TELKOMNIKA, Vol.11, No.2, February 2013, pp. 819~826
ISSN: 2302-4046

An IOT Security Risk Autonomic Assessment Algorithm

Ruijuan Zheng*[1], Mingchuan Zhang[1], Qingtao Wu[1], Chunlei Yang[1], Wangyang Wei[1], Dan Zhang[1], Zhengchao Ma[1]
[1]Electronic & Information Engineering College Henan University of Science and Technology Luoyang, China
*Corresponding author, e-mail:rjwo@163.com

Abstract

In terms of Internet of Things (IOT) system with the possibility criterion of fuzziness and randomness security risk, we qualitatively analyze the security risk level of IOT security scene by describing generalization metrics the potential impact and likelihood of occurrence of every major threat scenarios. On this basis, we proposed self-assessment algorithm of IOT security risk, adopting three-dimensional normal cloud model integrated consideration of risk indicators, researching the multi-rule mapping relationship between the qualitative input of safety indicators and the quantitative reasoning of self-assessment. Finally, we build security risk assessment simulation platform, and verify the validity and accuracy of the algorithm in the premise of substantiating the risk level and the safety criterion domain.

***Keywords*:** *Normal Cloud Model, IOT, Security Risk, Autonomic Assessment*

1. Introduction

As an ultra-large-scale network, it brings enormous challenges to its security and credibility because of composition of complex geometry, the application of the non-deterministic and running fuzziness of IOT. Moreover, the heterogeneity of the terminal and subnet more brings maximum technical difficulty to security of cross-domain and across subnet. Therefore, in the Internet of Things security research, it is necessary to comprehensively consider the dynamic change of resources and the many types of abnormal status, and overall take into account system security mechanisms and strategies time-sharing sequence. Autonomic computing has been regarded as a new effective way to achieve system autonomy and solve the problem of system security performance decline based on a system of internal and external changes in demand autonomously adjusting the software and hardware resources to improve service performance. How it autonomously converges, understands and assesses to many security factors affecting IOT system security and completes the fine measurement of autonomic security in dynamic changeful complex environment, is a key prerequisite for the autonomic security of the Internet of Things system.

Because IOT self-security research is still in its infancy, its directly related literatures now are relatively less. But the existing research shows a good prospect and trend of rapid development. These have provided a theoretical reference and technical direction for us to learn from the security of the computer network and the autonomic security mechanisms and ways of system, realize the depth fusion autonomy characteristics and IOT security and seek the trends and core essence of Things. The current research more focuses on the research and analysis of the risk assessment model. A dynamic trust model based on reputation and risk assessment [1] synthesizes dynamism and risk of the trust degree evaluation for the problem that the trusted network can not effectively deal with of malicious node attacks. Integrated fuzzy logic and real-time risk assessment of Petri nets [2] and risk assessment of the fusion of fuzzy theory and BP neural network [3] have constructed theoretical model of their own. Meanwhile, assessment strategies and methods have also made some progress. Document [4] referencing immune danger theory has proposed network intrusion risk detection and quantitative assessment methods using the antibody density. Document [5] proposed a network risk assessment method based on cloud model. A quantization, coding and control scheme is presented under communication constraints [6], a hierarchical model of survival situational awareness is

Received August 7, 2012; Revised December 28, 2012; Accepted January 13, 2013

proposed in [7]. And Integrating current study status, the relevant theories and strategies are not enough mature, as a result of autonomy problems in computer networks, the research in the field of system security and IOT security are in the exploration and the initial stage. Self-assessment process of security risk is proposed in this paper, focusing on the problem of IOT self-assessment, combining with high promiscuous and heterogeneous characteristics of IOT, adopting the three-dimensional normal cloud model to research the self-assessment algorithm of system security risk, and judging global multi-valued dependency characteristics between possibility criterion and security risks.

