Journal of Engineering and Applied Sciences 12 (24): 7453-7457, 2017
ISSN: 1816-949X

Encryption Algorithm Selection to Protect IoT Devices from Local Network Attacking using Analytic Network Process and BCR Model

Thien Nguyen Phu and Young-Chan Lee
Department of Business Administration, Dongguk University, 38066 Seoul, Republic of Korea

Abstract: From the beginning, the importance of IoT device's security was not considered as it should be. Now, this issue poses challenges for smart device manufacturers and software developers to improve their device's reliability. This study used the combination between analytic network process methodology and Benefit-Cost-Risk (BCR a derived version of BCOR) Model. To evaluate and select the most appropriate encryption algorithms applied for IoT devices, this combination is very suitable: The strength of ANP approach, providing a mathematical and logical way to take decision without affection of human emotion, combined with BCR, a ranking tools model to find out the right decision. A lot of being-wearied-IoT-devices are still using unsecured connection such as Bluetooth or poor security encryption system. These are the gold mine for hacker to dig user's private information. The most efficient method is applying more secure connection method using reliable encryption algorithm without losing the performance and cost. And among types of encryption algorithms, each of them has its own strength and weakness, it is not easy for IoT devices maker and programmers to choose the good algorithm to deploy on their device. The security requirements in this study are based on IoT device users and programmers point of view. Therefore, this study keeps well the objectivity and suggests a good viewpoint to evaluate encryption method for IoT device. This framework provides a useful, significant and comprehensive tool for IoT software developer, hardware manufacturers to solve the same or similar security problems. This research will be valuable for IoT devices manufactures and IoT devices software developers to find the most economical and efficient way to secure their devices.

Key words: Internet of Things (IoT), local attacking, encryption algorithm, Analytic Network Process (ANP), BCR Model, cryptography

INTRODUCTION

In recent decades, Internet of Things (IoT) changed the way the businesses, governments, customers interact with the physical world. With the number of IoT devices reported to hit billions in the next couple of years (HPEDLP., 2015), households will become fully automated and interconnected and wearable will become vital in tracking and optimizing our daily activities. The IoT could prove transformative and there are huge possibilities for companies to be more efficient and bring exciting products to market. However, recent security research has shown many of these smart devices are prone to security vulnerabilities that might compromise user's privacy and even the entire network security of their household. Most have been deemed not only privacy hazards but they have also been tagged as inherently insecure by design. As the IoT market size increases research analyst gartner predicted there will be 26 billion units by 2020 hackers have an expanded surface area and protecting company intellectual property, customer data and operational infrastructures is more urgent than ever. According to IoT technology's outburst, the security issues have become a vital problem with all device manufacturers, software developers and users as well.

Encryption is the process of encoding information in such a way that hackers cannot read it. There are two types of encryption techniques; symmetric and asymmetric. Symmetric cryptography, also called private-key cryptography uses only one key for encryption and decryption. Asymmetric key cryptography, also called public-key cryptography requires special keys to encrypt and decrypt messages. Both symmetric and asymmetric cryptographic techniques offer advantages and disadvantages. Symmetric encryption techniques provide cost-effective and efficient methods of securing data without compromising security however; sharing the secret key is a problem. On the other hand, asymmetric techniques solve the problem of distributing the key for encryption

Corresponding Author: Young-Chan Lee, Department of Business Administration, Dongguk University, 38066 Seoul, Republic of Korea

however, they are slow compared to symmetric encryption and consume more computer resources. Therefore, the best possible solution for encryption is the complementary use of both symmetric and asymmetric encryption techniques. Hybrid encryption attempts to exploit the advantages of both kinds of techniques while avoiding their disadvantages (Rizk and Alkady, 2015). The purpose of this research is to suggest and clear, reasonable and efficient decision making framework to select the best encryption algorithm to protect IoT devices from local network attacking by using the analytic network process incorporated with BCR Model. We expect that the results of this research will be useful for IoT device software developer, manufacturer to improve the security of their devices.

