Secured Service Discovery for Internet of Things: Context Awareness Perspective

K.Sakthidasan @ Sankaran, N.Vasudevan and V.Nagarajan, *Senior Member, IEEE*

***Abstract*— The up growing trend is Internet of Things (IoT) is the functional devices that encapsulate the services in the real world and interact with other web services to understand the seamless physical integration in the world; here the service discovery plays the vital role. Service discovery require much selection process, e.g., availability of device, positioning, service discovery of content and block of IoT are used for the reliable user-centric and provision environment. Two approaches are used in the proposed system for service discovery they are Web service discovery and Smart service discovery for context-aware perspective. Finally, the trustworthiness of services' providers is maintained by the Trust Evaluation model.**

***Index Terms*—Context-aware, Internet of Things, Smart service discovery, user-centric, Web Services**

I. Introduction

THE IoT vision is to incorporate flawless substantial world along with the digital world. It provides the platform to communicate with the environment and other things that include data exchanging and information sensing among the surroundings. When the autonomously are reacting to the world events it should be authoring one. The process is been triggered by running the action that provides the intervention of the visual based service among the human. The concept of this is to design the user oriented and awareness service. It also has the sensitive form to require the presence of the environmental terms and condition [1].

Initially, in the services under the real world, are been able to provide the environmental devices, which are accessing in the physical world. The traditional web services are wholly said to be virtual entities that also encapsulate the business logic. And it is real-world services that are able to organize the resource-constrained devices; they are also providing a limited computing capability, lower bandwidth of network and storage ability. It is similar to web service, which is more frequently found in the oscillation environments where the devices are fundamental. Whereas it constantly degrades, vanish and reappear the possible, because of the intermittent wireless disconnection on the network that is a wireless network, changing, having the bigger device resources thus it accurate the web based service on this constant approach [2].

Commonly, the protocol used for this service discovery must guarantee the performance reliable under certain way where they are likely to be maintain the scalability, fault tolerance, and the important thing is it in-corporate the poor resource devices. The service discovery in IoT is one of the approaches that are having the following services such as fault tolerance, mobility support and integration that are in the poor resource devices which is one of the open challenges at the same time. The important issues are arranged to focus on the existing protocols which provide the customization for IoT Technology. It also provides new functionality and maintains poor resource devices [3-5].

The proposed method is on the bases of the discovery and also it have the development in the high range of the environment and also it reacts with the user-centric and also deals with the situation awareness of the user request. This paper aims to be developed for discovery of service in the context-aware for IoT.

The rest of the paper is organized as follows Section II is the discussion about the Literature Survey and Section III is the proposed method for service discovery in IoT and followed by it Section IV is the Performance Metrics included for the IoT services and Finally, Section V is the Conclusion part of this paper.

II. Related Works

IoT characteristics are having some problems regarding the context-aware technologies for IoT where it has three categories such as context acquisition, modeling and reasoning. In the calculation of current context-aware system architecture are made with some purpose to define a concept named as "context of things", towards the context improvement for QoS –aware (Quality of Service) so the novel REST full Web based things are been developed based on environment [6]. The main requirement for this specification of service through IoT is done by RFID technology, where they are used for the context awareness, on a wide converge to IoT architecture [7].

The requirement for the IoT is having certain challenges for

K.Sakthidasan @ Sankaran is with Department of Electronics and Communication Engineering, Hindustan Institute of Technology and Science, Chennai (phone: +91-8056490436; e-mail: k.sakthidasan.1983@ieee.org).

N.Vasudevan is with Department of Electronics and Communication Engineering, Hindustan Institute of Technology and Science, Chennai (email:devasudevan3@gmail.com)

V.Nagarajan is with Department of Electronics and Communication Engineering, Adhiparasakthi Engineering College, Melmaruvathur (e-mail: nagarajanece31@gmail.com).

978-1-7281-4988-2/20/$31.00 ©2020 IEEE

the service discovery for the internet, in the future they are able to support the number of maintains that includes the scalability, security, etc., for the reliable trust. The system is able to build the context-aware service that is based on context-aware the service-oriented architecture, where the extension is done for the following ontology-based model. It represents the uncertain contexts and they are implemented by the Bayesian Network (BNs). It also merges the IoT characteristics, where they are used for designing. The contexts are more useful for the uncertain way where the several ways of the resources are been generate by the user-centric environment over the IoT [9].

In [10] the author has introduced a scalable self-configuring to communicate. The communication is based on take in the architecture under a higher scale of IoT networking, the goal is to provide a discovery based on the automated service and resource method, which enables the configuration without human intervention. Thus, it works on service discovery (SD) on locally and globally having the independent operation view. From this the IoT service are having the distance from the CoAP to run the middleware approach in the service oriented way for the betterment of the connection done on the network to the provider. Thus, the main deal of this middleware sensor is to enables a reliable connection through the layer of the sensor. It uses the application layer on the OSI model to provide the service and ensure effective communication among the different types of software.