2. Possibility Criterion

Cloud model [8] which is a model of qualitative and quantitative conversion employing a natural language expression by Academician Li Deyi is able to the uncertainty convert between qualitative concept and its quantitative representation a natural language. It has been applied in data mining, intelligent control, fuzzy evaluation, etc. In the various branches of the natural sciences and social sciences, the pervasiveness of the normal distribution and the normal membership function together has laid the foundation for the universality theory of the normal cloud model [9]. One-dimensional normal cloud model (X, Y) consists of particular cloud generator, generates quantitative conversion of the concept , embodies randomness and fuzziness of the concept by the expected value Ex, entropy En and hyper entropy He. Because of its good mathematical nature, the normal cloud model is used to indicate a large number of uncertain phenomenon [10] in natural science and social science. At present, the normal cloud model has become the most wide cloud model. The curve expression is represented as shown below.

$$y = \exp[-(x - E_x)^2 / 2(E'_n)^2]$$

In view of the universality [9] of the normal cloud model, combined with the feature of security indicator of IOT system, on the basis of IOT system with the possibility criterion of fuzziness and randomness security risk, the potential impact and likelihood of occurrence of every major threat scenarios will be described, evaluated and fine measured. And the level of security risk and system tolerance degree with the heterogeneous IOT security scene of incremental deployment characteristics will be qualitative analyzed.

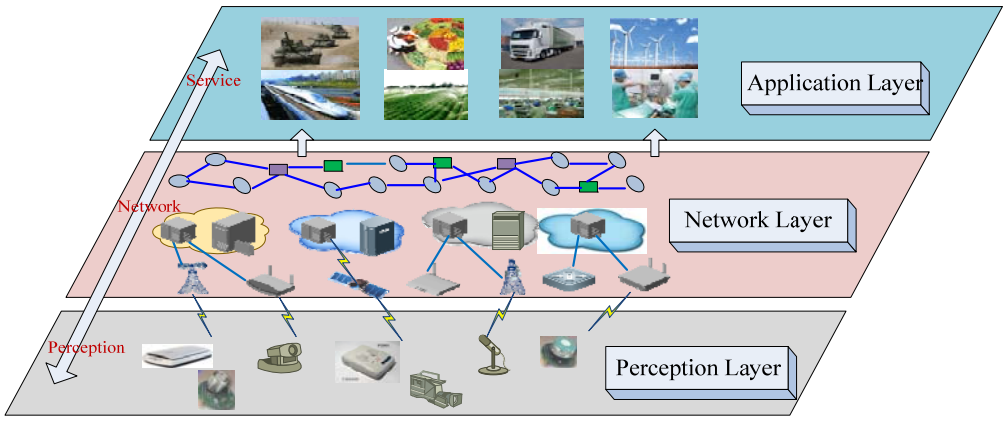

Figure 1. IOT architecture

IOT structures an "Internet of Things" of coverage of all things in the world utilizing these technologies such as RFID, wireless data communication on the basis of the Internet in the computer. In this network, goods (products) can communicate with each other without the need for human intervention. Its essence is to achieve automatically identification of items (products) and the interconnection and sharing of information through computer Internet by using radio frequency identification (RFID) technology. Things architecture is shown in Figure 1.

As a multi-source heterogeneous fusion network, IOT Security Criterion subject to constraints of the architecture security elements and security threats. Network layer of IOT has

the same security problems with sensor networks, mobile communication networks and the Internet. But there is a greater difference between IOT high-level and low-level with traditional network security. Perception layer has its own unique nature due to the difference of perception equipment and gather way. Application layer presents a different security attributes based on different scenario which is the content features, work environment, operator management of the application-oriented. Risk criterion influencing IOT system security will be extracted to clearly state the comprehensive restriction factor of IOT security, this paper based on Internet of Things hierarchical division.

The information of perception Layer is to go through these process flows, such as the information perception, acquisition, aggregation, fusion, transmission, storage, mining, decision-making and control, etc. Therefore, the perception criterion (pc) affecting the layer security is from several aspects , such as security of aware nodes (pc_1), resource constraint of perception and the convergence point(pc_2), the security of the information collection (pc_3), the privacy of the information transmission (pc_4) to prevent these potential security problems, such as node camouflage (pc_{11}), addition of nodes energy consumption (pc_{12}), signal leakage and interference (pc_{21}), information tampering (pc_{22}), the perceived damage of hardware/software (pc_{31}), non-authorized use (pc_{32}), perception data destruction (pc_{41}), perception data theft (pc_{42}), etc.

Network layer is be viewed as the core data forwarding level of Things. The network credibility and security (nc_1), security of data and privacy (nc_2), and reliability (nc_3) of routing protocols are simultaneously taken into account by Network Criterion (NC). These problems include occupied transmission bandwidth (nc_{11}), rapid spread of security threats (nc_{12}), message to steal (nc_{21}), message tampering (nc_{22}), message destruction (nc_{23}), protocol destruction (nc_{31}), shortening the network lifetime (nc_{32}), too long delay (nc_{33}), huge energy consumption (nc_{34}) caused by Flooding / LEACH / PEGASIS / SPIN routing protocols.

According to different applications and management mechanism in application layer, application Criterion (AC) is restricted by the service industry (ac_1), access control (ac_2), information storage (ac_3), and management models (ac_4), including multi-aspect content such as the type of service (ac_{11}), service object (ac_{12}), privacy protection (ac_{13}), authentication of heterogeneous network (ac_{21}), remote signing identification of application terminal (ac_{22}), attack of virus / hacker / malware (ac_{31}), illegal use of 3G terminal (ac_{32}), the internal authentication (ac_{41}), management contract (ac_{42}), etc.

The security criterion of perception layer, network layer and application layer is integrated, and its scope of application and the influencing factors are fused, extended to form a distribution structure of IOT security criterion, as shown in Figure 2.

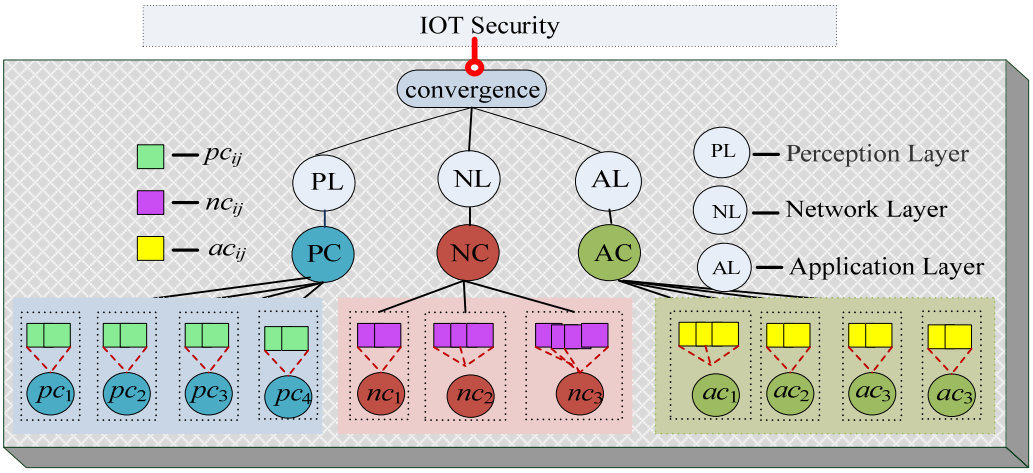

Figure 2. A distribution structure of Things security criterion

Multi-dimensional, multi-layered security criterion for the security of the Internet of Things has the effect of varying degrees in Figure 2 to form the set of attributes of the evaluation of the security risks of the Internet of Things. Accordingly, three-tier security criterion

that may affect IOT security is analyzed, from which extracts several attributes influencing the degree highest number of IOT security risk, to form the key criterion set (Key Criterion, KC) of IOT security assessment. Meanwhile, its security criterion level (Criterion Grade, *CG*) is divided into the following grades: $CG = \{cg_1, cg_2, ..., cg_R\}, R \in Z$, according to the bad or good degree of each index of KC in the actual work process. For different indicators encountered security risk probability in heterogeneous IOT environment, Integer R possesses a variety of options. Based on the principle of one-dimensional cloud model, single criterion is described by multi-level security. Security criterion C_{kc} formed can be expressed as $C_{KC} = KC \times CG$.