LITERATURE REVIEW

Cryptographic mechanisms are one of the most important tools to protect IT applications, communication protocols and infrastructures. Cryptographic techniques enable a large number of security features: they include data confidentiality, data integrity, entity authentication and non-repudiation. The effectiveness of cryptographic protection depends on a variety of issues such as cryptographic key size, mechanism, protocol design, implementation aspects and password management. All of them are has similar importance. For example, if the key size is too small or mechanism is poorly designed or implementd incorrectly, or the shared key is poorly protected and deliveried, the security of a system is at risk. In most of cases, the mechanism design and key size get most attention; however, most sussessful attacks are not due to inadequate mechanism strengths or keysize but to other deficiencies. In this research we tried to explore all of such deficiencies and suggest a mathematical point of view about secure IoT devices over network.

IoT device: Physical devices, vehicles, buildings, clothes, hand watch and other items-embedded with electronics, software, sensors, actuators and network connectivity that enable these objects to collect and exchange data calledIoT devices. They are smart phones, smart houses, cars, sensors, watches or eye glasses etc. And connecting methods are bluetooth, wifi network, cable network and so on.

Analytic network process: The Analytic Network Process (ANP) is a more general form of the Analytic Hierarchy Process (AHP) used in multi-criteria decision analysis (Saaty, 1996). AHP structures a decision problem into a hierarchy with a goal, decision criteria and alternatives while the ANP structures it as a network. Both then use a system of pairwise comparisons to measure the weights of the components of the structure and finally to rank the alternatives in the decision (Saaty, 1996). ANP is a mathematical theory that allows one to reduce dependency and systematic feedback that can capture and combine the tangible and intangible factors (Azis, 2003). A holistic approach in which all the clusters of parameters involved are laid out in a network system that allows for dependencies (Godse *et al*., 2008). ANP approach to qualitative methods, used for the process of decision-making and provide a common framework in treating decisions without making assumptions about the independence of the elements at higher levels of the elements with the low levels and the independence of the elements in one level itself.

BCR Model: In BCR approach, the alternatives are pairwise compared with respect to each criterion on the lowest level of each hierarchy; their derived priorities are expressed on a ratio scale as well again usually normalized to the unity sum per criterion. Synthesis of the alternative priorities and the criteria weights using a weighted sum produces composite alternative priorities for each hierarchy (Millet and Wedley, 2002). For each alternative, its composite benefit priority is then divided by its composite cost priority. The resulting ratio value serves as a means to rank the alternatives and choose the best one, i.e. The alternative with the highest benefit/cost-priority ratio (Wijnmalen, 2007). Examples of benefit/cost analysis using the ANP were published in (Saaty, 1980, 2000).

In other research (Wijnmalen, 2007) discussed about Benefit, Cost, Risk (BCR) Model and the helpfulness against ANP Model find out the right decision. It is a good way to find out a good encryption algorithm by considering alternative's benefit, cost and risk.

Data encryption algorithms

Symmetric key cryptography: This algorithm uses only one key for encrypting and decrypting data. So, there is potential risk in sharing the key progress. Symmetric key cryptography uses a trivially related, identical key instead of two key, i.e., public and private key for encryption and decryption. In symmetric key cryptography sender encrypts the plain text using a secret key and receiver decrypt the cipher text using the same key. So, there is a requirement to send the guarded key to the receiver along with the cipher text. Secrecy of information in symmetric key cryptography depends on the secrecy and size of

