TRUST MANAGEMENT FRAMEWORK FOR IOT-BASED P2P OBJECTS

Raghu Nallani Chakravartula[1]and V. Naga Lakshmi[2]

[1]Security Architect, Philips Healthcare, Bengaluru, India
[2]Head, Department of Computer Science, GIS, GITAM University, Visakhapatnam, India

ABSTRACT

The proliferation of physical objects connecting to the Internet leads to a novel paradigm called "Internet of Things (IoT)." The objects are equipped with microprocessors and transceivers for data acquisition and sensing the environment around them respectively. IoT is driven by distributed nature with pervasive presence. In such an environment, security and privacy are the major barriers and addressing these issues is vital for the penetration of IoT-based Medical devices. Traditional security solutions will not suffice to the needs of IoT-based resource constraint devices and pose potential limitations and patient safety issues. The paper proposes a novel approach for trust management framework called HEXAGON model, which represents the human notion of trust in the computational algorithm with six key factors Peer Recommendation, Operational Risk, Operational Cost, Reputation, Privacy, and Role and Identity management.

KEYWORDS

Trust, Human-notion of trust, mobile ad hoc network, Internet of Things (IoT), IoT-based medical deviceand applications.

1. INTRODUCTION

The term Internet of Things (IoT) was first coined by Kevin Ashton in 1999. Internet of things (loT) is the new paradigm that allows linking every physical object in the real world with that of the virtual world [1]. Due to the pervasive nature of these objects, sensitive data can be collected and transmitted to offer services which can be accessible to anyone, anytime, anywhere and anything. Security and privacy concerns pose a significant challenge to the further expansion of the IoT-based Adhocmedical applications [2].In such an environment, there is a possibility that unknown users may involve in malicious interactions. Traditional Access control rules cannotbe applied due to lack of centralized service. Therefore for an IoT-based peer-to-peer applications, The type of interaction an entity performs with another should dependon the "Degree of trust" and it evolves on the flyover a period [3][4]. The proposed “Hexagon framework” evolves dynamic trust negotiation to arrive at the degree of trust using six key factors called Peer recommendation, Operational Risk, Operational Cost, Reputation, Role, Identity management and Privacy.

Having given an initial introduction and motivation of our work, the rest of this paper is structured as follows. Section 2 describes the background and related work.The proposed architecture of Hexagon framework is presented in section 3.Section 4 provides more details of trust value calculation using Inference engine. The conclusion of the paper and future work is in section 5.

DOI : 10.5121/ijp2p.2017.8302

2. BACKGROUND AND RELATED WORK

Various research projects were undertaken towards the research and development of trust management framework. Simple Universal Logic-oriented Trust Analysis Notation (SULTAN) [5] is a trust management framework that allows specification, analysis, and management of trust relationships. In this context, all the policies are analyzed and managed at the centralized server. Itmakes it inappropriate for decentralized ad-hoc mobile Networks. Policy Maker [6] is probably one of the first distributed trust management frameworks which make trust decisions based on the static policies. However, Trust negotiation is a dynamic process, and a decision needs to be taken on the fly. Therefore, this approach also has limitations.

Some of the projects which are based on distributed human notion of trust management are a Human Trust Management Model and Framework (hTrust) [7], Secure Environments for Collaboration among Ubiquitous Roaming Entities (SECURE)[8],Risk Aware Decision Framework for Trusted Mobile Interactions [9], Supporting Trust in the Dynamic Establishment of peering coaLitions (STRUDEL) [10],and Trust Based on Evidence (TuBE)[11],[12].All the above research programs aimed at dynamic trust negotiation and generation, but these frameworks failed in capturing the significant factors needed to demonstrate the human notion of trust.None of the frameworks targets towards privacy in an IoT-based medical environment where it is extremely critical with regulations like HIPAA [13] and European privacy laws [14].The proposed Hexagon framework addresses authentication and authorization in IoT-based peer-to-peer medical applications by capturing trust and privacy dynamically with minimum user intervention.

3. PROPOSED ARCHITECTURE FOR TRUST MANAGEMENT FRAMEWORK

Trust plays a key role in security management particularly in decentralized environments due to lack of infrastructure [15]. Trust negotiation for typical IoT-based medical applications is as depicted in figure 1.

The idea behind trust management framework is to represent the human notion of trust in terms of computational algorithms for IoT-based ad-hoc medical applications [16][17]. The proposed framework has identified six factors to derive at the quantifying trust value and hence named it as "Hexagon Framework." Peer Recommendation, Operational Risk, Operational Cost, Reputation, Privacy, Role and Identity management are used for representing human-notion of trust. Any trust decisions between or among devices are solely taken by them without human interference, which closely resembles the way trust is built among the individuals in the physical world.