3 Self-assessment Algorithm

3.1 Generalized Risk Levels

Qualitative representation of Things safety risk is determined by the security criterion C_{KC} mapped by the key criterion *KC* and security criterion grade *CG* of third quarter. Therefore, in the beginning of establishing the evaluation model, we argues that the divided rule of level of risk (Level of Risk, L_Ri) is the similar with the division grade of its security criterion grade *CG*, which *P* grade is divided into mainly based on the difference between the oriented specific application and the accuracy requirements of assessment. Thus, $L_R = \{lr_1, lr_2, ..., lr_P\}, P \in Z$. In view of the above, one-dimensional normal cloud C_{KC} generated by the aforementioned key criterion is related to the security risk assessment process by employing reverse cloud generator generalizability to the risk level to establish the security risk assessment cloud model that depends on the multi-level and multi-dimensional criterion.

$KC = \{pc_1, pc_2, ..., pc_M, nc_1, nc_2, ...nc_N, ac_1, ac_2, ..., ac_T\}$ is the criterion domain of $M+N+T$, $M,N,T \in Z$, in which security criterion is not relevant to each other. L_R is qualitative comment in KC. The element $\{pc_1, pc_2, ..., pc_M, nc_1, nc_2, ...nc_N, ac_1, ac_2, ..., ac_T\}$ in KC for μ_{KC} of L_R is expressed as a random number with sTable trend.

$$\mu_{KC} : KC \to [0,1], \forall \{pc_1, pc_2, ..., pc_M, nc_1, nc_2, ...nc_N, ac_1, ac_2, ..., ac_T\} \in KC,$$

$$\{pc_1, pc_2, ..., pc_M, nc_1, nc_2, ...nc_N, ac_1, ac_2, ..., ac_T\} \to \mu_{KC}$$

Then the normal cloud of *M+N+T* dimension risk assessment can be described by the following 3(*M+N+T*) digital features.

$$((Ex_{pc1}, En_{pc1}, He_{pc1}), (Ex_{pc2}, En_{pc2}, He_{pc2}), ..., (Ex_{pcM}, En_{pcM}, He_{pcM}),$$

$$(Ex_{nc1}, En_{nc1}, He_{nc1}), (Ex_{nc2}, En_{nc2}, He_{nc2}), ..., (Ex_{ncN}, En_{ncN}, He_{ncN}),$$

$$(Ex_{ac1}, En_{ac1}, He_{ac1}), (Ex_{ac2}, En_{ac2}, He_{ac2}), ..., (Ex_{acT}, En_{acT}, He_{acT}))$$

3.2 Algorithm Procedure

The initial mapped relationship between the security criterion KC and the risk assessment is given by the assessment algorithm. The detailed reasoning rules between them need to be analyzed using the association rules between the multi-dimensional the security criterion cloud and IOT risk level cloud. Here, the potential relationship that exists between them is mainly described by the correlation rules between key security criterion KC of $M+N+T$ dimension and *R*-dimensional level of risk L_R. The fusion of security criterion set and level of risk has formed the correlation rule set I of IOT security risk. Then

$I = KC + L_R = \{pc_1, pc_2, ..., pc_M, nc_1, nc_2, ...nc_N, ac_1, ac_2, ..., ac_T; lr_1, lr_2, ..., lr_P\}, M, N, T, P \in Z$, in which V_I is stated as element value in *I*,

$V_I = \{V_{pc_m}, V_{nc_n}, V_{ac_t}; V_{lr_p}\}, m \in \{1,2,...M\}, n \in \{1,2,...N\}, t \in \{1,2,...T\}, p \in \{1,2,...P\}$.

As you see, both KC and L_R are subset of *I*, and $KC \cap L_R = \phi$. C_{KC} and C_{LR}, respectively, is multi-dimensional and one-dimensional normal cloud formed by the aforementioned 3.1. $C_{KC} = \{(E^{(pc_m)}x, E^{(pc_m)}n, H^{(pc_m)}e)_{cg_r}\} + \{(E^{(nc_n)}x, E^{(nc_n)}n, H^{(nc_n)}e)_{cg_r}\} + \{(E^{(ac_t)}x, E^{(ac_t)}n, H^{(ac_t)}e)_{cg_r}\}, m \in \{1, 2, ..., M\}, n \in \{1, 2, ..., N\}, t \in \{1, 2, ..., T\}, r \in \{1, 2, ..., R\}$, $C_{L_R} = (Ex_{lr_p}, En_{lr_p}, He_{lr_p}), p \in \{1, 2, ...P\}$.

Any element values in V_I are expressed by $v_i, i \in pc_m \cup nc_n \cup ac_t \cup lr_p$ to simplify above

expression. Then the expression form of correlation rules is $(pc_m = V_a) \wedge (nc_n = V_b) \wedge (ac_t = V_c) \Rightarrow lr_p = V_d$, $a,b,c \in pc_m \cup nc_n \cup ac_t, d \in lr_p$.

A reasoning idea of multi-condition and multi-rule is formed between our multi-dimensional security criterion and one-dimensional level of risk. The reasoning antecedent $C_{KC}(E^{(pc_m)}x, E^{(nc_n)}x, E^{(ac_t)}x; E^{(pc_m)}n, E^{(nc_n)}n, E^{(ac_t)}n; H^{(pc_m)}e, H^{(nc_n)}e, H^{(ac_t)}e)_{cg_r}$ and consequent $C_{L_R}(Ex_{lr_p}, En_{lr_p}, He_{lr_p})$ are shaped based on the correlation rule *I* of security risk. For every item multi-dimensional security criterion $(pc_m = V_a) \wedge (nc_n = V_b) \wedge (ac_t = V_c)$, specific algorithm process of autonomic assessment is as follows.

Step1 Determine their respective rules, if

$$E^{(pc_m)}x - 3 \cdot E^{(pc_m)}n < (pc_m = V_a) < E^{(pc_m)}x + 3 \cdot E^{(pc_m)}n$$

$$E^{(nc_n)}x - 3 \cdot E^{(nc_n)}n < (nc_n = V_b) < E^{(nc_n)}x + 3 \cdot E^{(nc_n)}n$$

$$E^{(ac_t)}x - 3 \cdot E^{(ac_t)}n < (ac_t = V_c) < E^{(ac_t)}x + 3 \cdot E^{(ac_t)}n$$

Then the rule $(pc_m = V_a) \wedge (nc_n = V_b) \wedge (ac_t = V_c) \Rightarrow lr_p = V_d$ is directly activated to step 4, or else to step 2;

Step2 Calculating respectively corresponding risk level support

$$S((pc_m = V_a) \wedge (nc_n = V_b) \wedge (ac_t = V_c) \Rightarrow lr_p = V_d)$$

And

$$S((pc'_m = V'_a) \wedge (nc_n = V_b) \wedge (ac_t = V_c) \Rightarrow lr_p = V'_d)$$

Else if

$$S((pc_m = V_a) \wedge (nc'_n = V'_b) \wedge (ac_t = V_c) \Rightarrow lr_p = V'_d)$$

Else if

$$S((pc_m = V_a) \wedge (nc_n = V_b) \wedge (ac'_t = V'_c) \Rightarrow lr_p = V'_d)$$