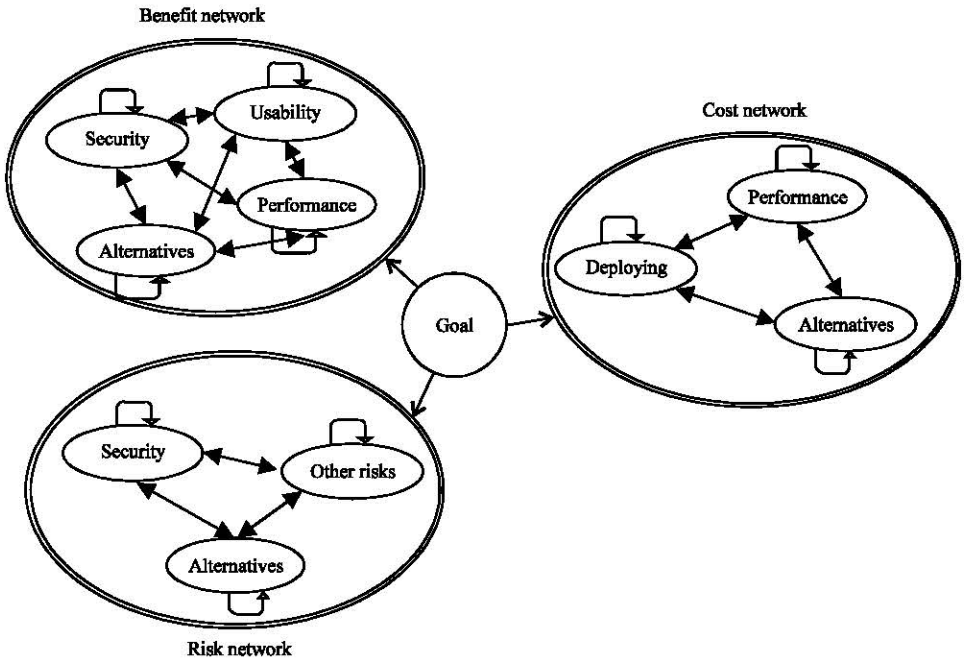

Fig. 1: The research model

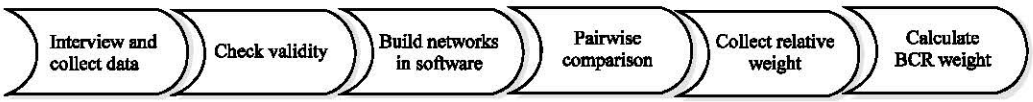

Fig. 2: The detail steps in empirical research

secret key (Chandra *et al*., 2015). Some example of this algorithm is DES, 3DES, DESX, AES, Blowfish and so on.

Asymmetric key cryptography: According to Chandra *et al*. (2014), the asymmetric key cryptography is known as public key cryptography. Asymmetric key cryptography use two different keys, i.e., public and private key which are complementary in function. The communication data which is encrypted using public key, can only be decrypted using the corresponding private key (Chandra *et al*., 2015). In this technique, the sender uses a public key of the receiver for encryption and the receiver uses his private key to decrypt the message. Common Asymmetric key algorithm system are RSA, D-H, DSA, ECC.

Hybrid encrytion algorithm: Both of above algorithms have their own strength and weakness, so, Alkady *et al*. (2013) has suggested the using of hybrid algorithm to deal with each disadvantage of them. A hybrid cryptosystem is one which combines the convenience of a public-key (asymmetric) cryptosystem with the efficiency of a symmetric-key cryptosystem. Some example of hybrid encryption systems are openpgp, SSL, TLS XOR-Dual RSA.

Research model: Figure 1 shows the research model.

PROPOSED WORK

In this research, we used super decision Version 2.7 as a support tool. Whenever making a decision with AHP or ANP methodology, super decision is the most powerful tool designed specifically for AHP and ANP theory. Qing *et al*. (2012) has applied this software and ANP theory in their research. Their research proved super decision software package is powerful and suitable to solve decision making problem with AHP or ANP methodology. Based on the ANP and BCR Model for selecting the most appropriate encryption algorithm discussed in above section, the network criterions collected via interviews will be passed into super decision software as research networks. The research progress is shown as "Fig. 2".

Step 1; Interview and collect data: The interview questionnaire was sent to the respondents, include IoT

software developers, manufactures and user as well. The respondents answered the questionnaire by explaining their judgment for each pair of criterions. This research, we used the questionnaire base on nine-point scale from equally important (1 point) to extremely more important than (9 points). The respondents then performed pair wise comparison between criterions of cluster and between clusters follow this scale. For more reliability, we prepared a sample answer as instruction for respondents. They can look and follow the sample to answer more correctly the question. Then the pair wise comparison result is gathered.

Step 2; Check validity: When the respondent's answered data received, the data was checked for validity before being used. All of comparison data of each respondent was passed into the Super Decision Version 2.7 Software packages. Then the validity of answered data checked by considering the inconsistency value. In ANP theory, the inconsistency ratio must be <0.1 to ensure the validity of data. This value is automatically calculated by software. Thus, all of answers have inconsistency ratio >0.1 must be rejected. In this research, we only used valid answers of respondents.

