Yashoda Multidisciplinary Research Journal

A SURVEY ON IOT NETWORK SECURITY SITUATION AWARENESS BASED ON USER-DEFINED RULES AND SEMANTIC ONTOLOGY

Principal Author[1], Co- Author[2]

[1]*Principal Dr. M. D. Bhosale, Dept. of MCA, Yashoda Technical Campus, Wadhe, Satara, India- 415011, mcahod_ytc@yes.edu.in,Mob.No.- 9823116810*

2Asst. Prof. H.O. Tapase, Dept. of MCA, Yashoda Technical Campus, Wadhe, Satara, India -415011 hot_mca@yes.edu.in Mobile No. 8624989696

3Asst. Prof. R.S. Sapakal, Dept. of MCA, *Yashoda Technical Campus, Wadhe, Satara, India -415011 rss_mca@yes.edu.in Mobile No. 8421953552*

Abstract-Internet of Things (IoT) makes users, network, and perception devices cooperate more closely. If IoT has occurred security problems, it can cause damage to human lives. To improve the ability of monitoring, emergency response providing, and predicting the development trend of IoT security, this paper proposed a new model known as network security situation awareness (NSSA). This paper proposes model of network security situation awareness for IoT by using a situation reasoning method based on user-defined rules and semantic ontology. This ontology technology provides us some semantic description to solve the heterogeneity problem in IoT security domain. The ability of ontology of limited description can recompense by the user defined rules, so the reasoning ability of proposed ontology model can be improved.

Key words- Semantic ontology, IoT, User defined rules, network security

INTRODUCTION

Now days IoT is a very important component in the Information Technology field. It is widely used in networking through pervasive computing, intellisence, recognition technology, and other communication technology. The applications of IoT are increased day by day due to its developmental growth such as in smart city, smart industries, smart home as well as smart industries[1]. As the applications of IoT are increased, the security issues of IoT are very important. If IoT has faced some network attacks, it may damage human lives and their properties. Fig 1 shows the architecture of IoT. It consists of three layers. First layer is Perception layer, second layer is Network layer and the third layer is Application layer. The perception layer collects the information from various sensors, RFID, GPS and so on. The Network layer transmits the information collected by the perception layer to the application layer. The main attack in the IoT is attack to the heterogeneous networks. The application network then processes the information transmitted by the application layer to fulfill the user requirements. If any layer is attacked, it will affect the whole system and the user. In IoT the security of application layer and the network layer is most important, so IoT requires real time and holistic security management which

contains prediction of possible attacks, detection of vulnerabilities, real time attacks[2].

Yashoda Multidisciplinary Research Journal

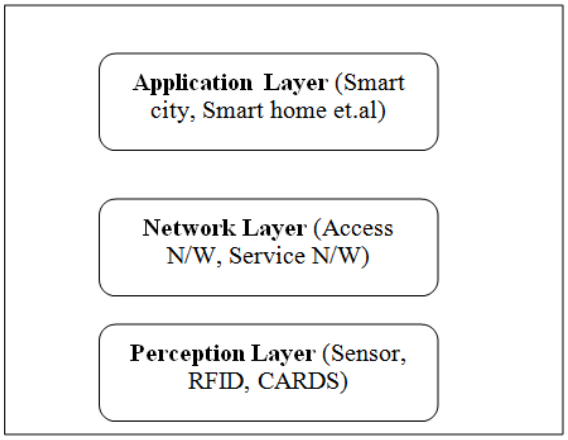


Fig.1 Architecture of IoT

Since IoT devices are heterogeneous and generates non-uniform data, the security management of IoT is very challenging task. So it is very necessary to analyze the heterogeneous data to make appropriate decisions. Existing security solutions does not scale the large networks of heterogeneous devices and thus does not satisfy the requirements [3]. So to solve these problems, Network Security Situation Awareness which is network security monitoring technology is proposed and it will play an important role in security of IoT. First time in 1999 Bas[5] proposed the NSSA i.e. Network security situational awareness concept to handle the network security problem with holistic approach based on situational awareness. But there is challenge related to the perception of network situations. Ontology plays an important role in resolving semantic heterogeneity [6] [9]. This paper proposed user defined rules and semantic ontology based situation reasoning method for IoT network security situation awareness. This method understands the formalized and unified description of network security situation information of IoT . It can also detect the security situation in real time of the network. The remaining paper is organized as follows: Section 2 summarizes

related work on NSSA. Section 3 is proposed ontology model for NSSA. Section 4 concludes this paper.

