IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.201X.DOI

ARCA-IoT: An Attack-Resilient Cloud-Assisted IoT System

SABEEN JAVAID[1], (Member, IEEE), HAMMAD AFZAL [2], MUHAMMAD BABAR [3], FAHIM ARIF [4],(Member, IEEE), ZHIYUAN TAN [5], (Member, IEEE), and MIAN AHMAD JAN [6] , (Member, IEEE)

[1]National University of Sciences and Technology, Islamabad, Pakistan (e-mail: sabeen@mcs.edu.pk)
[2]National University of Sciences and Technology, Islamabad, Pakistan (e-mail: hammad.afzal@mcs.edu.pk)
[3]National University of Sciences and Technology, Islamabad, Pakistan (e-mail: babar.phd@student.mcs.ed.pk, muhammad.babar@iqraisb.edu.pk)
[4]National University of Sciences and Technology, Islamabad Pakistan (e-mail: fahim@mcs.edu.pk)
[5]School of Computing, Edinburgh Napier University, United Kingdom (e-mail: z.tan@napier.ac.uk)
[6]Abdul Wali Khan University Mardan, KPK, Pakistan (e-mail: mianjan@awkum.edu.pk)

Corresponding author: Sabeen Javaid (e-mail: sabeen@mcs.edu.pk).

ABSTRACT Putting trust in the world of the Internet of Things, where served and serving entities are often unknown, is very hard especially when personal and business information is often being exchanged for providing and consuming services. Moreover, the issues of interoperability and scalability of billions of heterogeneous things in IoT systems require more attention. A user-centric model of complex interconnected things must be designed in a way that not only makes things trustworthy for common people but it also provides the solution for interoperability and scalability. ARCA-IoT is such a system which not only identifies the attributes (including quality of service) essential for trust but also presents a user-centric model that is robust enough to tackle the attacks made by dishonest entities to manipulate the trustworthiness. For scalability and interoperability, a cloud-assisted environment is introduced in ARCA-IoT. An intuitive Naive Bayes approach is used to train ARCA-IoT in a way that it calculates the probabilities of the trustworthiness of the entities and then identifies various types of attacks with the support of three proposed algorithms. The approach is validated with a specifically designed simulated environment. Based on our simulation results, ARCA-IoT demonstrates the effectiveness in term of performance metrics such as accuracy, sensitivity, specificity, and precision. Besides this, the system outperforms the existing related approaches in terms of a qualitative analysis based on different parametric metrics such as interoperability, scalability, context-awareness, and a human-like decision.

INDEX TERMS Cloud, Context, IoT, QoS, Service, Social, Trust, WoT

I. INTRODUCTION

IN a world being transformed by technology, people are getting connected with each other through different kinds of devices for getting the privileges of modern technology. Internet of Things (IoT) is a remarkable example of this transform. It defines a network of various devices, digital and mechanical, that exchange data over the Internet. This network has the ability to work without human intervention [1] and unlimited 'things' are going to be connected through it. The services provided by these 'things' range from smart businesses to smart homes and from smart health monitoring to smart agriculture. However, this complex network of smart 'things' faces many challenges. One of the complex challenges is the trustworthiness of smart 'things' . Since members of the public, who are main beneficiaries of IoT, may have little or no technical knowledge of a 'thing', there are chances that they may fall prey to malicious entities which are present in the network. Therefore, the trustworthiness of entities becomes significantly important as ordinary people receive and deliver services from/to unknown entities through 'things' . For example, remote health monitoring through IoT helps in reading a patient's vital signs and sending them to cloud for a medical practitioner to keep track of a patient's condition. Get-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2897095, IEEE Access

ting health-related life-critical services for cancer or cardiac patients, for example, must be from trustworthy entities. However, malicious and dishonest entities may be present in the network with different motives. A patient's life can be in danger if the selected entity is not able to provide quality services such as late response in case of emergency. Similarly, sensitive data can be used for achieving their malicious objectives because 'big' personal and business data is transmitted among the 'things'. It is fairly said that ensuring the trustworthiness of 'things' with respect to Quality of Services (QoS) is extremely important, and identification of malicious and dishonest entities in the network should be handled with great care.

The second challenge faced by IoT is the interoperability of heterogeneous devices [2]. A survey found that Java is a common programming language for developing IoT applications as 61% of the developers use it for building IoT applications. However, this trend is a hindrance towards the freedom of choice for the developers because those, who are experts in other languages, learn Java for IoT applications [3]. Interoperability works as a fuel in IoT innovation. It is estimated that by 2025 over $11 trillion in revenue per year will be generated by IoT applications and it is also expected that up to 40% of the revenue will be generated by those IoT applications which ensure interoperability [3].

World Wide Web and its associated technologies can be helpful in resolving the issue of interoperability [2]. Another advantage of integrating 'things' with Web technologies is to make 'things' easy to discover, bookmark and share. [4]. The approach of integrating smart things with the Web is called Web of Things (WoT). For this purpose, Representational State Transfer (REST) architectural style [5] is applied to resources in the physical world. REST abstracts the services in a uniform interface and a platform independent universal Application Program Interfaces (APIs) [6] for smart things are built. In short, the purpose of REST is to develop loosely coupled reusable web services. It uses a Uniform Resource Identifier (URI) for web services' identification and encapsulation on the Web. These qualities make it an ideal candidate architecture to build an API for smart things [7].

The third issue faced by IoT applications is scalability. It is an important required ability for IoT applications because increasing service requests within limited capacity of IoT infrastructure can adversely affect the efficiency of a system. The characteristics associated with IoT are limited processing and storage capacity with widely distributed small 'things' [8]. The shortcomings of IoT, such as limited processing and storage capacity, can be overcome by Cloud computing as it has virtually unlimited capabilities in terms of storage and processing power. Thus, cloud and IoT are two technologies that complement each other and by using them together, it becomes feasible to create on-demand access to a pool of computing resources with the least minimal management effort or service provider interaction [8].

Therefore, to enhance the reliability of IoT applications, the level of dishonesty of a smart entity or malicious attack will be first measured or detected by our proposed ARCA-IoT using its proposed algorithms and Naive Bayes classifier. As trust is a context-dependent concept [9] and varies from one 'thing' to another 'thing', context-relevant attributes are carefully extracted in ARCA-IoT.

Then, to enhance i) scalability (through resource pooling and on-demand features), ii) and interoperability (through APIs) cloud computing and web technologies are integrated with 'things' as services in the Web, i.e., WoT. It is noteworthy that in a service-based approach, 'things' offering services are called 'service providers' whereas those who seek and then consume services from service things are called 'service seekers' and 'service consumers', respectively. Besides this, it is also important to measure QoS provided by a service provider. For this purpose, feedback is taken from service consumers. Moreover, service seekers also get recommendations from the social network if they do not have any previous history of that type of service consumption.

The contributions of this research are as follows:

1) Identification of context and QoS related attributes which are considered important for the trustworthiness of entities in IoT.
2) A cloud-assisted WoT environment is introduced to resolve the interoperability issue and enhance the scalability.
3) ARCA-IoT also provides resilience against ballot stuffing, bad-mouthing, and oscillation attacks. For this, the Naive Bayes Classifier is used which helps in the identification of untrustworthy entities and then the proposed algorithms for attacks (such as ballot stuffing, bad-mouthing and oscillation) are applied to identify the type of attack.
4) The efficiency of the system is tested with a specifically designed environment. Performance metrics are used to measure the performance of ARCA-IoT. Moreover, a qualitative analysis of ARCA-IoT based on parametric metrics with already defined systems in the related areas is carried out.

The rest of the paper is organized as follows. The related work in trust management is described in Section II. The system model is elaborated in Section III. Section IV presents the details of ARCA-IoT whereas Section IV discusses the effectiveness of ARCA-IoT by describing the experiments. Section V concludes the research.

II. BACKGROUND STUDY

In this section, the related work from the literature on trust management, interoperability, and scalability in IoT and related areas is discussed. Trust is a subjective phenomenon which is complex to assess and its presence or absence in an interaction plays a significant role. This is the reason, it has been in focus in various research areas. Consequently, many trust management systems have been proposed. These systems monitor the activities of the entities to identify dishonest behavior and irregular activities. However, it is difficult to identify dishonest entities present in a network of billions of entities, i.e., IoT. A reasonable work has been done in the area of trust in terms of privacy and security. However, it is identified that there are the deficiencies which are not addressed fully in the related work. The state-of-the-art related approaches along with these deficiencies are discussed below.

Angelo et al. [10] proposed a trust model based on Apriori Learning and Bayesian Classification for pervasive computing. By observing the interactions with other entities and then through Data Mining techniques, the authors proposed two steps for decision making. For extracting the behavioral pattern, Apriori algorithm was used whereas for final decision making, Bayesian classifier was used. An attribute vector to show the experience of an entity was defined. These include entity identification, trust score, counting trust, counting untrust, last time, transaction context (games, e-commerce), direct experience, source entity in tree-based relation and level of the hierarchy. Three types of attacks are taken care of in the system which include the counting-based attack, time-based attack, and context-based attack. It is identified that QoS based trustworthy evaluation was not carried out in the system. There was only one parameter for the context-based attack which is the type of service. Three common attacks such as ballot-stuffing, bad-mouthing and oscillation attacks were also not given attention [10]. The interoperability and scalability were also not the focus of this research.