Degree of confidence

$$C((pc_m = V_a) \wedge (nc_n = V_b) \wedge (ac_t = V_c) \Rightarrow lr_p = V_d)$$

And

$$C((pc'_m = V'_a) \wedge (nc_n = V_b) \wedge (ac_t = V_c) \Rightarrow lr_p = V'_d)$$

Else if

$$C((pc_m = V_a) \wedge (nc'_n = V'_b) \wedge (ac_t = V_c) \Rightarrow lr_p = V'_d)$$

Else if

$$C((pc_m = V_a) \wedge (nc_n = V_b) \wedge (ac'_t = V'_c) \Rightarrow lr_p = V'_d);$$

Step3 In the same condition elements, the rule

$$(pc^{(\max)}{}_m = V^{(\max)}{}_a) \wedge (nc^{(\max)}{}_n = V^{(\max)}{}_b) \wedge (ac^{(\max)}{}_t = V^{(\max)}{}_c) \Rightarrow lr^{(\max)}{}_p = V^{(\max)}{}_d$$

corresponded by the maximum of the product of *S* and *C* is activated.

Step4 The deduction result $V^{(\max)}{}_d$ of risk value is output according to corresponding rule. And the support and confidence coefficient of corresponding rule are adaptively adjusted. Then it is input to operation process of Step3, thus, the autonomic deduction of reasoning rule is accomplished.

Note: reasoning process of other criterions is executed by complying with thinking of Step3, Step4 and Step5.

4. Simulation Experiment

To verify self-assessment effect of the proposed security risk self-assessment algorithm to network status data determined by the mass data of IOT, a simulation experiment platform is built in this paper and its data sets are trained, including perception port scanning samples set, packets steal sample set and internal authentication data set. By which, a multi-dimensional risk assessment normal cloud is generated, on this basis, actual operation performance of self-

reasoning rule is analyzed. The simulation experiment platform of IOT autonomic risk assessment is shown in Figure 3.

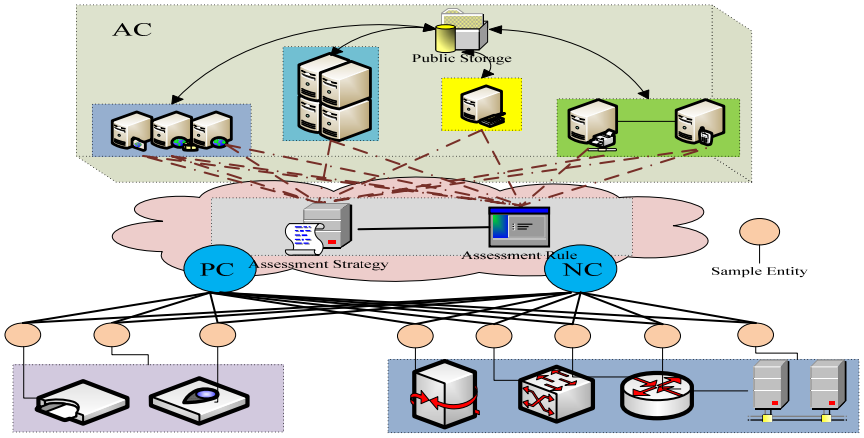

Figure 3. Simulation Experiment platform of IOT Autonomic Risk Assessment

According to simulation platform in Figure 5, $M+N+T$ dimensional security criterion of the theory domain $KC=\{pc_1, pc_2,..., pc_M, nc_1, nc_2,...nc_N, ac_1, ac_2,..., ac_T\}$ is embodied as $KC'=\{pc_1, nc_2, ac_4\}$. Analogously, both level of risk L_R and grade of security criterion CG of IOT are divided into P grade. Here, P is embodied as P=7, that is $CG'=L'_R=\{lr_1, lr_2, lr_3, lr_4, lr_5, lr_6, lr_7\}=\{worst, worse, bad, medium, good, better, best\}$. Based on the above information embodied, the specific division of three kinds of possibility security criterion and level of risk is shown in Table 1.