The services under the IoT are having the dynamic environment on which the services are steady degraded, disappearance and reappearance, etc., it also make a trend of the data which are having the abnormal and non consistent. The different types of this observed solution given for this type of issue is very limited and imperfection, in order to consider the additional Quality of Context (QoC) knowledge to gain the metadata, eg., accuracy, up-to-date it gives the better characteristic to acquire the data. Thus, the additional information is relevant and they can pass through the argument and procedure on service discovery. It shows the better way of the decision- making and also performs the action to enables the filter to acquire more irrelevant data in the context and also it has insufficient quality, it also ranks which information should be used [10].

In most cases, the service discovery is having the decidable approach that is not been addressed the requirement of IoT services. It also has services that are in difference IoT and also it has the web traditional services that are uniformly having a web rich description about their functionality it looks like a straightforward method. The semantic web technologies like OWLS provide the communication and also it uses the whole formats which are more suitable for the consideration of the environment and discovery of models. They are more extended and also it has the attributes of heavyweight service description. On the other way, the Rest style provides a lightweight service requirement. The properties are basically related to Spatio-temporal features and also it includes them in some way but also it must be able to give the sufficient and guarantee of service and the availability. Thus the new way of IoT on service is been described and its needs are done in an optimal manner [8].

III. PROPOSED METHOD

In this part the service are oriented regarding the IoT that are using the basic set of devices which are been having the specific categories of devices. It obtains the available IoT service for all users who have are lead to be disposal for the required. To generate the IoT services the dissimilar way of devices are been obtained among the user should acquire different types of devices. It requires an IoT that is identifiable definitely. The automated way of generating the service discovery is to recognize togetherness of the IoT service devices and accessibility for the user. They are two protocols for service discovery they are mDNS Multicast Domain Name Service and DNS. The proposed method for context modeling is classified by schemes of data structure that are used for exchanging contextual information to the respective system. The proposed context-awareness supports both the modeling and reasoning with respect to timestamp. A Dynamic Bayesian network (DBN), is used to support the context which is the extension of BNs. The BNs are the graphical model that represents the Directed Acyclic Graph (DAG) where it denotes the set of objects and events exists under the actual world. Whereas the DBN is holding the temporal devices s consist of temporal features. Figure 1 illustrates the process block diagram of the proposed method.

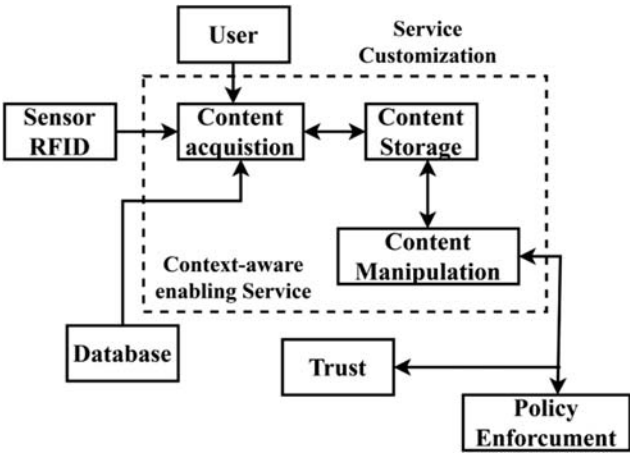

Fig.1.Process Block of the Proposed DAG based Trust System

They are formed defined as the pair (B0,B), where B0 is represented as the probability of prior P (Z1 1), and B represents the double slices (i.e., intra slice and inters lice) the probability distribution for temporal Bayesian network are as follows:

$$P\left(\frac{Z_t}{Z_{t-1}}\right)=\prod_{i-1}^{N} P\left(\frac{Z_t^i}{P_a(Z_t^i)}\right) \quad (1)$$

Z_t^i, represent san i[th] devices of time slice t; it is in the

hidden state or observation state. Where $P_a(Z_t^i)$ is the parent devices of Z_t^i, it relies on the similar time interval t or a preceding slice of t-1.

Each context predicate is mapped with the devices of DBN. After the DBN identifies the set of uses at the present state, and the event are been triggered and the service are invocate. It carries out the action of the event, or separately makes available of smart service for the user. The discovery of the context-aware service supplies a communications that are to be in the well-organized to smart web service provided in IoT. The three components are mainly used for this approach are as follows:

1.Context Acquisition: It collects the contextual information from the heterogeneous platforms, eg., profile to be considered by the user, intellect data, tagged information of RFID- things, and devices description.