Mehmood et al. [11] proposed a system which was based on Naive Bayes Classifier for providing resistance against DDoS attacks in IoT. It was a multi-agent which worked along with Bayesian classifier and identified Distributed Denial of Service (DDoS) attacks. The multi-agents were proposed to be present throughout the network so that information could be gathered and attacks could either be prevented or tackled. The system only considers the securing computing in IoT. Moreover, interoperability and scalability were not given consideration in this system.

For task automation, a context-aware system [12] was designed for IoT. The objective was to help users in selecting the sensors based on meaningful information and to introduce the sensing-as-a-service concept. For this, four internal and two external layers were introduced which fulfilled the propose of automation and reasoning. However, neither QoS nor attack identifications, scalability were given attention. No human-like decision technique was incorporated into the system. Another framework FACT [13] was introduced for information distribution in the vehicular network. It checked the authenticity of the information by calculating trust values and then found the best path for the delivery. A Trust-Aware Access Control System for IoT (TACIoT) [14] was introduced which considered four dimensions of trust. Those were the social relationship, QoS, security aspects, and reputation. The secure and reliable communication-based system consider access control of IoT application, however, only four QoS attributes (such as availability, throughput, delay, and successful interaction) were considered in the system. No attention was given to context-awareness, interoperability and attack identification (such as ballot stuffing, bad-mouthing) in the system.

A trust protocol was proposed by I. Chen et al. [6] which worked on adaptive filtering technique. Social relations were used to get recommendations whereas experience and historical data were also used for trust calculation. Attacks like opportunistic attack, bad-mouthing, and ballot stuffing were considered in the research. The trust is maintained only at user's end which makes it difficult for other users who have less social contacts. However, context awareness and QoS were not given attention in the system.

A context-aware trust management system was proposed by Saied et al. [15]. Different phases were suggested for information gathering and entity selection. Finally, the selection was based on the competition and best-rated nodes were selected. Then after getting services, client nodes gave feedback and trust score was updated accordingly. The cognitive phase which was a learning phase was used as an adaptive process. Simulation results showed that several attacks were stopped by the proposed system. The system provided resistance against off-on attack, bad-mouthing, and selective behavior. However, this was generic context-aware trust management which did not emphasize the detailed analysis of QoS attributes. Moreover, interoperability and scalability were also not considered in the system.

Delsing et al. [16] enabled IoT automation using local clouds without the usage of external resources which assured safety, scalability and multi-stakeholder integration. However, QoS based trustworthiness did not get attention in this research. A federated edge-assisted mobile cloud was proposed by Farris et al. [17] which enabled service provision in IoT applications. The proposed hybrid approach enhanced scalability and the deployment cost was also reduced. However, no attention was given to trustworthiness of the entities present in the network. Stergiou et al. [18] described

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2897095, IEEE Access

security as a big threat in a survey. Moreover, they recognized that there was a lack of trust in service providers when both technologies integrated. In short, it is evident that the focus of research community has been on the integration of cloud computing and IoT because these technologies overcome the deficiencies of each other, however, trust management in cloud-assisted IoT requires more consideration. It is identified that less attention was given to trust management while integrating both technologies.

In view of the above discussion, it is identified that previous models consider one or two major problems faced by IoT in a single solution. To the best of our knowledge, no model has provided a single solution for three major problems (trustworthiness, scalability, and interoperability) faced by IoT. Trustworthiness in terms of on QoS and context-aware parameters specifically related to IoT remain less attended in state-of-the-art approaches. Therefore, there is a need to consider trustworthiness (in terms of QoS and context-aware parameters), interoperability and scalability for IoT related applications in a single solution. Moreover, a human-like decision technique is required to handle the trustworthiness of these billions of things so that in case of absence of human-interference, human-like decisions can be made.

III. SYSTEM MODEL

ARCA-IoT is a system that takes up the three challenges (trustworthiness, interoperability, and scalability) faced by IoT. To design a trustworthy environment, the attributes which play a significant role in identifying trustworthy and untrustworthy 'things' are identified. The system not only evaluates the service providing entities but also the service consuming entities for creating a good and balanced trustworthy environment. Assessing their trustworthiness is necessary so that any kind of malicious behavior can be identified in the system. Therefore, trustworthy 'things' and the types of attacks carried out by untrustworthy entities are considered in the system model. For resolving the issues of scalability and interoperability, a cloud-assisted environment is introduced in the system.

A. CLOUD-ASSISTED SOCIAL WOT MODEL

In ARCA-IoT, a cloud-assisted social WoT Model is considered where entities are connected via a public cloud using REST APIs and socially connected via the owners' social network. Using REST APIs makes entities to be part of the World Wide Web hence introducing Web of Things (WoT) in the system. WoT is the term which comes under the umbrella of IoT. REST APIs help in making the services abstract whereas for context modeling and messaging, JSON (JavaScript Object Notation) is used. It is machine-readable hence making it possible for things to interact with each other through the web. The incorporation of these web technologies also helps to index things like web pages which may also be bookmarked.

There are two types of entities: users and devices. A user may have one or many devices. These devices are controlled by a central device such as a smartphone or a laptop, thus, a user has better control of the system making it a user-centric. Each thing has a unique URI for its identification. In the system, entities act as service providers and service consumers. By exploiting the concept of the social web, the things/devices of an owner may receive/provide services from/to the things/devices of another owner through their central devices if the owners are connected through a social network. 'Things' share their respective owner's social relations, the level of cooperation depends upon the authentication and authorization level granted by an owner to those in his social network. In addition, 'things' can also provide or receive services to and from other devices which are not in the social network. For this, a service seeking entity sends a message for the recommendation of the required service provider entity through its central device. Based on the requirements, the social contacts recommend the potential service providers which are nearer to its location and are trustworthy.

Moreover, ARCA-IoT also leverages the concept of cloud computing which introduces scalability, high performance, and efficiency in the system. It is noteworthy that these are the key elements for the success of IoT [19]. Integrating cloud computing in ARCA-IoT ensures sharing and maximizing the resources which are the requirements of IoT.

It is fairly said that the convergence of three technologies will bring huge opportunities for IoT, Cloud and the Web. For example, the geographical distribution of IoT devices over heterogeneous platforms and multiple-management domains is well managed by the integration of three technologies.

B. TRUSTWORTHY THINGS

In the presence of billions of 'things' , it is difficult to identify 'things' which are trustworthy in terms of providing quality services in a given context. This is the reason, the main focus of ARCA-IoT is to identify trustworthy and non-trustworthy 'things'.

Trust being a subjective and complex concept has been in the focus of various areas. Deutch defines trust as the situation when someone faces an ambiguous path that the outcome is either valuable or destructive [20]. It is identified that this outcome depends on the behavior of one another. Since the level of a destructive outcome is more than that of a valuable outcome, therefore, the trusting choice should be wise enough. Table 1 defines five key characteristics of trust which

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2897095, IEEE Access

TABLE 1: Attributes of Trust

Attributes	Definition
Binary Relation	The existence of a relation between two things.
Contextual	A thing which is trustworthy in one context may not be trustworthy in another context
Quantifiable	Level of a thing's belief in another thing
Asymmetric	A thing may trust another thing but not vice versa
Dynamic	The level of trust may develop or change with time.

are described as key characteristics in state-of-the-art [21]. ARCA-IoT also considers these characteristics.

Keeping the characteristics of trust in view, the system helps in identifying trustworthy 'things' . When an entity consumes a service from a service provider then a level of trust establishes between them. Hence, binary relation, the first attribute of trust, is fulfilled. However, information about this trust level can be disseminated among other entities in the form of recommendations. Trust is dynamic in context. For instance, if an entity provides services in a remote health monitoring system, a trustor who needs services in an IoT based agriculture system cannot trust in this entity. This is the reason that ARCA-IoT considers context dependent trust in its model. In ARCA-IoT, trust is quantified through various parameters of trust and then the aggregated trust value is computed based on these parameters. A service consumer may trust in a service provider but not vice versa, an asymmetric property of the trust. This is a significant characteristic of trust because having trust on each other, for a trustor and a trustee, is important. The dynamic property of trust is also true in the proposed system as ARCA-IoT recalculates the trust level everytime a service is consumed and feedback is provided.

C. TYPES OF ATTACKS

To differentiate honest entities from dishonest ones is a complex problem. It is identified that dishonest 'things' may attack in various ways. Dishonest 'things' try to malign the purpose of a social WoT environment by providing either poor quality services or dishonest feedback. Some of these trust related attacks have been defined in [22] and listed in Table 2. The table describes the types of attacks, and their respective descriptions as well as tells the type of entity that carries out each of the attacks. In Table 2, a service consumer is denoted by 'SC' and a Service Provider is denoted by 'SP'.