Step 3; Build networks in software: Networks of security requirements and relationship between them were built in super decision software. Each network has its own cluster and criterions underneath. Clusters and criterions are built based on the requirements of users, devices manufactures or software developer's point of view, thus the objectivity is conserved.

Step 4; Pairwise comparison: The early step's answer of each question was used to calculate geometric mean value. This value was used as the most common answer of respondents. These values are data that, we set when perform pair wise comparison in super decision software.

Step 5; Collect relative weight: When all necessary data passed into the super decision software, the weights of criterion, cluster and alternatives are automatically calculated. First, all pair wise comparison data of elements within clusters of each network will be synthesized using eigenvalue method and put into super matrix table. The super matrix table then will be multiplied with cluster's weigh in respect to the network to form the weighted super matrix. Finally, the weighted super matrix is raised to power to get limiting matrix. The weight of elements in limiting matrix is the relative weight. The relative weight of elements is displayed as Table 1. According to relative weight table, the hybrid alternative has greatest score, followed by asymmetric (0.26458) and symmetric (0.18253). In benefit network in cost network, the greatest score alternative is symmetric with 0.4235 then asymmetric (0.3201), hybrid (0.2564). And in risk network symmetric with 0.41665 score, hybrid with 0.3199 is at 2nd position, the last one is asymmetric with 0.26345.

Table 1: Relative weight of cluster's element

Network/Cluster	Name	Normalized by cluster	Limiting
Benefit network			
Alternatives	Asymmetric	0.26458	0.07148
	Hybrid	0.55286	0.14936
	Symmetric	0.18256	0.04932
Performance	Latency	0.35600	0.08221
	Memory Efficiency	0.33582	0.07755
	Speed	0.30819	0.07117
Security	Bruce speed	0.22210	0.05451
	Key size	0.77790	0.19092
Usability	Compatibility	0.51840	0.1314
	Controllability	0.39839	0.10098
	Implement ability	0.08321	0.02109
Cost network			
Alternatives	Asymmetric	0.32010	0.02613
	Hybrid	0.25640	0.02093
	Symmetric	0.42350	0.03457
Deploying	Cost	0.41920	0.16164
	Resources	0.39731	0.1532
	Time	0.18349	0.07075
Performance	Latency	0.23854	0.12709
	Memory Efficiency	0.76146	0.4057
Risk network			
Alternatives	Asymmetric	0.26345	0.07071
	Hybrid	0.31990	0.08586
	Symmetric	0.41665	0.11183
Other risks	Controllability	0.41613	0.15269
	System crash	0.40512	0.14865
	User ability	0.17875	0.06559
Security	Bruce speed	0.30022	0.10948
	Key delivery	0.08260	0.03012
	Key size	0.50308	0.18346
	Key storing	0.11410	0.04161

Table 2: The final score of alternatives

Alternatives	Benefit score	Cost risk score	Final score
Asymmetric	0.26458	0.08433	3.13742
Hybrid	0.55286	0.08202	6.74036
Symmetric	0.18256	0.17645	1.03462

Step 6; Calculate BCR weight: In BCR Model theory, the final score of each alternative is calculated with the following equation:

$$W_{Alternative} = W_{benefit}/(W_{cost} \times W_{risk})$$

Thus, based on the relative weight shown in above step, we calculated the final score of each alternative, shown in Table 2.

Finally, Table 3 shows the sequence of alternative's weight by each network and compare to final score sequence.

Table 3: Alternative's sequence

Network	1st	2nd	3rd
Benefit	Hybrid	Asymmetric	Symmetric
	0.55286	0.26458	0.18256
Cost	Symmetric	Asymmetric	Hybrid
	0.4235	0.3201	0.2564
Risk	Symmetric	Hybrid	Asymmetric
	0.41665	0.3199	0.26345
Final	Hybrid	Asymmetric	Symmetric
	6.740357142	3.137423427	1.034619897

CONCLUSION

Both symmetric and asymmetric cryptography has their own advantages and disadvantages, the hybrid algorithm can combine the convenience of a public-key (asymmetric) cryptosystem with the efficiency of a symmetric-key cryptosystem to form a better encryption algorithm. Therefore, hybrid encryption algorithm should be used to encrypt the communication data between IoT devices. Through this study, programmers or IoT device manufacturers can more exactly evaluate and choose good encryption method for their devices communication, build the rational and consistent networks to rightly point out the concerns of IoT devices security problems and the assessment in respect to benefit-cost-opportunity-risk dimension.