Following are the details of the modules of HEXAGONFramework, which help incapturing the six factors, to determine the trust value

a) **Peer Recommendation:** This module accepts the recommendations from the peers that aids in making trust decisions.

b) **Privacy:** This module looks into the privacy level defined for the application while making trust decisions.

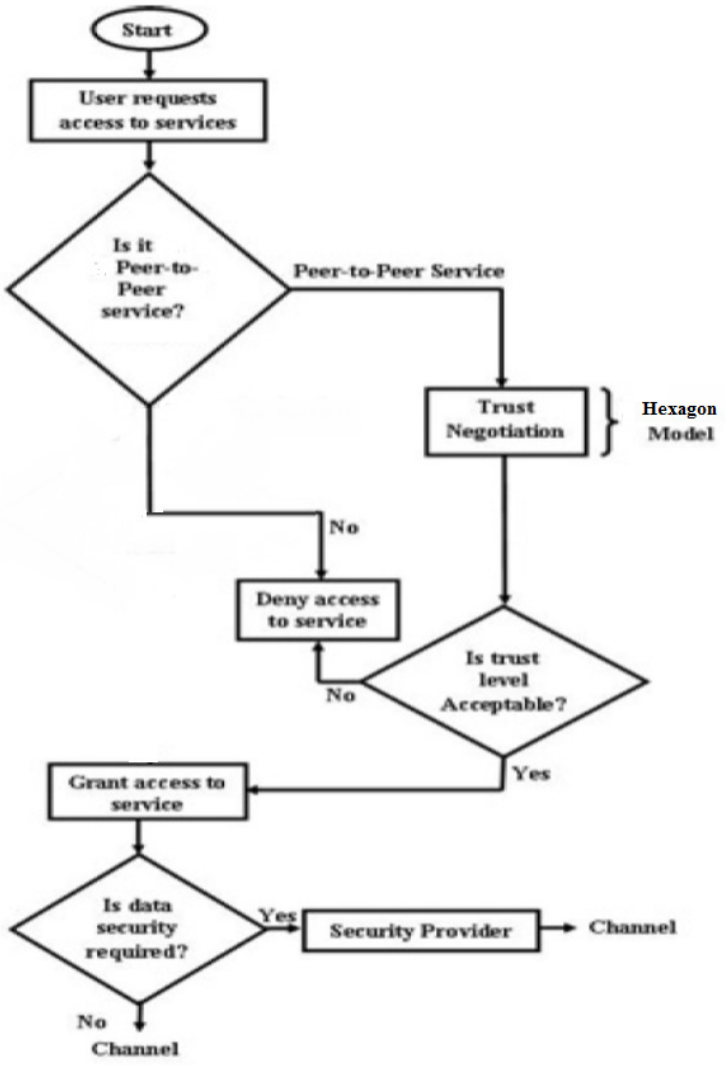

Figure 1Trust Negotiation Framework for IoT-based Ad-hoc Medical Applications

c) **Operational Cost:** This module measures cost involved in performing the action. The factors like battery power,bandwidth used and processing required etc. are consideredwhile giving access to the applications.

d) **Operational Risk:** This module carries out the risk-benefit analysis basedon the knowledge base information. The knowledge base is the database build over a period.

e) **Reputation:** This module helps to rate peers and thereby build trust based on the past interactions.

f) **Role and Identity Management:** This module helps the user to access the resources anonymously, by using pseudonyms thereby ensuring privacy level. The required behavior to the entity is determined based on client or server behavior in peer-to-peer application.

g) Privacy: This module asks the user to key in the privacy value and helps in managing the configuration.

Various components of Trust management framework as depicted in the figure 2

1. Request handler
2. Security Profile Manager
3. Knowledge Base
4. Inference Engine
5. Decision Dispatcher and Cryptographic API

Trust Management Framework receives the request from peer-to-peer application through request handler for negotiating the trust value[18][19]. Request handler forwards the request to six modules for computing the various factors, which in turn provides to inference engine for calculating the final trust value. Preferences of different IoT-based medical applications as well as past interaction details are given in the knowledge base, which is maintained at clientele devices. Security profile manager helps in configuring the application preferences. These preferences are used by request handler while computing the trust value. Finally, the decision is dispatched to the application. Communication across the peers while calculating the trust value is secured using pre-shared key through cryptographic API.Role and Identity management modules help in capturing the preferences and identity of the user to maintain the session details, which in-turn provides input to the other modules. Inference engine makes decision based on the outcome of Reputation, Operational Cost, Operational Risk, Privacy and Peer Recommendation modules