Table 1. Division of security criterion and risk level

Comment	pc_1	nc_2	ac_4	L'_R
best	[0.0,0.1)	[0.0,0.1)	[0.9,1.0)	[0.0,0.1)
better	[0.1,0.2)	[0.1,0.2)	[0.8,0.9)	[0.1,0.2)
good	[0.2,0.4)	[0.2,0.4)	[0.6,0.8)	[0.2,0.4)
medium	[0.4,0.6)	[0.4,0.6)	[0.4,0.6)	[0.4,0.6)
bad	[0.6,0.8)	[0.6,0.8)	[0.2,0.4)	[0.6,0.8)
worse	[0.8,0.9)	[0.8,0.9)	[0.1,0.2)	[0.8,0.9)
worst	[0.9,1.0]	[0.9,1.0]	[0.0,0.1)	[0.9,1.0]

Based on the generalized security criterion, the evaluation expectation of the generated three-dimensional risk assessment normal cloud set $C_{KC'-LR'}$ based on forward cloud generator is shown in Table 2 adopting the proposed self-assessment process. It assumes that ac_4 could be set to any value. Thus, three-dimensional self-assessment cloud is gained, shown in Figure 4.

Multi-group $KC'=\{pc_1, nc_2, ac_4\}$ is trained according to the algorithm process and semantic combination of theory evaluation. Part of training samples is shown in Table 2. Multi-combination relationships between three-dimensional sample and assessment result are synthesized, including several types such as one-dimensional corresponding, two-dimensional corresponding, and three-dimensional corresponding, one-dimensional error, and two-dimensional error, three-dimensional error.

The generated self-assessment errors of security risk are shown in Figure 5 based on result of training sample. It can be seen that the error between assessment result and theoretical evaluation prediction value should be less or equal 0.0015, and evaluation conclusion between them is basically consistent, which can satisfy the evaluation accuracy requirements in the premise of two-dimensional corresponding, and three-dimensional corresponding, one-dimensional error, and two-dimensional error. Only when the situation of one-dimension corresponding and three-dimensional error appears simultaneously, it will cause

error relative larger because sample input exists the mobility of operation and selection of support and confidence. It will achieve 0.003 in specific case.

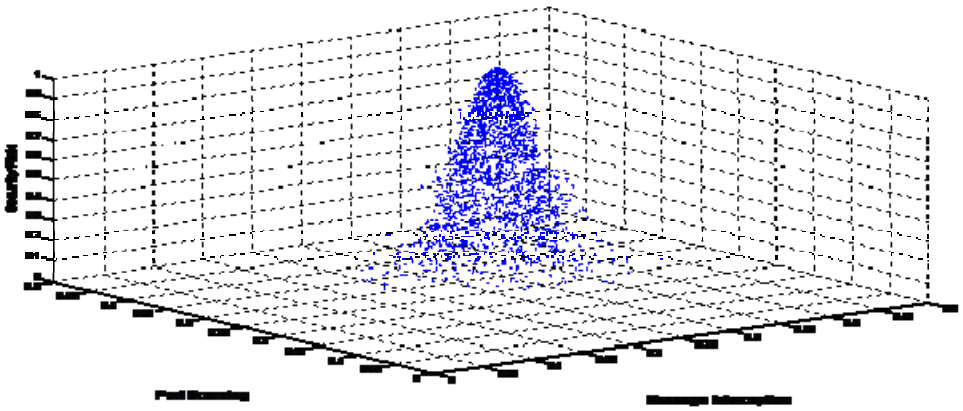

Figure 4. Self-assessment cloud for *good*

Table 2. Part of training samples

Sample Input			Assessment Result	
pc_1	nc_2	ac_4	Theory evaluation	Error value
0.0	0.09	0.92	best	0.001
0.13	0.15	0.85	better	0.0014
0.28	0.33	0.77	good	0.0015
0.58	0.48	0.45	medium	0.0012
0.75	0.69	0.28	bad	0.0014
0.88	0.85	0.17	worse	0.0015
0.92	0.98	0.08	worst	0.0013
0.79	0.88	0.58	bad	0.0015
0.25	0.44	0.55	good	0.016
0.60	0.57	0.64	medium	0.0030
0.12	0.55	0.7	better	0.0028

