jeffrey J.P. Tsai, “*A survey of trust computation models for service management in internet of things systems*”, Computer Communications, Volume 97, 2016.
- [14] Charith Perera, Arkady Zaslavsky, Peter Christen, and Dimitrios Georgakopoulos, “*Context Aware Computing for The Internet of Things: A Survey*”, IEEE Communications Surveys and Tutorials, 2013.

- [15] GU Lizet, WANG Jingpei, and SUN Bin, “*Trust Management Mechanism for Internet of Things*”, China Communications, 2014.
- [16] Carmen Fernandez-Gago, Francisco Moyano, and Javier Lopez, “*Modelling trust dynamics in the Internet of Things*”, Information Sciences, Volume 396, 2017.
- [17] L.A. Bryan and E.A. Bryan, “*Programmable Controllers, Theory and Implementation*”, second edition, section 5, chapter 17, 1997.
- [18] Ovidiu Vermesan and Peter Friess, “*Internet of Things-From Research and Innovation to Market Development*”, River Publishers, 2014.
- [19] Statista-The Statistics Portal for Market Data, Market Research, and Market Studies, <https://www.statista.com>, April 2018.
- [20] Internet of Things news and strategies-IoT Tech News, <https://www.iottechnews.com>, April 2018.
- [21] History of IoT-Background Information and Timeline of the Trending Topic, <https://www.postscapes.com/internet-of-things-history/>, April 2018.
- [22] A Very Short History of The Internet of Things, <https://www.forbes.com/sites/gilpress/2014/06/18/a-very-short-history-of-the-internet-of-things/#4a0cee9510de>, April 2018.
- [23] Vera Suryani, Selo Sulistyono, and Widyawan, “*Trust-Based Privacy for Internet of Things*”, International Journal of Electrical and Computer Engineering, 2016.
- [24] Neeraj, and Amitpal Singh, “*Internet of Things and Trust Management in IoT-Review*”, International Research Journal of Engineering and Technology, 2016.
- [25] Jingwei Huang, Mamadou D. Seck, and Adrian Gheorghe, “*Towards Trustworthy Smart Cyber-Physical-Social Systems in The Era of Internet of Things*”,

12th IEEE International Symposium on Service-Oriented System Engineering, 2016.

[26] Syed Rehan Afzala, Sander Stuijka, Majid Nabia, and Twan Bastena, “*Effective link quality estimation as a means to improved end-to-end packetdelivery in high traffic mobile ad hoc networks*”, Digital Communications and Networks, Volume 3, 2017.

© Arabic Digital Library-Yarmouk University

ملخص

محمد بسام عبيدات، منهاج مدرك للحيثيات لتقديم الخدمات بناءً على مستوى الثقة في إنترنت الأشياء، ماجستير العلوم في النظم المضمنة-قسم هندسة الحاسوب، جامعة اليرموك، 2018، المشرف الرئيسي: د. هشام المساعيد

في مجال تكنولوجيا المعلومات ، تقود إنترنت الأشياء (IoT) تحولاً كبيراً نحو التفاعل السلس بين مليارات الأجهزة غير المتجانسة والواسعة الانتشار عبر الإنترنت. تحتاج هذه الشبكة المعقدة والمنشرة إلى إدارة الثقة لتوفير علاقات جديرة بالثقة ، اتخاذ قرارات قوية ، والتعاون الموثوق به. ومع ذلك ، فإن الثقة في أنظمة إنترنت الأشياء يتم تقديمها على مستويات ومنظورات مختلفة تبعاً للغرض من النظام. ومن ثم ، فإننا في هذا العمل ، نقدم الثقة كمقياس لمدى المناسبية والجودة لتوفير الخدمات في نموذج إنترنت الأشياء من أجل استنباط قرارات قوية بشأن المعاملات المحتملة للخدمة. الهدف الرئيسي للعمل المقترح هو توفير الخدمات الكافية لمستهلكي الخدمة المؤهلين في ظروف مناسبة بحيث يتم تحقيق فوائد قيمة إلى كيانات إنترنت الأشياء المعنية (مستهلك الخدمة ومقدم الخدمة) والمخاطر المحتملة والنتائج غير المرغوب فيها. نموذج الثقة المقترح ، المسمى (CATB-IoT) ، يعتمد على السياق ويتضمن العديد من العوامل المتعلقة بمستهلك الخدمة ومقدم الخدمة والبنية الأساسية لعمليات إنترنت الأشياء. يقدم نموذج CATB-IoT مساهمتان رئيسيتان. أول مساهمة هي النظر في الثقة الاجتماعية لمستهلك الخدمة بالإضافة إلى مزود الخدمة. بينما المساهمة الثانية تتمثل في تقديم خدمة التوصية، حيث يُقترح من خلالها مزودي خدمة متعددين قادرين على تقديم الخدمة المطلوبة. تظهر نتائج المحاكاة أن CATB-IoT تقدم دقة متزايدة وتحسن في اتخاذ القرارات في تقدير مدى موثوقية صفقات إنترنت الأشياء المحتملة الموجهة نحو الخدمات. علاوة على ذلك ، تتعامل CATB-IoT مع هجمات معروفة تتعلق بالثقة مثل BMA و BSA و SPA و OSA. كما تظهر النتائج أن نظام CATB-IoT يوفر تنبؤاً موثقاً به للثقة الاجتماعية لكل من مستهلك الخدمة ومزود الخدمة من خلال تعيين مصداقية لتقارير التغذية الراجعة على أساس الوقت.

كلمات مفتاحية: إنترنت الأشياء، إنترنت الأشياء الموجه للخدمة، نموذج الثقة، خدمة التوصية، اتخاذ القرار، الدقة، عامل الثقة، المنطق الضبابي، تعديل الوزن