The ANP methodology has been shown to be a powerful technique to solve the decision making problem in general and to choose the appropriate encryption algorithm in particular. It means, we totally can apply this useful tool for other decision making problem as well. With the support of super decision software and BCR Model, it is easy to solve the complex problems such as resource allocation, planning, making choice, investment decision and so on. All practitioners have to do is just construct the networks, determine relationship between elements and perform pair wise comparison.

Also, through this research, researchers not only gain the knowledge about IoT devices, encrypt cryptography, security but also the knowledge about ANP theory as well. They totally can apply this scientific methodology in security or IoT research domain.

This framework provides a useful, significant and comprehensive tool for IoT software developers, hardware manufacturers to solve the same or similar security problems, the practitioners can apply it flexibly (modify the clusters, change the elements and upgrade the networks or even though make their own framework). The researchers could get an idea to utilize the different other scientific methodologies like AHP, BCOR, ANP or enhance the finding in this study by continuing the further research.

REFERENCES

Alkady, Y., M.I. Habib and R.Y. Rizk, 2013. A new security protocol using hybrid cryptography algorithms. Proceedings of the 2013 9th International Conference on Computer Engineering Conference, December 28-29, 2013, IEEE, Giza, Egypt, ISBN:978-1-4799-3370-9, pp: 109-115.

Azis, I.J., 2003. Analytic network process with feedback influence: A new approach to impact study. University of Illinois at Urbana-Champaign, Champaign County, Illinois.

Chandra, S., B. Mandal, S.S. Alam and S. Bhattacharyya, 2015. Content based double encryption algorithm using symmetric key cryptography. Procedia Comput. Sci., 57: 1228-1234.

Chandra, S., S. Paira, S.S. Alam and G. Sanyal, 2014. A comparative survey of symmetric and asymmetric key cryptography. Proceedings 2014 International Conference on Electronics, Communication and Computational Engineering, November 17-18, 2014, IEEE, Hosur, India, ISBN:978-1-4799-5748-4, pp: 83-93.

Godse, M., R. Sonar and S. Mulik, 2008. Web service selection based on analytical network process approach. Proceedings of the 2008 IEEE Conference on Asia-Pacific Services Computing, December 9-12, 2008, IEEE, Yilan, Taiwan, ISBN: 978-0-7695-3473-2, pp: 1103-1108.

HPEDLP., 2015. Internet of things research study. Hewlett Packard Enterprise Development LP, Palo Alto, California.

Millet, I. and W.C. Wedley, 2002. Modelling risk and uncertainty with the analytic hierarchy process. J. Multi Criteria Decis. Anal., 11: 97-107.

Qing, H.H., L. Lan, W. Jian, K.L. Yong and Z. Lei, 2012. Using analytic network process to analyze influencing factors of project complexity. Proceedings of the 2012 International Conference on Management Science and Engineering, September 20-22, 2012, IEEE, Dallas, Texas, ISBN:978-1-4673-3015-2, pp: 1781-1786.

Rizk, R. and Y. Alkady, 2015. Two-phase hybrid cryptography algorithm for wireless sensor networks. J. Electr. Syst. Inf. Technol., 2: 296-313.

Saaty, T., 1996. Decision Making with Dependence and Feedback: The Analytic Network Process: the Organization and Prioritization of Complexity. 2nd Edn., RWS Publications, Pittsburgh, ISBN: 13-9780962031793, Pages: 370.

Saaty, T.L., 1980. The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation. McGraw-Hill, New York, USA., ISBN-13: 9780070543713, Pages: 287.

Wijnmalen, D.J., 2007. Analysis of benefits, opportunities, costs and risks (BOCR) with the AHP-ANP: A critical validation. Math. Comput. Modell., 46: 892-905.