2. Context Knowledgebase: It is mentioned to be derived from the low to higher set of model that includes the context in addition with the adding, altering and query charactestics.

3. Context Reasoner: It provides the service from low level to high-level contexts and also it maintains the knowledgeable context and determines the disagreements regarding the context. The DBN is used for the reason for uncertain context and sequential quality.

Service Repository- here the web services are been used under the real-world and also it maintains the repository, thus they are used for the various set of parameters used under the single class as the service in abstract. It also monitors the repository and also maintains the service information up to date.

Event detection and service provision- the concept of using is to the reliable dynamic environment for the IoT condition. The components represents the events that are to be occurred and also they are includes the stable service to the QoS value. It also acquires the traditional web services which are been composed.

The service taken in this proposed system is the web based discovery done on the context-aware which are named as the user context that includes the position of the device and the human. The other way is done on the second set of approach where it uses the smart discovery of service in case of the request of the hidden knowledge and the gathering of the context. They identifies the present state of the service to be requested and also generates the changes in dynamic environment and also to the capability of the user. Both the trust and the mechanism for this reputation are been considered on the consumer side to exhibit the optimal set of service for the authentic one and unauthentic ones.

Reputation, Experience, and Knowledge (REK) is a Trust Evaluation Mode. The trust indicator is knowledge base and there isa partial form of trust that is having the limited information about the trustee as well as the environment. Formula 1 is the calculation of trust in the IoT service. The IoT service discovery is having two classes they are Active and Passive class.

$$T_A^B = \delta\left[Rep_B\right] + \rho\left[Exp_A^B\right] + \sigma\left[Kn_A^B\right] \quad (2)$$

Where T_A^B is the trust value of B which is perceived by A and δ, ρ and σ are the three-parameter that are picked up from a certain interval of time.

Active- The active attackers (users) are willing to get the information by sending the queries for a service. The queries include the presence service instances, extract the version number from the TXT records, and recognize the vulnerable versions and attacks the communicating hosts. To make someone connect the user can also offer the fake service.

Passive- the passive attackers want to get more information that is possible by just listening to multicast traffic. The plaintext of the information is gained by these attackers.

IV. Performance Metrics

A. Trust

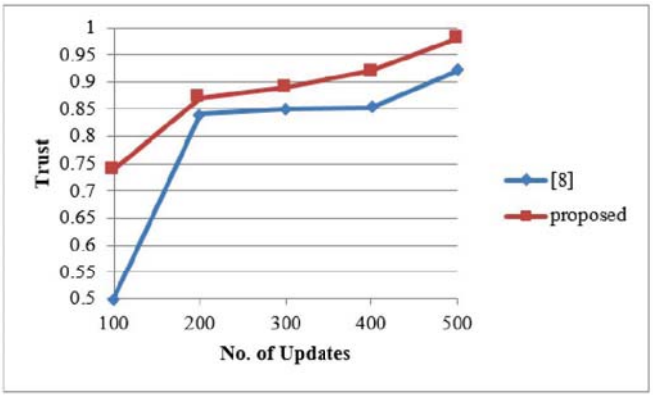

Fig.2. Trust Analysis

In Figure 2, the trust estimated from the varying updates is compared with the method in [8]. Using Bayesian classification the devices are updated with their trust from the recent update based on the transmission observed in the previous time state. This helps to update the trust in a periodic manner, reducing the impact of malicious devices in the communication process.

B. Packet Delivery Ratio

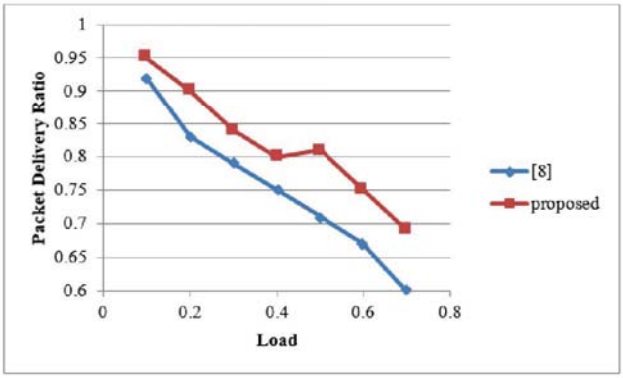

Fig.3. Packet Delivery Ration Analysis

As the detection of malicious devices is spontaneous, the

network load is disseminated in a consistent manner, without loss. This helps to retain the throughput of the network, achieving high packet delivery ratio (Figure 3).