ONTOLOGY MODELING FOR NSSA

Formation of an ontology model is not an engineering activity but it can be used manual methods like enterprise ontology, Ontology life cycle, Ontoweb, TOVE.

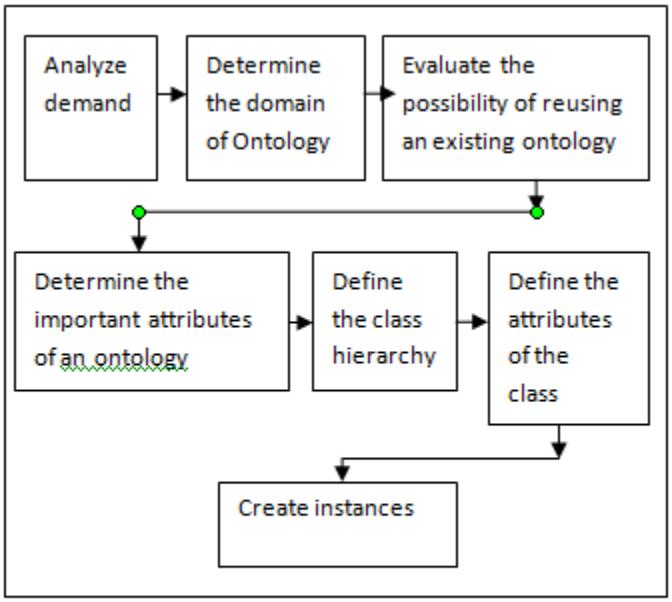


Fig. 2 Ontology building process

Fig. 2 summarizes the domain ontology building process. In that process of building an process following four principles should be followed.

1. Clarity: Use the formal description at the time of defining the related terms.

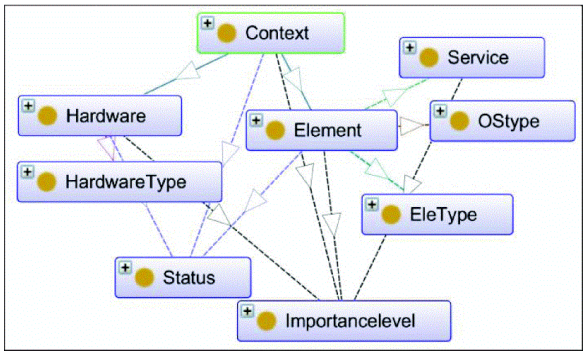
2. Coherance: The consistency check of the reasoning machine must be satisfied by the Ontology definition.

3. Extendibility: It can be used in future also.

4. Minimal coding bias: Coding methodology cannot be limited.

Ontology model can be built in the NSSA domain to get the network security situation.

Yashoda Multidisciplinary Research Journal



Some elements can be considered for ontology. First element can be context. It contains various host and network security equipments. It can be used to accommodate user needs. Second element can be Vulnerability. It is the basic part of the network security situation. Vulnerability can be like attacker can does the unauthenticated access or any other attack for illegal purpose. Third element can be attack. Attack is the very important threat or issue to the network security situation. Attacker can use any type of attack to damage the hardware or software or any kind of sensitive data. Another element can be considered that is network flow. It is very useful element in network security situation since it not only defines the network traffic but also can used to detect the any abnormal behavior in the network. Proposed ontology model is based on the above security concepts. For that Web Ontology Language can be used. This OWL is expressive and has reasoning ability. Two types of properties can be used here object type and data type. Object type can define the relation between the instances and belonging classes. The data type property can define the relation between the classes and literals.