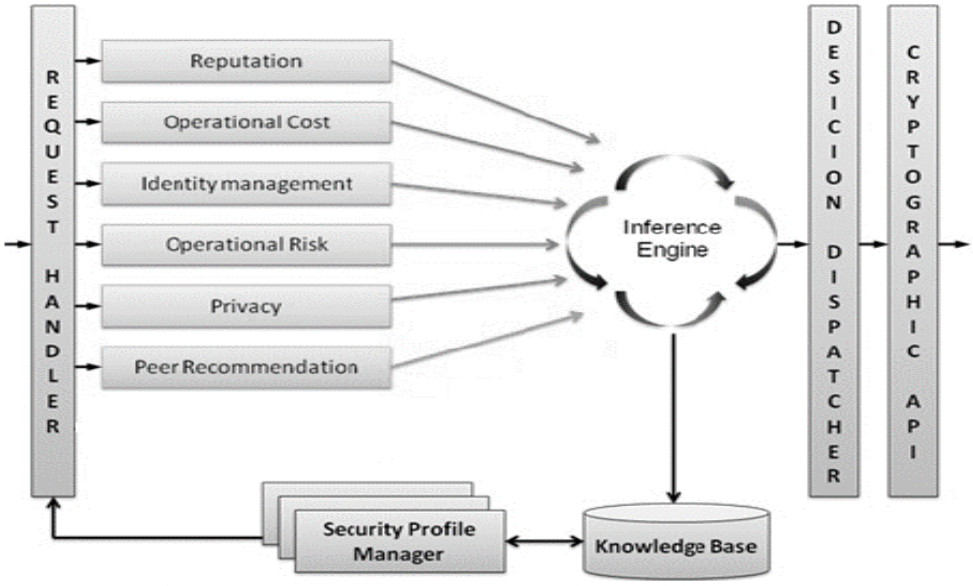

Figure 2: HEXAGON Framework and various modules

4. TRUST VALUE CALCULATION USING INFERENCE ENGINE

Privacy is one of the important factors for an IoT-based application to determine whether to provide access to the requested resource. It is defined by Privacy Value (TTV), which represents Trust-Privacy requirements of an IoT-based application. The value is represented by fuzzy sets [20] [21] and must be between 0 and 1. Each user is provided with an interface to configure the Privacy Value (TTV) as shown in figure 3

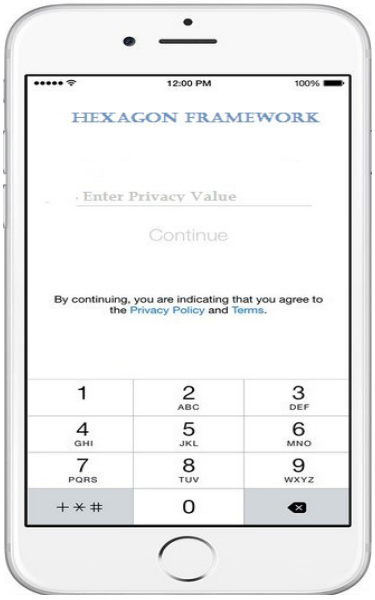

Figure 3: Privacy configuration user Interface

When a user request for a resource then a service request is made, Trust Value (TV) is calculated based on the outcome of other modules Operational Cost, Operational Risk, Reputation and Peer Recommendations. If this Trust Value is greater than or equals to PV, then the service request is successful and the access to the resource is permitted. Request processing for peer-to-peer applications is depicted through flowchart as shown in Figure.4

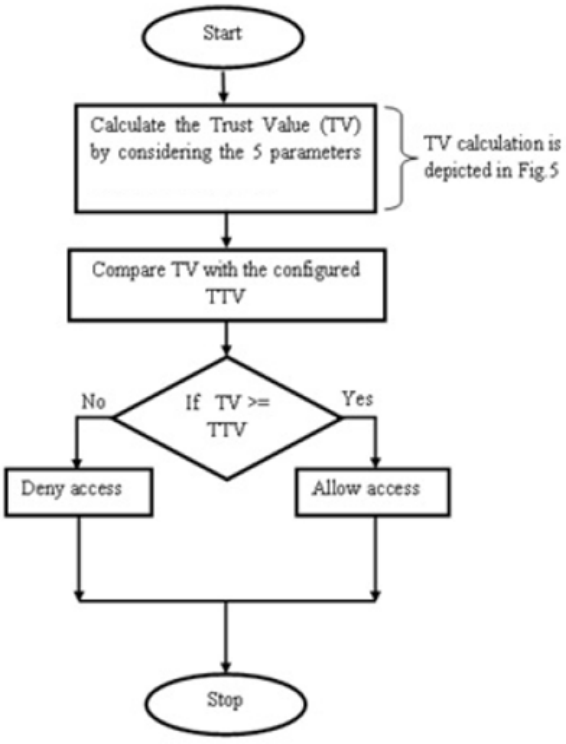

Figure 4: Request Processing for Peer-to-Peer thing in IoT-based medical application