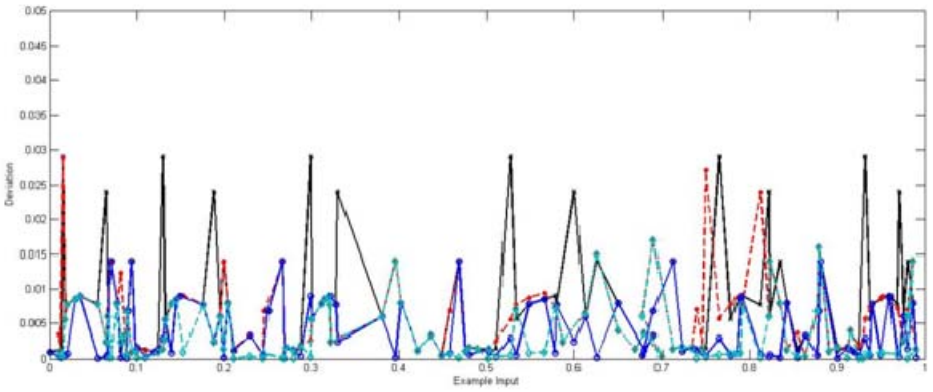

Figure 5. The error of IOT security risk self-assessment

5. Conclusion

An autonomic characteristic is given to IOT aiming at system feature and security information of IOT and uncertainty, unprediction and fuzziness of its change. Focusing on self-assessment of security risk, the self-assessment algorithm of IOT security risk based on three-

dimensional normal cloud was studied based on the dynamic fusion result of heterogeneous security factors. We strive to make a breakthrough in the research of autonomic security mechanism of heterogeneous security of IOT. It provides application service security of ensuring IOT in uncertain environment for new solution and thinking.

References

[1] Zhou Q, Yu J. Dynamic Trust Model Based on Reputation and Risk Assessment in Trusted Network. *Computer Application Research*. 2010; 27(11): 4211-4214.
[2] Liao ND, Li F, Song Y. *Research on real-time network security risk assessment and forecast*. Proceeding of 2010 International Conference on Intelligent Computation Technology and Automation. 2010; (3): 84-87.
[3] Hu CJ, Lv CM. *Method of risk assessment based on classified security protection and fuzzy neural network*. Proceeding of the 2010 Asia-Pacific Conference on Wearable Computing Systems. 2010; 379-382.
[4] Cai ZY, Zheng LP, Zhu SF. Quantitative assessment of Network intrusion risk Based on immune antibody concentration. *High Technology Letters*. 2010; 20(10): 1027-103.
[5] Liu Y, L YH. An evaluation model for network risk based on cloud theory. *Computer Simulation.* 2010; 27(10): 95-98.
[6] Liu QQ. Coordinated Motion Control of Autonomous and Semiautonomous Mobile Agents. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2012; 10(8).
[7] Zhao JH, Zhou Y, Shuo LX. A Situation Awareness Model of System Survivability Based on Variable Fuzzy Set. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2012; 10(8).
[8] Li DY, Du Y. *Uncertainty artificial intelligence*, Beijing: Defense Industry Press, 2005.
[9] Li DY, Liu CY. Study on the universality of the normal cloud model. *Chinese Engineering Science*. 2004; 6(8): 28-34.
[10] Zhang HB, Pei QQ, Ma JF. An algorithm for sensing insider threat based on cloud model. *Chinese Journal of Computers*. 2009; 32(4): 784-792.