The detection of these attacks is a tedious task and it is in the focus of the researchers. At this stage, ARCA-IoT tackles three common attacks which are bad-mouthing, oscillation and ballot stuffing. The others will be tackled in the extended work.

TABLE 2: Types of Attacks

Attack Type	Description	Carried out by
Bad-Mouthing	This is also called Slandering through which an entity maligns the reputation of an honest and fair entity.	SC
Oscillation	It is also called On and Off attack. Behaving like an honest entity but later shifting the behavior through bad performance hence deluding others.	SP
Ballot Stuffing	Boosting the reputation of a bad node by recommending that node.	SC
Sybil Attack	Getting unfair benefits by creating multiple identities	SP
White Washing	Entity with a bad reputation may quit and re-enter in a community for the sake of fresh reputation	SP

IV. RESILIENT AGENT FOR TRUST MANAGEMENT

The architecture of ARCA-IoT is shown in Fig. 1. The proposed system has a main component called "Resilient Agent". It resides on the public cloud to manage the trustworthiness of both service providing and service consuming entities. It provides resilience against the attacks, which try to malign the trustworthiness of an entity, by identifying the malicious entities. For this purpose, three types of managers which include 'Service Provider (SP)', 'Service Consumer (SC)', and 'Social Contact' are the parts of Resilient Agent. These managers take care of service providers, service consumers and social contacts of an entity. Besides this, there is an 'Attack Monitoring Analyst' which analyzes and evaluates the trustworthiness of an entity. The Attack Monitoring Analyst uses a Naive Bayes Algorithm which classifies an entity either as a trustworthy or as a non-trustworthy.

In this section, we explain the three types of managers, i.e., Service Provider, Service Consumer and Social Contact, followed by Attack Monitoring Analyst.

A. SERVICE PROVIDER MANAGER

The profiles of each Service Provider (SP) is maintained and managed by a Service Provider manager. Various attributes are identified for maintaining the profiles of each service provider which are described in Table 3. There are three categories defined for the identified attributes.

1) Identification: This category helps in the identification of a service provider
2) Capability: The attributes, in this category, define the capability in terms of capacity, service timing, processing power, and battery level.
3) Trust Level: It describes the level of trustworthiness which a service provider is able to establish after providing services. It is maintained at two levels. One level maintains the quantified total or global trustworthiness whereas another level

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2897095, IEEE Access

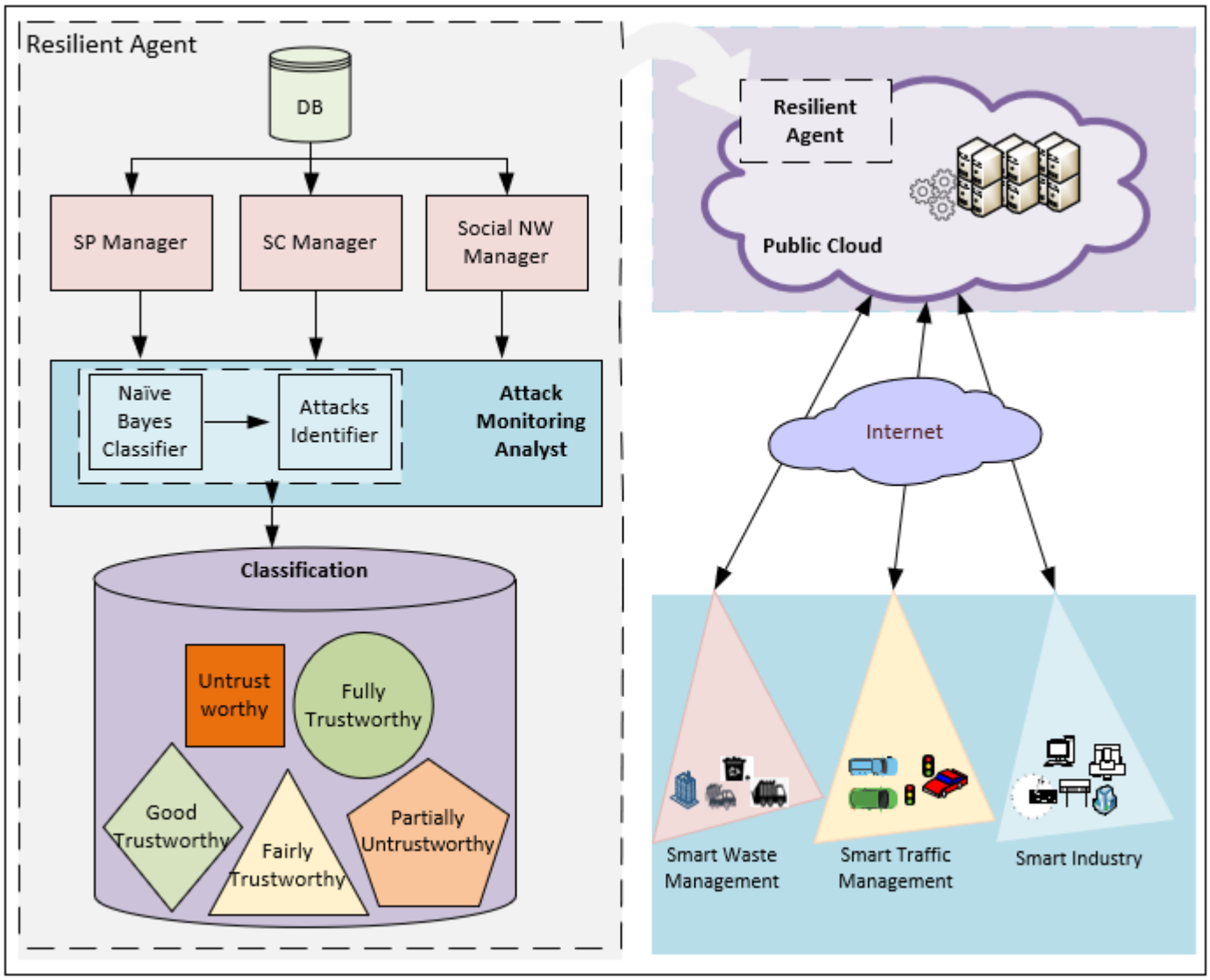

FIGURE 1: The architecture of ARCA-IoT

maintains local trustworthiness for each time a service is provided to a service seeker. Local trustworthiness is kept in the central device of a service consumer.

The attributes belonging to identification and capability categories are related to the context of trust. The context-awareness requires the answers of i)Who, ii)What, iii)When, iv)and Where [23]. The 'Who' describes the identity of an entity which in this case, for example, is URI. The 'What' reflects the type of service and capability. The 'When' describes the service timing and the 'Where' tells the location of an entity. These are the basic concepts of Context Awareness [23]. The answers of these 4 W's are being given through these attributes. For example, the attributes spURI and spIPAddress describe the term 'Who' whereas the attributes spType, spCapacity, and spStdCompliance tell the answer of 'What '. The attribute spTime reflects the term 'When'. Finally, the attributes spLong and spLat describe the term 'where '.

A service-provider registers itself by entering the information about all the 'input attributes' mentioned in Table 3 on a public cloud. Things are accessible through their URIs. After registration, the service provider can be discovered by a service-seeker. The trust level 'TLevel' is calculated based on the feedback of the attributes defined in Table 4. The feedback for these attributes is given by a service-consumer after consuming a service. The method of calculation 'TLevel' is described in IV-D2. The individual trustworthy values in the form of feedback given by each service consumer are also maintained which help in identifying various types of attacks. For this purpose, service consumers

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2897095, IEEE Access

TABLE 3: Attributes of a service provider

Attribute	Description	Category	Type
spURI	Identifies SP uniquely	Identification	Input
spId	Identity of a service provider which may provide many services because of having many SP	Identification	Input
spType	Type of service it is providing	Identification	Input
spIPAddress	IP address of a SP	Identification	Input
spCountry	Name of the country from which a SP is operating	Identification	Input
spLong	To identify the exact location of SP, longitude is considered	Identification	Input
spLang	To identify the exact location of SP, latitude is considered	Identification	Input
spCapacity	The capacity of WoT for which it may provide the services like low, medium and high	Capability	Input
spTime	Time at which the services of SP can be provided	Capability	Input
spStdCompliance	Describes how many standard bodies certifies its operations	Capability	Input
TLevel	Aggregated value of trustworthiness of a SP by considering feedback values of each service consumer	Trust Level	Derived

TABLE 4: Attributes of QoS

Attribute	Description	Type
Reliability	Reliability degree for service	Input
Availability	Existence and availability of the service	Input
Latency	The interval between stimulation and response	Input
Reputation	Feedback score is given by service consumers to a web service	Input
Response Time	The duration within which a SP provides the service whenever it is asked	Input
Throughput	The number of services processed per unit time	Input
PriceSatisfaction	To which level, a service consumer is satisfied with service-providing cost	Input
Consumer Care Services	It describes the level of consumer care services	Input

TABLE 5: Attributes of Service Consumer

Name	Description	Category	Type
ScId	Unique identity of service consumer	Identification	Input
ScIP	The IP address of a service consumer helpful for identifying dishonest SC	Identification	Input
ScC	The country of a service consumer	Identification	Input
ScLong	The exact location of a Service consumer is identified through longitude.	Identification	Input
ScLat	The exact location of a Service consumer is identified through latitude.	Identification	Input
TLevel	The overall trust value of a service consumer based on feedback given by it	Trust Level	Derived

evaluate service-providers based on quality attributes. These attributes are described in Table 4. Some of these attributes are described in [24] whereas the attributes 'consumer-care services' and 'price-satisfaction' are specifically introduced in ARCA-IoT. Consumer-care service is a pro-active tool that helps in creating happy and loyal customers if a service provider deals service consumers' problems with care then quality of service definitely improves. Similarly, service consumers are concerned about getting what they require and getting what they have paid for. Therefore, taking feedback regarding price-satisfaction level becomes significant. After consuming a service, the service consumer rates the service quality for each attribute (also called feature 'F') on a scale from 0 to 1.

B. SERVICE CONSUMER MANAGER

The profile of each service consumer is maintained and monitored by this manager. For this, six attributes are considered for a service consumer which are mentioned in Table 5. These attributes help in identifying honest and dishonest service consumers. These attributes are divided into two categories which are identification and trust level. In addition, the type of attribute whether it is taken as input or derived is also mentioned in Table 5. The attributes related to identification category help in keeping the record of the complete identity of a service seeker. Before consuming a service, it is necessary for a service consumer to register itself by entering 'identification attributes' whereas 'TLevel' is calculated based on the evaluation of the feedbacks given by a service consumer and then comparing them with the feedbacks of other consumers is carried out. The detail of the calculation of this attribute is described in IV-D2.

C. SOCIAL NETWORK MANAGER

Three types of social relations are considered in this research including i) Friends, ii) Social Contact, and iii) Community of Interest. These relations are also considered in [6]. The level of cooperation depends upon the authentication and authorization level granted by an owner to those in his social network. Four attributes are identified to keep the record of the recommendations made by social relations. These attributes are described in Table 6 which are stored locally in a service con-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2897095, IEEE Access

sumer's local database and act as a history. It helps a service consumer in identifying which recommender's recommendations are proved to be correct.

TABLE 6: Attributes of Social Network

Name	Description
CId	Unique identity for the social relation
CType	The type of contacts like a friend, CoI or Social Contact
RNo	The no of recommendations given by a contact
VR	The number of valid recommendations

The attribute 'CId' is the identity of a recommender whereas 'CType' describes the type of social relation. The service-seeker/service-consumer also keeps the record of total no of recommendations made by a recommender. A recommendation is considered valid if a service-seeker decides to consume that service and QoS is satisfactory. In future, the preference is given to the recommendations of those recommenders who have provided more valid recommendations in the past.

D. ATTACK MONITORING ANALYST

The Attack Monitoring Analyst of ARCA-IoT continuously monitors the entities. It separates dishonest entities from honest entities by identifying various attacks. In order to enable this analyst to do the assigned tasks, it is trained based on a Naive Bayes algorithm which is explained in V-A. However, feature scaling and categorization are done before training. Feature scaling and categorization is an important step which should be performed before the classification of entities. The need and the process of feature scaling are discussed in the subsection IV-D2. If an entity is proved to be untrustworthy, the Analyst assigns the level of untrustworthiness and then identifies the type of attack. If the entity appears to be trustworthy, then the record is updated accordingly. The details of the processes are described in the following subsections.

1) The Attributes and the Vectors

To identify any potential attack, the attributes mentioned in Table 7 are considered. These attributes are calculated with the help of input attributes which are mentioned in Table 4.

TABLE 7: List of Attributes

Attribute	Description	Type
F_i	Feedback for the feature i of a service	input
F_{ij}	Feedback given by service-consumer j for a feature i of a service	input
FS_{ij}	Feature scaling of the feedback given by j for a feature i	derived
μFB_i	Arithmetic mean of the feedbacks of a feature	derived
FC_{ij}	Feature categorization for the classifier	derived

Feedback for each attribute (also called 'feature') of a service is taken from a service consumer who consumes the service. The record of the feedback for each feature of a service is kept as F_i. The feedbacks about each feature is then used collectively to measure the overall quality of a service. Similarly, F_{ij} helps in evaluating the trustworthiness of feedback, for a feature, given by a service consumer. For this, a comparison is made with μFB_i. The details of FS_{ij} and FC_{ij} are described in the following sub-section IV-D2.

2) Feature Scaling and Categorization

Feature scaling helps in standardizing the features of data before using them in any machine learning algorithm. It is also called the normalization of data. It is important to standardize the range of features so that the objective function can be achieved. In ARCA-IoT, it is done using (1) as described in [25]. It scales the data in a range from 0 to 1.

$$FS_{ij} = \frac{(F_{ij} - Min(F_i))}{(Max(F_i) - Min(F_i))} \tag{1}$$

Where 'i' represents feature no and service consumer 'j's evaluation. The arithmetic mean of SP and SC is calculated separately. It will help in evaluating the trustworthiness of SP and SC separately which is elaborated in IV-D3.

1) The arithmetic mean of all the feedbacks for each feature of a service is calculated using (2).

$$\mu FB_i = \frac{1}{n}\left(\sum_{l=1}^{n} FS_l\right) \tag{2}$$

Where FS_l represents the feedback given for the feature i.

2) The arithmetic mean of the feedbacks of all the features of a service given by a SC 'j ' after consuming that service is calculated as described in (3).

$$\mu FB_j = \frac{1}{n}\left(\sum_{l=1}^{n} FS_l\right) \tag{3}$$

Where FS_l represents the feedback given by SC j.

After feature scaling, categorization of feedback given by SC 'j ' for each feature is carried out. Equation (4) compares the feedback given by 'j ' for the feature 'i ' and then assigns it the flag values as described in (4). If the difference between the mean feedback and the feedback given by SC 'j ' is 0 then it is assigned the value 1 i.e., trustworthy. If the difference between the mean feedback and the feedback given by SC 'j ' is ± 0.2 then it is assigned the value 0.75 because it a minor difference. However, if the difference is ± 0.4 then it is assigned the value 0.5 and 0.25 is assigned for ± 0.6. For a difference,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2897095, IEEE Access

greater than ± 0.6, it is assigned 0 which declares the entity as a dubious entity.

$$FC = \begin{cases} 1, \text{ if } FS_{ij} = \mu FB_i \\ 0.75, \text{ if } (FS_{ij} - \mu FB_i) <= 0.2 \;||\; (\mu FB_i - FS_{ij}) <= 0.2 \\ 0.5, \text{ if } ((FS_{ij} - \mu FB_i) > 0.2 \; AND \; (FS_{ij} - \mu FB_i) < 0.4) \;||\; ((\mu FB_i - FS_{ij} > 0.2) \; AND \; (\mu FB_i - FS_{ij} < 0.4) \\ 0.25, \text{ if } ((FS_{ij} - \mu FB_i) > 0.4 \; AND \; (FS_{ij} - \mu FB_i) < 0.6) \;||\; ((\mu FB_i - FS_{ij} > 0.4) \; AND \; (\mu FB_i - FS_{ij} < 0.6) \\ 0, \text{ Else} \end{cases} \tag{4}$$

Following five classes were defined to predict the levels of trustworthiness or untrustworthiness of the entities in ARCA-IoT. These help in identifying to which level an entity is trustworthy. Equation (5) reflects how much trust score is required to be trustworthy at an appropriate level.

1) Untrustworthy
2) Partially UnTrustworthy
3) Fairly Trustworthy
4) Good Trustworthy
5) Fully Trustworthy

$$TLevel = \begin{cases} \text{Untustworthy, if } T = 0 \text{ AND } T < 0.25 \\ \text{Partially UnTustworthy, if } T >= 0.25 \text{ AND } T < 0.5 \\ \text{Fairly Tustworthy, if } T >= 0.5 \text{ AND } T < 0.75 \\ \text{Good Tustworthy, if } T >= 0.75 \text{ AND } T < 1 \\ \text{Fully Tustworthy, if } T = 1 \end{cases} \tag{5}$$

Where T is calculated in (6).

$$T = \frac{1}{n}\left(\sum_{m=1}^{n} FC_m\right) \tag{6}$$

Where the mean of FC for all the features of a service is calculated after its consumption. By calculating the mean based on feedback categories, it becomes easy to assess the trustworthiness of both service consumer and the service provider. If T lies within the range of 0 and 0.25 then it is further evaluated if it an attack or not. The algorithms for the identification of various attacks are described in the following sub-section.

3) Algorithms for tackling three attacks

The algorithms to tackle three attacks, which are bad-mouthing, ballot-stuffing, and oscillation, are devised here.