As part of trust value calculation, the device needs to check whether enough battery power is available for processing the request. Two levels of threshold battery power (X and Y) can be configured for different applications by the user. In the case of not having enough battery power, either the service can be denied, or the user can be involved in taking a decision. Otherwise, Operational Risk (OR) will be evaluated, and in case if it is less than the threshold risk $(OR)_T$, it is processed further. An outcome of Reputation and Recommendation modules will be considered for calculating the trust value. Trust value calculation is as depicted in Figure 5

In case if the device 'Y' is providing a serviceto another device 'Z' is consumingthe respective services, their past interactions are depicted in reputation module as $\mu_Y(Z)$. It represents the reputation device 'Y' has on device 'Z'. $\mu_Y(Z)$can be a real value in [0.0, 1.0], which is defined through fuzzy set and is considered as reputation value (RP). Device requests for the recommendation from the peers for calculating the trust value. For example, ifRa(Z), Rb(Z) …Rz(Z) are the recommendations given by respective devices a, b ... z on device 'Z', then final Peer Recommendation (PR) value is a function of these recommendations is calculated as $PR=f(R_t(Z) \forall \text{ peers } t)$

The final trust value is computed from Operational Risk (OR), Reputation (RP) and Peer recommendation (PR). Trust Value (TV) is directly proportional to Peer Recommendations and Reputation and is inversely proportional to Operational Risk. If weightages given to PR, RP and OR are A, B and C respectively, then the final Trust Value is given by Trust Value=((A*PR)+(B*RP))/(C*OR).

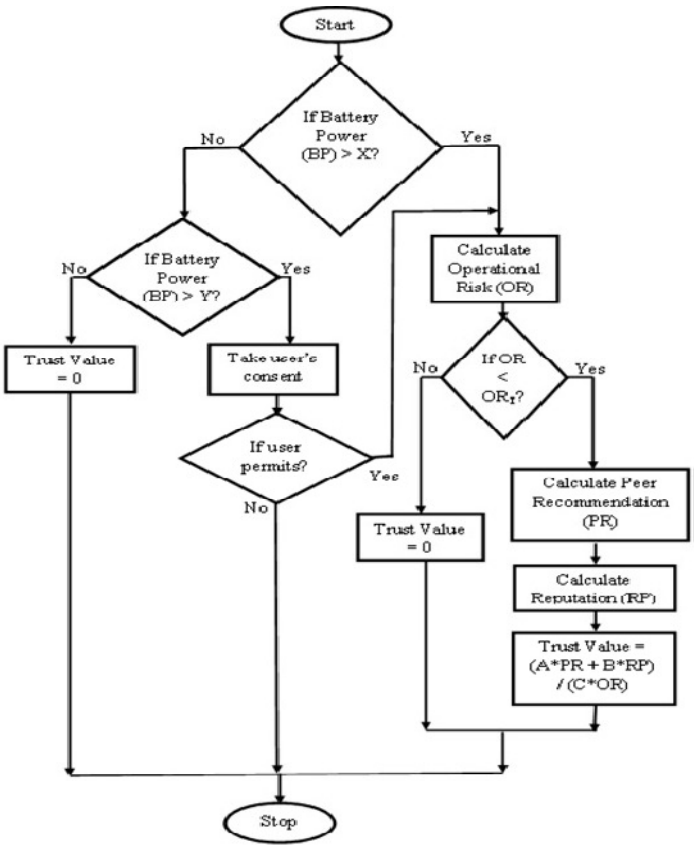

Figure 5: Trust negotiation in Peer-to-Peer IoT-based medical device

5. CONCLUSION AND FUTURE WORK

This paper presented a Trust Management Framework to evolve the trust value in the IoT-based environment. Efforts are made to represent the human notion of trust using computational algorithms using six key factors Role and Identity Management, Reputation, Peer Recommendation, Operational Cost, Operational Risk and Privacy to arrive at the trust value and hence named it as HEXAGON framework. We presented the architecture of the Trust Management Framework as well as the design of the Inference engine, which calculates the trust value using fuzzy logic. Future work includes implementation of the Trust Management Framework and testing its functionality with IoT-based medical devices.