USER DEFINED RULES

In above section It have been seen that how to build the ontology model for network security situation using OWL. Now in proposed system SWRL is used as the rule language because it is the semantic web description language. In ontology each rule in the SWRL is a type of OWL axioms. New rules can also interact with the old OWL axioms which ontology contains. Here is one example of SWRL rule usage. It shows Mother's sister is aunt can be written in SWRL language as follows:

*M*other(?x,?y) ^ *hasSister*(?y,?z) ! *Aunt*(?*x*; ?*z*)

In above rule *M*other(?x,?y) shows relationship that x's mother is y. If "*M*other(?x,?y)" and "*hasSister*(?y,?z" is a relationship then the result can be the z is the aunt of x. As the OWL query cannot make by the SWRL. So by using Semantic query Enhanced Web Rule Language (SQWRL), the ontology model can be queried. To retrieve the knowledge from OWL ontology SQWRL can be used.

CONCLUSIONS

This paper surveys a new model known as network security situation awareness (NSSA). Also model of network security situation awareness for IoT by using a situation reasoning method based on user-defined rules and semantic ontology. This ontology technology provides us some semantic description to solve the heterogeneity problem in IoT security domain. The ability of ontology of limited description can recompense by the user defined rules, so the reasoning ability of ontology model can be improved.

REFERENCES:

[1] F. Wortmann and K. Flüchter, ``Internet of Things technology and value added," *Bus. Inf. Syst. Eng.*, vol. 57, no. 3, pp. 221_224, Jan. 2015.

[2] T. Hänisch and S. Rogge, ``Industrie 4.0," in *IT-Sicherheit in der Industrie 4.0*. Wiesbaden, Germany: Springer, Feb. 2017, pp. 91_98.

[3] A. R. Sadeghi, C. Wachsmann, and M. Waidner, ``Security and privacy challenges in industrial Internet of Things," in *Proc. 52nd Annu.DA. Conf.*, Aug. 2015, pp. 1_6.

[4] M. R. Endsley, ``Design and evaluation for situation awareness enhancement," in *Proc. Hum.*

Factors Ergonom. Soc. Annu. MTG, Jan. 1988, pp. 97_101.

[5] T. Bas, ``Multisensor data fusion for next generation distributed intrusion detection systems," in *Proc. IRIS Nat. Symp. Sens. DataFusion*, May 1999, pp. 24_27.

[6] W. Gödert, ``An ontology-based model for indexing and retrieval," *J. Assoc. Inf. Sci. Technol.*, vol. 67, no. 3, pp. 594_609, Jan. 2015.

[7] Jorge Granjal et al. "Security for the Internet of Things: A Survey of Existing Protocols and Open Research issues" IEEE Communications Surveys & Tutorials (Volume: 17, Issue: 3, thirdquarter 2015)

[8] O. J. Lee *et al.*, ``Towards ontological approach on trust-aware ambient services," *IEEE Access*, vol. 5, pp. 1589_1599, 2017.

[9] J. Li, X. Li, B. Yang, and X. Sun, ``Segmentation-based image copy-move forgery detection scheme," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 507_518, Mar. 2015.

[10] W. Wong, W. Liu, and M. Bennamoun, ``Ontology learning from text: A look back and into the future," *ACM Comput. Surv.*, vol. 44, no. 4, Aug. 2012, Art. no. 20.

[11] J. Huang and M. S. Fox, ``An ontology of trust: Formal semantics and tran- sitivity," in *Proc. 8th Int. Conf. Electron. Commerce, New e-Commerce, Innov. Conquering Current Barriers, Obstacles Limitations Conducting Successful Business Internet*, Aug. 2006, pp. 259_270.

[12] N. Dokoohaki and M. Matskin, ``Structural determination of ontology-driven trust networks in semantic social institutions and ecosys-tems," in *Proc. Int. Conf. Mobile Ubiquitous Comput., Syst., Services Technol. (UBICOMM)*, Nov. 2007, pp. 263_268.

[13] T. R. Gruber, ``A translational approach to portable ontologies," *Knowl. Acquisition*, vol. 5, no. 2, pp. 199_220, Jun. 1993.

[14] W. N. Borst, ``Construction of engineering ontologies for knowledge sharing and reuse," *Univ. Twente.*, vol. 18, no. 1, pp. 44_57, Jan. 1997.