C. *False Positive Rate*

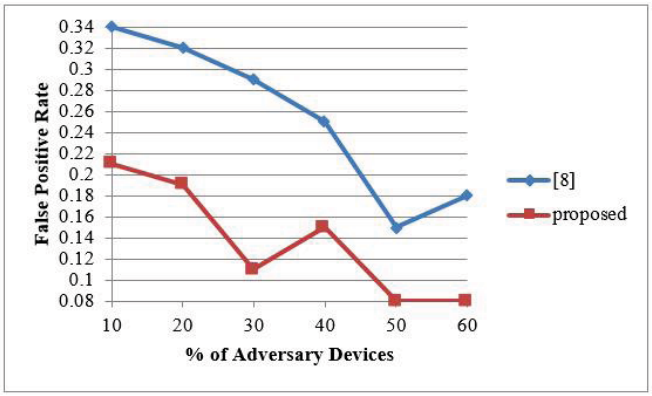

Fig.4. False Positive Rate Analysis

In Figure 4, describes the rate under the false positive for the proposed and existing method in [8] is compared. As the detection is instantaneous using the Bayesian classification, the detection of malicious devices are performed at ease, achieving less false positive rate.

V. CONCLUSION

In this paper, the context awareness is done by the service discovery on IoT. The proposed method is designed to acquire the effective way of user-centric and the awareness regarding the provision of service. It also addresses minimal human intervention in a highly dynamic environment. The model which is used for the ontology are indicating the representation and uncertain of the Sequential quality that is modeled in the proposed DBN to the contexts related to the time series on the bases of the data streams on the present situation. The service provider gives the trust obtained by the REK evaluation method. The performance metrics show that the proposed system works well when compared to the previous methods.

REFERENCES

[1] Zeng, D., Guo, S., and Cheng, Z. 2011. The Web of Things: A Survey. Journal of Communications, 6, 6 (Sept. 2011), 424-438. DOI= 10.4304/jcm.6.6.424-438.

[2] Krishnan Sakthidasan, Natarajan Vasudevan, Parameswarane Kumara Guru Diderot; Chellakkutti Kadhiravan, "WOAPR: An affinity propagation based clustering and optimal path selection for time-critical wireless sensor networks", IETNetworks, Vol 8, NO. 2, pp. 100 – 106, 2019

[3] Qiang Wei, Zhi Jin," Service discovery for Internet of Things: A context awareness perspective", Wei, Q., & Jin, Z. (2012). Service discovery for internet of things.Proceedings of the Fourth Asia-Pacific Symposium on Internet aware – Internet aware, 2012.

[4] Villaverde, B. C.; de Paz Alberola, R.; Jara, A. J.; Fedor, S.; Das, S. K. &Pesch, D. Service Discovery Protocols for Constrained Machine-toMachine Communications. IEEE Communications Surveys and Tutorials, 2014, 16, 41-60.

[5] Kousalya, A., Sakthidasan, K. & Latha, "Reliable service availability and access control method for cloud assisted IOT communications", in Wireless Network-Springer, https://doi.org/10.1007/s11276-019-02184-3, 2019

[6] Preuveneers, D., Berbers, Y. 2008. Internet of Things: A Context-Awareness Perspective. In The Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems, Y. Lu, Y. Zhang, L. T. Yang, H. Ning, Ed. Auerbach Publications, Taylor & Francis Group, 287-307.

[7] Issarny, V., Georgantas, N., Hachem, S., Zarras, A., Vassiliadist, P., Autili, M., Gerosa, M. A., Hamida, A. B. 2011. Service-oriented middleware for the Future Internet: state of the art and research directions. Journal of Internet Services and Applications, 2, 1 (Oct. 2011), 23-45. DOI=10.1007/s13174-011-0021-3.

[8] X.Jin, S.Chun et al. "A fast and scalable approach for IoT service selection based on a physical service model."In Information Systems Frontiers.Springer.2016.pp 1-16.

[9] Gu, T., Pung, H. K., Zhang, D. Q. 2005. A service-oriented middleware for building context-aware services. Journal of Network and Computer Applications, 28, 1 (Jan. 2005), 1-18. DOI= 10.1016/j.jnca.2004.06.002.

[10] Marie P, Desprats T, Chabridon S, Sibilla M. Extending Ambient Intelligence to the Internet of Things: New challenges for QoC management In: Hervás R, Lee S, Nugent C, Bravo J, editors. Proceedings of the 8th International Conference on Ubiquitous Computing and Ambient Intelligence.vol. 8867 of Lecture Notes in Computer Science. Cham, Switzerland: Springer International Publishing: 2014. p. 224–31.

[11] N. Sridevi, V. Nagarajan, K. Sakthidasan @ Sankaran, "Efficient traffic control and lifetime maximization in mobile ad hoc network by using PSO–BAT optimization", in Wireless Network-Springer, https://doi.org/10.1007/s11276-019-02173-6,2019