1) Bad Mouthing: It is mentioned before that bad mouthing is carried out by service consumers. Whenever a required service is provided to a malicious or dishonest node. It deliberately provides bad recommendations for an honest service providing node. The purpose is to minimize the selection chances of that node. This behavior badly affects the trustworthiness concept. Therefore, the presence of such kind of dishonest nodes needs to be identified to run the system unbiasedly. For this, an algorithm 1 is proposed. As soon as a service consumer 'j' starts giving feedback about the features of a service consumed by it. The system compares the given feedback with the mean feedback of that feature if it is below than the mean feedback of the feature of that service then the feedback given by the service consumer 'j' is considered dubious. Then the system assesses whether it is a bad-mouthing attack or not. For this, it counts how many times the feedbacks, given by service consumer 'j ', are less than the mean feedbacks of the services consumed by 'j'. If the percentage of the lower feedbacks given by 'j' is greater than fifty percent of the total feedbacks of 'j' and the service consumer 'j' has given more than ten feedbacks then this service consumer 'j' is declared an entity which is involved in "bad-mouthing". The minimum threshold ten is considered so that newly entered service consumers can't be declared as malicious.

Algorithm 1 Assessing Bad Mouthing Attack

```
Get the value of μFB_i and FS_ij
if FS_ij < μFB_i then
    for each FS_ij < μFB_i in the past do
        count++
    end for
    if ( ( count/(total μFB) *100 ) > 50 ) AND ( total FB_j >10 ) then
        j= Bad Mouth
    else
        j = Not a Bad Mouth
    end if
end if
```

2) Ballot-Stuffing: Whenever a service consumer gives feedback after consuming a service, it tries to increase the good reputation of a service provider by providing an unfairly high rating. Hence, the presence of such kind of dishonest nodes in the system also brings imbalance to the system. To tackle this kind of behavior, another algorithm 2 is presented in ARCA-IoT. Whenever a service consumer 'j' gives feedback for a feature, it is compared with mean FB of that feature. If it is

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2897095, IEEE Access

greater than the mean feedback then the system considers this feedback as dubious. The system checks the history of feedbacks given by the service consumer 'j'. If fifty percent of the feedbacks given by 'j' is greater than the mean feedback of each feature of various services consumed by 'j' and the service consumer 'j' has given more than ten feedbacks then it is considered as "ballot-stuffer"entity.

Algorithm 2 Assessing Ballot Stuffing Attack

Get the value of μFB_i and FS_{ij}
if $FS_{ij} > \mu FB_i$ **then**
  for each $FS_{ij} > \mu FB_i$ in the past **do**
    count++
  end for
  if $\left(\left(\frac{count}{total \mu FB} * 100 \right) > 50 \right) AND \left(\text{total } FB_j > 10 \right)$ **then**
    j= Ballot Stuffer
  else
    j= Not a Ballot Stuffer
  end if
end if

3) Oscillation Attack: As mentioned in Table 2, this attack is related to service providers. The service provider creates a good reputation by providing quality services and then on and off, it provides bad services. To identify this, an algorithm 3 is used. It is based on punish and reward method. If any service consumer gives feedback lower than the mean feedback for this service provider and it is identified that this is not bad mouthing then the service provider gets punishment for providing a poor service. Hence, a service provider gets negative feedback for each low-quality service which is aggregated into its total trust score resultantly decreasing its good reputation. If a service provider provides good service and the feedback is higher than the mean feedback and if the service consumer is not a ballot-stuffer then positive feedback is aggregated in the service provider's trust score hence increasing the good reputation. In ARCA-IoT, the variable β is set to 5% which means 5% of the mean feedback of a feature of a service provider will be added to or deducted from mean feedback as a reward or a punishment. The purpose of setting the large value of β is to keep a service-provider careful in providing services. However, it can be adjusted to some other value as well.

The flowchart in Fig. 2 summarizes the evaluation process for the trustworthiness of the entities where information of both service providers and service consumers is analyzed first. A decision is made about the trustworthiness of both entities with the help of a Naive Bayes Classifier. If an entity is trustworthy then the categorization of trustworthiness is made. If it is assessed as non-trustworthy then the system categorizes the attack and takes appropriate action.

Algorithm 3 Assessing Oscillation

Get the value of μFB_i and FS_{ij}
if $FS_{ij} < \mu FB_i \; AND \left(\text{j} != \text{Bad Mouth} \right)$ **then**
  Punishment = - β *μFB_i
else if $FS_{ij} > \mu FB_i \; AND \left(\text{j} != \text{Ballot Stuffer} \right)$ **then**
  Reward= β * μFB_i
else
  Neither reward nor punishment
end if

V. EVALUATION OF SMART TRUSTWORTHINESS IDENTIFICATION

The efficiency of the proposed model is demonstrated with a specifically designed simulated environment. In addition, a qualitative analysis based on parametric metrics is also carried out.

Two groups of experiments were conducted.

1) Group A: In this group of experiments, bad-mouthing attacks were carried out by a group of service consumers
2) Group B: In these experiments, ballot-stuffing attacks were carried out to assess the performance of ARCA-IoT.

A specifically designed environment was implemented in .NET platform which is explained below.

1) Public Cloud: Microsoft Azure was used as a public cloud where Resilient Agent resides. In addition, REST APIs along with training data are also deployed here.
2) Service Consumer: It plays the role of a service seeker and seeks a service provider. After that, it gives feedback. Keeping in view the types of attack models, three types of service consumers are implemented. 1) Honest service consumers 2) Service consumers for ballot-stuffing 3) Service consumers for bad-mouthing
3) Service Provider: This entity plays the role of a service provider. Two types of service providers are implemented. 1) Honest service providers 2) Service providers for oscillation attack
4) Social Entity: This is also called recommender entity as explain in IV-C. It supports in conducting the experiments.

A. TRAINING THE MODEL

A dataset [26] was used for training the model so that it can differentiate between trustworthy and un-

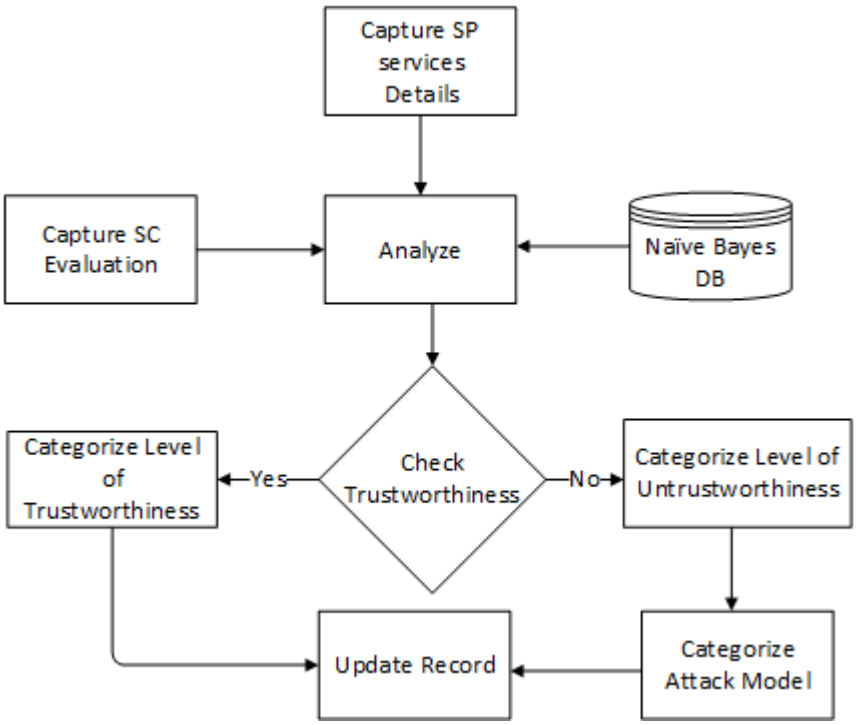

FIGURE 2: Flowchart of the proposed model for trustworthiness

trustworthy 'things' . Since the capacity and time attributes of context level were not present in the dataset, therefore, the values of capacity and time were generated randomly in the dataset. Initially, the system was trained using Naive Bayes Algorithm on 338*1000 matrix which is the evaluation for 1000 services by 338 service consumers. The evaluations of QoS constraints (throughput and response time) by service consumers are statistically normalized within the range of 0 and 1 using (1). Each evaluation for each QoS constraint is then categorized using (4) to assess the trustworthiness of service consumers and service provider as well. By categorizing each evaluation, it will be easy to calculate the trustworthiness of SC and SP using (5).

The Naive Bayes Classifier works on the assumption that a feature present in a class is not related to other features present. It is significant to note that all the properties contribute independently to the probability no matter if the features depend on each other. Equation for Naive Bayes is (7) where c represents the class of trustworthiness and f reflects the feature. The probabilities for each factor given the category of trustworthiness are calculated. The data is then adjusted with Laplacian smoothing (8) so that zeros become more or less arbitrary small values as the observed zeros are wrong, therefore, there is a need to adjust them using a priori knowledge.

$$P(c|f) = \frac{P(f|c)P(c)}{P(f)} \tag{7}$$

$$P(f|c) = \frac{count(f \,\&\, c) + 1}{count(c) + no\ of\ classes} \tag{8}$$

The process of Naive Bayes is summarized in Fig. 3. After feature selection in Phase I, preprocessing is done on raw data using mathematical models mentioned in IV-D2. After categorizing the dataset, Naive Bayes classifier classifies the training dataset. The classifying model is then tested on testing data. Finally, the model is prepared to predict the trustworthiness of the entities. Initially, two QoS attributes throughput and response time are considered whereas for simplicity, capacity and time are defined in three categories. The service capacity of a service provider is considered as low, medium and high. The service timings are morning, noon and evening.

B. PERFORMANCE METRICS

To assess the effectiveness of a proposed model for a classification problem of machine learning, the confusion matrix is one of the intuitive metrics used for this purpose in related approaches [9]. This matrix, which is shown in Table 8, is used for evaluating the accuracy of ARCA-IoT. An entity is either trustworthy or untrustworthy. For simplicity, the classes defined in section IV-D2 are here considered as two main classes. For this, TLevel less than 0.5 is considered as untrustworthy and greater than or equal to 0.5 is considered

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2897095, IEEE Access

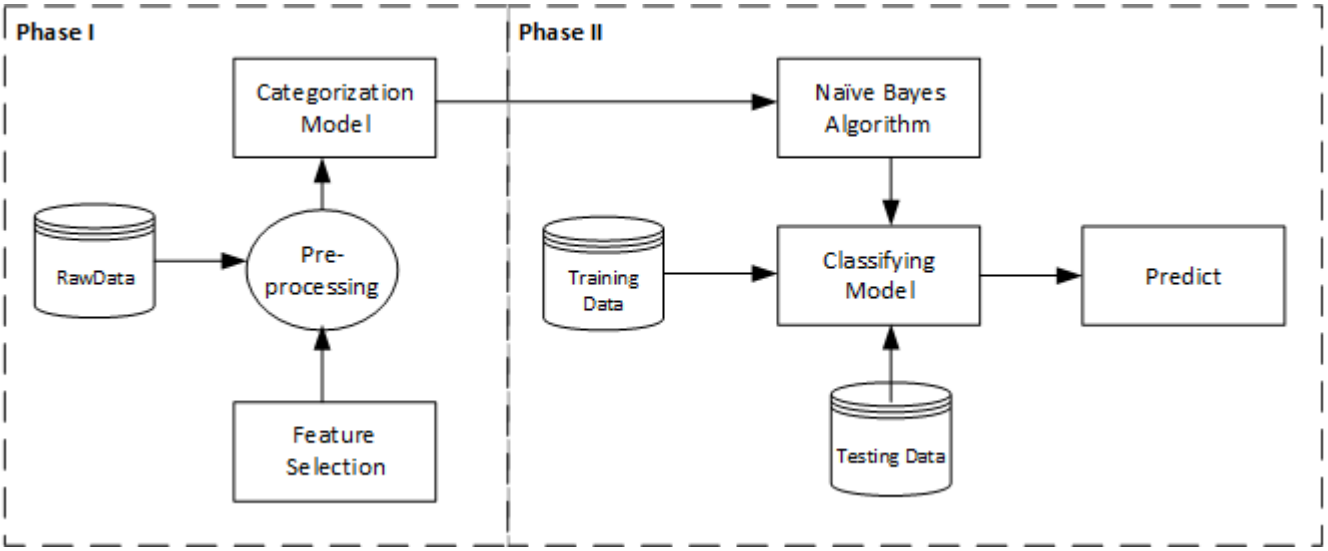

FIGURE 3: Naive Bayes Training

TABLE 8: Confusion Matrix

	Anticipated		
Actual		Trustworthy	Untrustworthy
	Trustworthy	TP	FN
	Untrustworthy	FP	TN

as Trustworthy. Following terms are used to define the confusion matrix as described in [27].

1) True Positive (TP): When an entity is actually honest and ARCA-IoT also classifies it as dishonest.
2) True Negative (TN): When an entity is actually dishonest and ARCA-IoT also classifies it as dishonest.
3) False Positive (FP): When an entity is actually dishonest but ARCA-IoT classifies it as honest.
4) False Negative (FN): When an entity is actually honest but ARCA-IoT classifies it as dishonest.

Diab et al. [28] refer a commonly used performance metrics to represents results in machine learning. The description of these metrics is given in Table 9.

TABLE 9: Performance Metrics

Metric	Description	Details
Accuracy	$\psi = \frac{TP+TN}{TP+TN+FP+FN}$ (9)	measures correctly identified entities
Sensitivity	$\eta = \frac{TP}{TP+FN}$ (10)	measures correctly identified trustworthy entities
Specificity	$\rho = \frac{TN}{TN+FP}$ (11)	measures correctly identified unstrustworthy entities
Precision	$\pi = \frac{TP}{TP+FP}$ (12)	measures actual trustworthy w.r.t all entities specified as postive
AUC	$AUC = \frac{\eta+\rho}{2}$ (13)	plots η on y-axis, and complement of ρ on x-axis

C. EXPERIMENTS

Two types of experiments based on two scenarios are carried out.

1) Scenario 1

In this scenario, the requests for the required services are put up in the system by the group of services seekers. With the requests, the service consumers also enter the required service type, service timing, and capacity. ARCA-IoT suggests those top-quality service providers which match the criteria of the service seekers. For this, ARCA-IoT checks the database of the service seekers and also sends the requests to the social circle of the service seekers. After getting the suggestion from ARCA-IoT, service seekers consume the required services and then give feedback as service consumers which in this scenario are the bad-mouth and honest entities. The system evaluates the feedback everytime it is given by a service seeker whether it is honest or not. Fig. 4 shows trust estimation Accuracy for measuring correctly identifying the entities including Bad-Mouth. Fig. 5 depicts to which extent ARCA-IoT identifies trustworthy entities with respect to all positive entities. Similarly, Fig. 6 reflects the assessment of correct identification of trustworthy entities which is also known as Recall. Fig. 7 shows to which extent ARCA-IoT recognized the Bad-Mouthing Entities. The graphical assessment for AUC is displayed in Fig. 8. The results of this scenario show that ARCA-IoT has successfully identified the honest

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2897095, IEEE Access

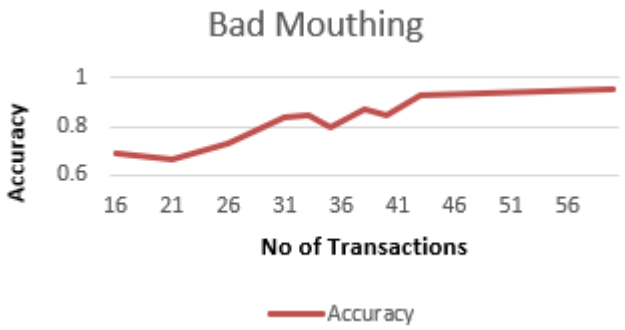

FIGURE 4: Trust Assessment Accuracy for Bad Mouthing

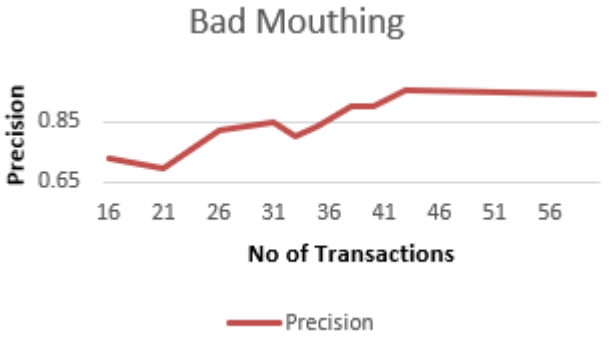

FIGURE 5: Trust Assessment Precision for Bad Mouthing

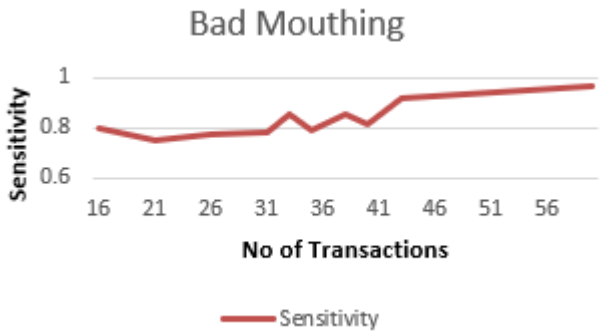

FIGURE 6: Trust Assessment Sensitivity for Bad Mouthing

and dishonest entities. The performance improves as soon as the number of transaction increases.

2) Scenario 2

After getting suggestions, in the way used in Scenario 1, from ARCA-IoT service consumers give feedback about the quality of the services. In this scenario, the ballot stuffing entities take part. Fig. 9 - 13 display the performance metrics for ARCA-IoT based on its assessment for Ballot Stuffing. The metrics show that the per-

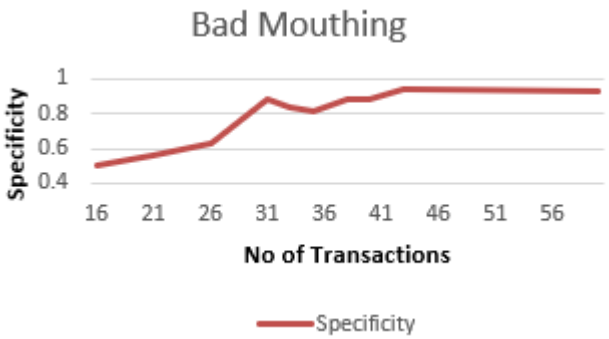

FIGURE 7: Trust Assessment Specificity for Bad Mouthing

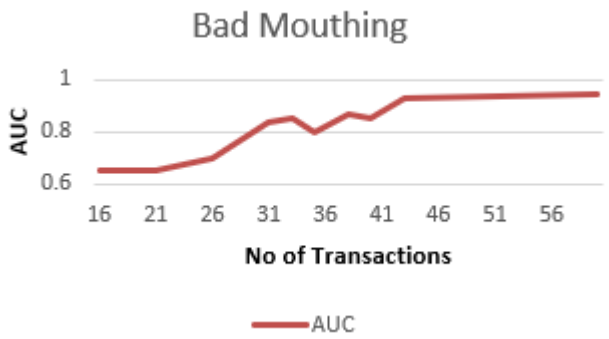

FIGURE 8: Trust Assessment AUC for Bad Mouthing

formance reaches to higher score after few transactions which in short display that ARCA-IoT has successfully identified the malicious and dubious acts of Ballot stuffer which it learns from the proposed Naive-Bayes model. It is observed that ARCA-IoT achieves higher accuracy score as soon as the number of transactions increases depicting in Fig. 9. Precision which is also

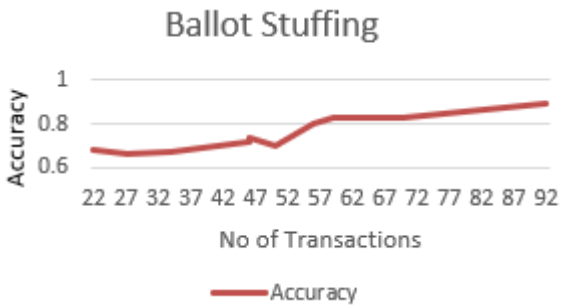

FIGURE 9: Trust Assessment Accuracy for Bad Mouthing

known as Positive Predictive value is displayed in Fig. 10. The sensitivity which is also called True positive rate and Fig. 11 shows the rate of identification of positive entities increases when the no of transaction increases.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2897095, IEEE Access

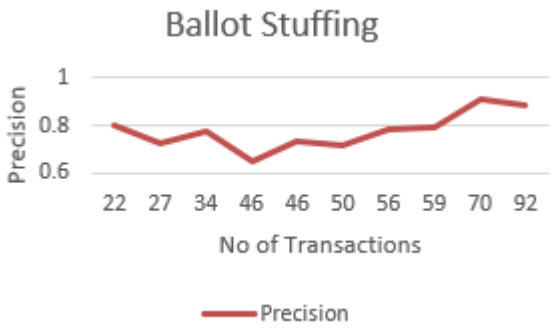

FIGURE 10: Trust Assessment Precision for Bad Mouthing

Similarly, the rate of identification of negative entities

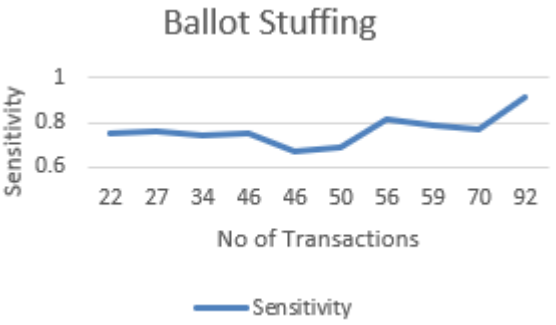

FIGURE 11: Trust Assessment Accuracy for Ballot Stuffing

also increases after a few numbers of transactions as shown in Fig. 12. Fig. 13 displays the performance

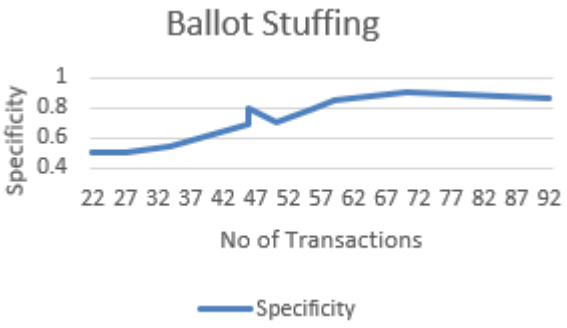

FIGURE 12: Trust Assessment Accuracy for Ballot Stuffing

of ARCA-IoT by testing the classifier over a range of sensitivities/specificities.

For oscillation attack, it is identified whenever a service provider does not provide quality service and ARCA-IoT evaluates that the service consumer is not a dishonest entity then it successfully applies the punishment and reward criteria defined in Algorithm 3.

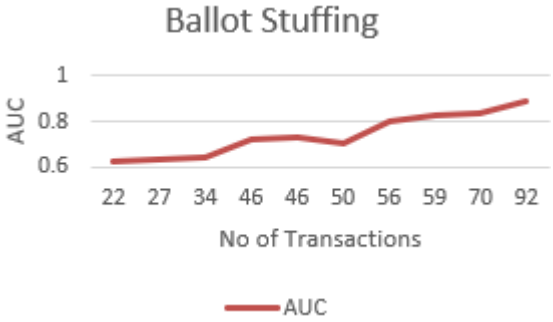

FIGURE 13: Trust Assessment Accuracy for Ballot Stuffing

D. COMPARISON WITH EXISTING SYSTEM

The comparison of ARCA-IoT with related trust management system is carried out in Table 10. The key criteria which contribute to the novelty of ARCA-IoT are considered here for the comparison. It is fair to say that to the best of our knowledge, there was a lack of system in related work that considers all of the mentioned criteria. Interoperability which is a major issue in the way of growth of IoT as described in [3] has not got much attention of the researchers. People pay for services and in return expect quality service from service providers. It can be said that not considering the QoS attributes specifically related to IoT in trust management is really a matter of concern. This is the reason, trust management in ARCA-IoT has focused on these attributes. Trusting on someone who is unknown is not easy, therefore, it is better to take recommendations from the social network and this area is in the limelight of the research community. That is why it is not ignored in ARCA-IoT. Context Awareness specifically related to IoT is less considered in state of the art. ARCA-IoT has made it sure by the contribution of new attributes in literature. In the absence of human interaction where 'things' autonomously communicate with each other, these 'things' must be capable enough to make a human-like wise decision so that malicious entities present in the network can be avoided.

VI. CONCLUSION AND FUTURE WORK

In this paper, three challenges faced by IoT world are discussed which are interoperability, scalability, and trustworthiness. A solution called ARCA-IoT is proposed to take up these challenges. ARCA-IoT leverages the concept of the cloud and the Web technologies for the facilitation of interoperability and scalability. Serving 'things' named SP make use of web services and provide services to service seeking entities. For trustworthiness, it is identified that trust is dynamic in context. Therefore, ten context related attributes for SP are considered in the proposed system to make the system context aware for providing the service.

TABLE 10: Comparison with related systems

Prev Work	Interop.	Scalability	QoS Attributes	Social Recommender	Context Aware	Human-like Decisions
[6]	Yes	No	No	Yes	No	No
[10]	No	No	No	Yes	Yes, but not specific to IoT	Yes
[11]	No	No	No	No	No	Yes
[12]	No	No	No	No	Yes	No
[13]	No	No	No	No	Yes	No
[14]	No	No	Yes	Yes	No	No
[15]	No	No	Yes	No	only capability, type	No
ARCA-IoT	Yes	Yes	Yes	Yes	Yes	Yes

Besides this, the attributes for maintaining the quality of service are also identified. However, it is discovered that malicious and dishonest entities try to maneuver the trustworthiness level of others. To intercept their attacks, Naive Bayes classifier along with three proposed algorithms are integrated into the system. Experimental results show that ARCA-IoT has successfully identified such entities. This is proved through performance metrics that the results are quite successful. Moreover, the comparative analysis based on parametric metrics also reflects the novelty of the proposed system.

In future, the resilience against more attack models will be incorporated into the system. More attributes related to context awareness and quality of service will be identified to establish trustworthiness in cloud-assisted IoT environment.

REFERENCES

[1] L. Tan, and N. Wang, " Future internet: The internet of things", In 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), Vol. 5, pp. V5-376. Aug 2010, IEEE.

[2] S. Javaid , H. Afzal, F. Arif and N. Iltaf, Trust management for SOA based social WoT system, *IEEE 20th International Conference on Advanced Communication Technology (ICACT)*, 2018 Feb 11, (pp. 387-392).

[3] Interoperability and the Internet of Things, NDP Analystics, Washington, USA: Univ. Dec, 2017. [Online]. Available: www.ndpanalytics.com/s/Interoperability-and-IoT-120617-Final.pdf

[4] D. Guinard, V. Trifa, and E. Wilde, "A resource oriented architecture for the web of things", ' IEEE Internet of Things (IOT), Nov, 2010.

[5] A. Kamilaris, "Enabling smart homes using web technologies", PhD Thesis, 2013.

[6] R. Chen, J. Guo and F. Bao, "Trust management for SOA-based IoT and its application to service composition", IEEE Transactions on Services Computing, vol 9, pp. 482-495, 2016.

[7] D. Guinard, A web of things application architecture: Integrating the real-world into the web, 2011, ETH Zurich.

[8] A. Botta, W. De Donato, V. Persico, and A. PescapÃľ, "Integration of cloud computing and internet of things: a survey", Future Generation Computer Systems, 56, pp.684-700, 2016.

[9] S. Javaid , H. Afzal, F. Arif and A. Majeed, "Reputation Management System for Fostering Trust in Collaborative and Cohesive Disaster Management", International Journal of Advanced Computer Science and Applications, Vol 7, pp. 347-357, 2016

[10] G. D Angelo, S. Rampone, and F. Palmieri, , "Developing a Trust Model for Pervasive Computing Based on Apriori Association Rules Learning and Bayesian Classification", Soft Computing, 21(21), pp.6297-6315, 2017, Springer.

[11] A. Mehmood, M. Mukherjee, S.H Ahmed, H. Song and K.M Malik, NBC-MAIDS: Naive Bayesian classification technique in multi-agent system-enriched IDS for securing IoT against DDoS attacks". The Journal of Supercomputing, pp.1-15,2018.

[12] C. Perera, A. Zaslavsky, P. Christen and D. Georgakopoulos, "Ca4iot: Context awareness for internet of things", IEEE International Conference on Green Computing and Communications (GreenCom), pp. 775-782, 2012.

[13] K. Rostamzadeh, H. Nicanfar, N. Torabi, S. Gopalakrishnan and V.C. Leung, "A context-aware trust-based information dissemination framework for vehicular networks", IEEE Internet of Things Journal, vol 2, pp. 121-132, 2015. IEEE.

[14] J.B. Bernabe, J.L.H. Ramos and A.F.S Gomez, "TACIoT: multidimensional trust-aware access control system for the Internet of Things", Soft Computing, vol 20, pp. 1763-1179, 2016, Springer.

[15] Y. B. Saied, A. Olivereau, D. Zeghlache, and M. Laurent, "Trust management system design for the internet of things: A context-aware and multi-service approach", Computers & Security, 2013.

[16] J. Delsing, J. Eliasson, J. van Deventer, H. Derhamy, and P. Varga, "Enabling IoT automation using local clouds", *In IEEE 3rd World Forum on Internet of Things (WF-IoT)*, pp. 502-507, Dec 2016, IEEE.

[17] I. Farris, L. Militano, M. Nitti, L. Atzori, and A. Iera, "Federated edge-assisted mobile clouds for service provisioning in heterogeneous IoT environments. In Internet of Things (WF-IoT)", IEEE 2nd World Forum on (pp. 591-596). Dec. 2015, IEEE.

[18] C. Stergiou, K. Psannis, B.G. Kim, and B. Gupta, "Secure integration of IoT and cloud computing", *Future Generation Computer Systems*, 78, pp.964-975, 2018.

[19] A.R. Biswas and R. Giaffreda, " IoT and cloud convergence: Opportunities and challenges", *In 2014 IEEE World Forum on Internet of Things (WF-IoT)*, (pp. 375-376), Mar, 2014, IEEE.

[20] M. Deutsch, "Cooperation and trust: Some theoretical notes", Nebraska University Press In Jones, M. R. (ed), Nebraska Symposium on Motivation, 1962.

[21] P. Hasan, "Privacy Preserving Reputation Systems for Decentralized", Institut National des Sciences Appliquees de Lyon, 2010.

[22] A. Josang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision", Decision support systems, Elsevier, vol. 43, no. 2, pp. 618–644, Mar. 2007.

[23] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the internet of things: A survey", *IEEE communications surveys & tutorials*, 16(1):414- 454, 2014.

[24] L. Garces, A. Ampatzoglou, P. Avgeriou and E.Y. Nakagawa, "Quality attributes and quality models for ambient assisted living software systems: A systematic mapping", Information and Software Technology, 82, pp.121-138. 2017

[25] I.B. Mohamad, D. Usman, "Standardization and its effects on K-means clustering algorithm", Research Journal of Applied Sciences, Engineering and Technology, pp.3299-3303, 2013.

[26] WS-Dream Team, "Towards open source Datasets", 2018, [Online]. Available: http://wsdream.github.io/

[27] S. Turgut, M. Dagtekin and T. Ensari, "Microarray breast cancer data classification using machine learning methods", In 2018 Electric Electronics, Computer Science, Biomedical Engineerings' Meeting (EBBT,) (pp. 1-3). April, 2018, IEEE.

[28] S. Diab and B. Sartawi,"Classification of Questions and Learning Outcome Statements (LOS) Into Blooms Taxonomy (BT) By Similarity Measurements Towards Extracting Of Learning Outcome from Learning Materia", 2017, arXiv preprint arXiv:1706.03191.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2897095, IEEE Access

SABEEN JAVAID is a PhD scholar in Department of Computer Software Engineering at Military College of Signals, National University of Sciences and Technology (NUST), Islamabad, Pakistan. She holds a MS degree in Computer Software Engineering from NUST, Pakistan. Her research interests include web services, trust management, Web of Things and Internet of Things. She is also an IEEE member. She is also the recipient of IEEE outstanding volunteer award.

DR. HAMMAD AFZAL is currently heading The Center of Data and Text Engineering and Mining (CoDTeEM) group at NUST. His primary interests are machine learning, text and data mining systems. He completed PhD from School of Computer Science, University of Manchester, UK in Dec, 2009 under supervision of Dr. Goran Nenadic in Text Mining Group. Before PhD, he completed MSc in Advanced Computing Sciences from University of Manchester, UK where he was awarded Program Prize of the year from Department of Computation for acquiring highest grades in MSc courses. He has also been affiliated with Digital Enterprise Research Institute (DERI), National University of Ireland, Galway as a Research Assistant from July, 2009 to Dec, 2009.

DR. MUHAMMAD BABAR completed his PhD at Signals College of National University Sciences and Technology (NUST), Islamabad, Pakistan. He did his Masters of Sciences from National University Sciences and Technology (NUST), Islamabad, Pakistan in 2012. He receives his Bachelors in Computer Sciences with distinction from University of Peshawar, Pakistan in 2008. His research area includes but not limited to Big Data Analytics, Internet of Things (IoT), Smart City Design and Planning, and Social Web of Things (SWOT). He has published his research work in various IEEE, Elsevier and ACM/Springer International reputed journals.

PROF DR. FAHIM ARIF receives his Bachelors in Telecommunication from College of Telecommunication Engineering (UET Lahore) in 1995 and Master in Sciences in Computer Software Engineering from National University Science and Technology, Islamabad in 2003. He has won NUST Endowment fund scheme scholarship for NUST in 2003 and International Research Support Initiative Program Fund from HEC in 2007. He worked as international research scholar in System and Computer Engineering Department, Carleton University, Ottawa, Canada in 2007 and participated in numerous research and academic activities. He is principal investigator (PI) for a project funded by NUST. Recently, his biography has been published by South Asian Publication Who's Who in the World 2008 Edition and awarded with Star Laureate 2008 in recognition to his contributions to knowledge and research.

ZHIYUAN TAN is a Lecturer at the School of Computing at the Edinburgh Napier University. He was awarded his PhD degree by University of Technology Sydney, Australia in 2014. Prior to joining Edinburgh Napier University, he had been a postdoctoral researcher at the University of Twente since2014. Zhiyuan has a research background in network security and pattern recognition. Zhiyuan has published over 40 quality scholarly articles. His most recent research achievements have been published in several highly-cited IEEE Transactions and Elsevier journals including IEEE Transactions on Computers (TC), IEEE Transactions on Parallel and Distributed Systems (TPDS), IEEE Transactions on Cloud Computing (ToCC), Future Generation Computer Systems (FGCS), and Computer Networks (CN). His research contribution on network security is internationally recognized. According to Google Scholar, he has an H-Index of 13 and his research articles have received over 830 citations since 2010. Moreover, he has earned various research awards, including the National Research Award 2017 (The Research Council of the Sultanate of Oman), and IEEE Outstanding Service Award, over the past years.

DR. MIAN AHMAD JAN completed his PhD at the Faculty of Engineering and Information Technology (FEIT) of the University of Technology, Sydney (UTS). His research interests are on Wireless Sensor Network Clustering Protocols, Congestion Control, Internet and Web of Things and efficient Network Intrusion detection techniques. He has published his research in top ranked Elsevier, IEEE Transactions and Conference in these areas of research. He has been recipient of various research awards such as UTS International Research Scholarship and CSIRO Top-up scholarship. Besides, he was awarded the best researcher award for the year 2014 at the University of Technology, Sydney Australia. After completing PhD, he has joined Abdul Wali Khan University Mardan, Pakistan as Assistant Professor in March 2016.