REFERENCES

[1] Ashton K. That 'Internet of things' thing. RFID Journal, 2011, http://www.rfidjournal.com

[2] Dennis Gessner; Alexis Olivereau; Alexander Salinas Segura; AlexandruSerbanati,"Trustworthy Infrastructure Services for a Secure and Privacy-Respecting Internet of Things". 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications

[3] SunethNamal; HasinduGamaarachchi; GyuMyoungLee; Tai-Won Um, "Autonomic trust management in cloud-based and highly dynamic IoT applications". 2015 ITU Kaleidoscope: Trust in the Information Society (K-2015)

[4] HamedHellaoui; AbdelmadjidBouabdallah; MouloudKoudil, "TAS-IoT: Trust-Based Adaptive Security in the IoT". 2016 IEEE 41st Conference on Local Computer Networks (LCN).

[5] T. Grandison and M. Sloman. "Trust management tools for internet applications". In Proc. of the 1stInternational Conference on Trust Management, Crete, Greece, May 2003.

[6] M. Blaze, J. Feigenbaum, and J. Lacy. "Decentralized trust management". In Proc.of IEEE Symposium on Security and Privacy, pages 164-173, Oakland, Ca, May1996.

[7] Capra, L. "Engineering human trust in mobile system collaborations". In Proceedings of the 12th International Symposium on Foundations of Software Engineering,pages 107-116, Newport Beach, CA, USA, November 2004. ACM Press.

[8] "Secure environments for collaboration among ubiquitous roaming entities". InProceedings of the First Internal iTrustWorkshop on Trust Management in DynamicOpen Systems, Glasgow, Scotland, September 2002.

[9] A. Abdul-Rahman and S. Hailes. "Using recommendations for managing trust indistributed systems". In Proc. ofIEEE Malaysia International Conference on Communication (MICC'97), Kuala Lumpur, Malaysia, November 1997.

[10] Quercia, D., Lad, M., Hailes, S., Capra, L. and Bhatti, S. "STRUDEL: SupportingTrust in the Dynamic Establishment of peering coaLitions". In Proceedings of the21st ACM Symposium on Applied Computing, Dijon, France, April 2006.

[11] Ruohomaa, S., Viljanen, L., and Kutvonen, L. (2006, March). "Guarding enterprisecollaborations with trust decisions - The TuBE approach. In proceedings of the firstinternational workshop on Interoperability Solutions to Trust, Security, Policies andQoS for enhanced enterprise systems" (IS-TSPQ 2006). Bordeaux, France: Springer-Verlag.

[12] Marco Carbone, Mogens Nielsen, and VladimiroSassone. "A formal model for trustin dynamic networks". BRICS Report RS-03-4, 2003.

[13] “HIPAA Compliance”, https://www.hhs.gov, 2017.

[14] “European Privacy Laws”, http://www.eugdpr.org/, 2017.

[15] Xiong Li; Zhou Xuan; Liu Wen,"Research on the Architecture of Trusted Security System Based on the Internet of Things". 2011 Fourth International Conference on Intelligent Computation Technology and Automation

[16] Mohsen Dorodchi; Maryam Abedi; BojanCukic, "Trust-Based Development Framework for Distributed Systems and IoT". 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC).

[17] Yang Liu; Zhikui Chen; Feng Xia; XiaoningLv; Fanyu Bu, "A Trust Model Based on Service Classification in Mobile Services". Green Computing and Communications (GreenCom), 2010 IEEE/ACM Int'l Conference on & Int'l Conference on Cyber, Physical and Social Computing (CPSCom).

[18] Michele Nitti; Roberto Girau; Luigi Atzori; Antonio Iera; Giacomo Morabito,"A subjective model for trustworthiness evaluation in the social Internet of Things". 2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC)

[19] Anupam Kumar Bairagi; DebasishChakroborti, "Trust based D2D communications for accessing services in Internet of Things". 2015 18th International Conference on Computer and Information Technology (ICCIT)

[20] Igor Kotenko; Igor Saenko; Sergey Ageev, "Countermeasure Security Risks Management in the Internet of Things Based on Fuzzy Logic Inference". 2015 IEEE Trustcom/BigDataSE/ISPA.

[21] AgusKurniawan; Marcel Kyas, "A trust model-based Bayesian decision theory in large scale Internet of Things". 2015 IEEE Tenth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP).