An Overview of Risk Estimation Techniques in Risk-based Access Control for the Internet of Things

Hany F. Atlam[1, 2], Ahmed Alenezi[1], Robert J. Walters[1] and Gary B. Wills[1]
[1]*Electronic and Computer Science Dept., University of Southampton, University Road, SO17 1BJ, Southampton, U.K.*
[2]*Computer Science and Engineering Dept., Faculty of Electronic Engineering, Menoufia University, 32952, Menouf, Egypt*

Keywords: Internet of Things, Security Risk, Access Control, Risk Estimation, Risk-based Access Control.

Abstract: The Internet of Things (IoT) represents a modern approach where boundaries between real and digital domains are progressively eliminated by changing over consistently every physical device to smart object ready to provide valuable services. These services provide a vital role in different life domains but at the same time create new challenges particularly in security and privacy. Authentication and access control models are considered as the essential elements to address these security and privacy challenges. Risk-based access control model is one of the dynamic access control models that provides more flexibility in accessing system resources. This model performs a risk analysis to estimate the security risk associated with each access request and uses the estimated risk to make the access decision. One of the essential elements in this model is the risk estimation process. Estimating risk is a complex operation that requires the consideration of a variety of factors in the access control environment. Moreover, the interpretation and estimation of the risk might vary depending on the working domain. This paper presents a review of different risk estimation techniques. Existing risk-based access control models are discussed and compared in terms of the risk estimation technique, risk factors, and the evaluation domain. Requirements for choosing the appropriate risk estimation technique for the IoT system are also demonstrated.

1 INTRODUCTION

The Internet of Things (IoT) is growing in different ways. It is considered the next stage of the evolution of the Internet. In addition, the IoT is moving towards a stage in which all items around us will be connected to the Internet and will have the ability to communicate with each other with the minimum human intervention (Shanbhag and Shankarmani, 2015). The IoT faces many challenges that stand as a barrier to the successful implementation of IoT applications. Security and privacy are considered the most difficult challenges that need to be addressed. These challenges are complicated due to the dynamic and heterogeneous nature of the IoT system (Shaikh et al., 2012; Ricardo dos Santos et al., 2013). Authentication and access control models are the essential elements to address security and privacy challenges in the IoT. They prevent unauthorized users from gaining access to system resources, prevent authorized users from accessing resources in an unauthorized manner whilst still allowing authorized users to access resources in an authorized manner (Chen et al., 2007; Yin et al., 2006).

Due to the dynamic nature of the IoT, traditional access control approaches cannot provide the necessary security levels as they are context insensitive and require a complex authentication infrastructure. Dynamic access control approaches are more appropriate to IoT systems. This is because they are characterized by using not only the policies but also environment features that are estimated in real-time to determine access decisions. The dynamic features can include trust, risk, context, history and operational need (Kulk et al., 2009; Ni et al., 2010).

A risk-based access control model is one of the dynamic models that permit or deny access requests dynamically based on the estimated risk of each access request (Chen et al., 2007). This model performs a risk analysis on each user access request to make the access decision (Dos Santos et al., 2014). Risk estimation process is one of the primary tasks in the risk-based access control model. This process is concerned with estimating the risks that have been specified and creating the data that will be needed for making decisions. The objective of the estimation

Atlam, H., Alenezi, A., Walters, R. and Wills, G.
An Overview of Risk Estimation Techniques in Risk-based Access Control for the Internet of Things.
DOI: 10.5220/0006292602540260
In *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security (IoTBDS 2017)*, pages 254-260
ISBN: 978-989-758-245-5

process is to establish a way of arranging risks in the order of importance and using the risk numeric values for making the decision (Yin et al., 2006).

The main objective of this paper is to provide a review of different risk estimation techniques that have been used in existing risk-based access control models. Furthermore, discussing requirements for choosing the appropriate risk estimation technique for the IoT system.

The rest of this paper is organized as follows: Section II presents the concept of the access control and different access control models; Section III presents the risk-based access control model; Section IV presents different risk estimation techniques; Section V discusses the IoT requirements to determine the appropriate risk estimation technique, and Section VI is the conclusion 2.

2 ACCESS CONTROL MODELS

To ensure confidentiality and integrity of system resources, an access control is used to guarantee that only authorized users granted the appropriate access permissions. There are several access control models which can be divided into two classes; traditional and dynamic access control models (Liu et al., 2012; Ye et al., 2014).

Traditional access control approaches are based on policies that are static and rigid in nature. These policies are predefined and always give the same outcome regardless of the situation. This static approach fails to adapt to varied and changing conditions when making access decisions in the IoT system (Chen et al., 2007). There are three main traditional access control models; Discretionary Access Control (DAC), Mandatory Access Control (MAC) and Role-based Access Control (RBAC). On the other hand, dynamic access control approaches are appropriate to the IoT system. This is because they take into consideration not only access policies to make access decisions, but also dynamic contextual features which are estimated in real-time at the time of making the access request. These real-time features can include trust, risk, context, history and operational need (Kulk et al., 2009; Ni et al., 2010).

Using the security risk to make the access decision is a promising research point in the IoT. The NIST (Stoneburner et al., 2002) surveyed different access control models in terms of flexibility as shown in Figure 1. It showed that Risk Adaptable Access Control (RAdAC) model provides more flexibility in accessing system resources which make it as a suitable model for the IoT.

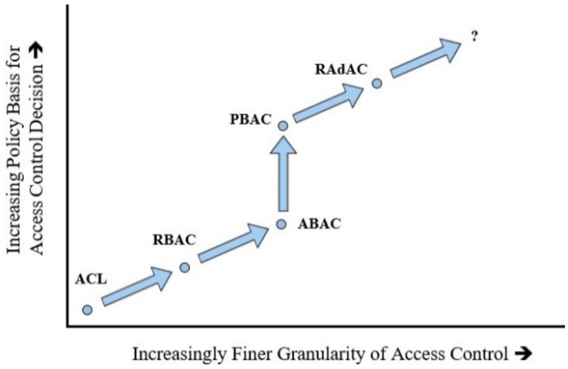
Increasing Policy Basis for Access Control Decision ➔
ACL
RBAC
ABAC
PBAC
RAdAC
?
Increasingly Finer Granularity of Access Control ➔

Figure 1: Progression of access control models in term of flexibility (Zhi et al., 2009).

3 RISK-BASED ACCESS CONTROL MODEL

The risk can be defined as the possibility of loss or injury. Generally, the risk is about some event that may occur in the future and cause losses. One such risk is the leakage of sensitive information by users. An access control is one of the approaches used to mitigate against the security risk (Langaliya and Aluvalu, 2015). Risk-based access control model permits or denies access requests dynamically based on the estimated risk of each access request (Chen et al., 2007). This model performs a risk analysis on each user access request to make the access decision (Dos Santos et al., 2014). Mathematically, the most common formula to represent the risk in quantitative terms is:

$$\text{Quantified Risk} = \text{Likelihood} \times \text{Impact} \qquad (1)$$

Where likelihood represents the probability of an incident to happen while impact represents the estimation of the value of the damage regarding that incident (Chen et al., 2007).

There are several approaches for creating risk-based access control models. These approaches share some general characteristics from diverse models. An overview of the risk-based access control model is shown in Figure 2. There are three modules. The access control manager is the main module. It receives requests from users, analyses them, collects other context parameters and sends the data to risk estimation module. The risk estimation module is the key part of the model. It estimates risk values based on the input data collected by the context retrieval module. After that, the access decision is made for each access request based on the estimated risk value (Diep et al., 2007).

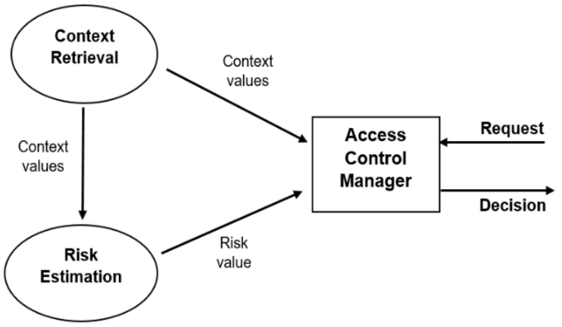

Figure 2: Risk-based access control overview (Diep et al. 2007).

4 RISK ESTIMATION TECHNIQUES

The security risk can be used as an access control feature where a risk analysis is performed on each access request to make the access decision (Dos Santos et al., 2014). The security risk can be defined as the potential damage that can emerge from an operation and is generally represented by the probability of occurrence of an undesired incident multiplied by its impact.

Clearly, the essential stage of developing a risk-based access control model in the IoT is the risk estimation process that based on the possibility of an information leakage in the future and the value of this information. The risk is estimated in different ways. The objective of the risk estimation operation is to create a way of arranging risks in the order of importance and use risk numeric values for making the decision. The risk estimation process can be qualitative or quantitative (Yin et al., 2006). In this paper, only quantitative risk estimation techniques will be discussed. Quantitative risk estimation attempts to attach specific numerical or linguistic values to risks. These values can be like very risky, not so risky; high, low, medium, high medium, and low medium. Numerical techniques for decision analysis are used in this approach (Kulk et al., 2009). Quantitative risk estimation techniques are preferred since it results in a numeric value for the risk.

Risk estimation process faces many challenges for various reasons. For instance, the goal of the risk estimation process is to predict the future possibility of information disclosure that results from the current access. Determining such a possibility is not an easy task (Habib and Leister, 2015). Moreover, if the estimation has relied on incomplete or imprecise information and knowledge about relevant risk features, it will result in difficulties in identifying the value of information (Ni et al., 2010). Therefore, a complete investigation about different risk estimation techniques that are related to dynamic access control models needs to be performed so as to select the appropriate risk estimation technique for the IoT. An overview of the most common risk estimation techniques is provided in this section. These techniques are as follows:

4.1 Fuzzy Logic

Fuzzy logic is a set of mathematical rules for representing the knowledge that based on degrees of membership. It manages degrees of membership and degrees of truth. Moreover, it ensures that we do not neglect human common sense, intuition, and experiences (Li et al., 2013). Fuzzy logic and fuzzy set operations enable characterization of defined fuzzy sets of likelihood and consequence severity and the mathematics to combine them using expert knowledge (Abul-Haggag and Barakat, 2013). A typical fuzzy logic estimation process comprises of three stages: (1) Fuzzification of inputs, (2) Imprecise reasoning using fuzzy rules, and (3) Defuzzification of outputs. Input and output parameters can be either linguistic or numeric. Fuzzification is the process of finding the membership of an input variable with a linguistic term. While the membership function can be either defined by experts or analytically extracted from data, and fuzzy rules are usually defined by experts. Finally, defuzzification provides a crisp number from the output fuzzy set (Pokorádi, 2002).

Many researchers are attracted to use the fuzzy logic to estimate the risk in access control models. Chen et al. (2007) used the fuzzy logic to build a fuzzy Multi-Level Security (MLS) access control model to allow humans to access information from IBM systems. This fuzzy MLS model estimates the risk of the access request based on differences between the subject security level and the object security level. For instance, the larger the difference is, the higher the risk is. The result is described as a real number in the interval [0, 1], where 1 represents an absolute deny (the highest risk), and 0 represents an absolute permit (the lowest risk). The fuzzy MLS model further divides the interval [0, 1] into n subintervals referred to as risk bands. If the risk of an access request is evaluated to a band, then the request is allowed only if the risk mitigation measures associated with the band are applied. Also, Li et al. (2013) presented a fuzzy modelling-based approach for evaluating the risk associated with the access request of a healthcare information access. In this model, the risk value that is associated with the data sensitivity, action severity, and risk history is determined as a fuzzy value, which is used to determine appropriate controls of the healthcare information access in a cloud environment. This model showed that the fuzzy logic approach can generate accurate and realistic outcomes in assessing current risk and forecasting the scope and impact of different risk factors. Ni et al. (2010) introduced a fuzzy inference technique to estimate the risk. This approach is used for estimating access risks and develop an enforcement mechanism for the risk-based access control model. The estimated risk is computed by using the object security level and the subject security level. However, the scalability of the fuzzy inference-based access control model faces some issues. The fuzzy inference system needs large time to estimate risks especially when there are tens of parameters and hundreds of fuzzy rules. Furthermore, the access control model may need to serve billions of users. Therefore, a fuzzy inference-based access control model might be too computationally expensive.

4.2 Risk Assessment

Risk assessment is one of the most important processes in the risk management methodology. People use the risk assessment to define the extent of the potential threat and the risk associated with an IT system. The goal of the risk assessment is to determine the risk context and acceptability that can be done by comparison to similar risks. The type of risk analysis should be appropriate for the available data and severity of potential loss. A successful risk assessment offers many advantages. For instance, a well-defined assessment of risks can provide a rational basis for injury prevention and exposure prevention (Stoneburner et al., 2002).

The risk assessment has been used in the existing risk-based control models. For instance, Khambhammettu et al. (2013) introduced three different approaches that conduct a risk assessment framework for the risk-based access control. The three approaches are based on the object sensitivity level, the subject trustworthiness level and the difference between object sensitivity and subject trustworthiness. This framework demonstrated that risk estimates differ based on the risk assessment approach that has been selected. The selected approach can be based on the context of the application or the priority of organizations. Moreover, Diep et al. (2007) proposed an approach for access control that based on risk assessment and context. The risk assessment estimates the risk value based on outcomes of actions in term of availability, confidentiality, and integrity and context of the user, environment, and resource. The risk value is compared with the threshold, and then access control manager returns the decision.

4.3 Game Theory

Game theory is a branch of applied mathematics that has been used in many fields like economics, political science, evolutionary biology, information security and artificial intelligence. Game theory consists of four elements: the players, their strategies, payoffs and the information they have. The players are the strategic decision makers within the context of the game. Whereas, the strategy is the plan that the player has to use in response to the contender's movement. Therefore, it is essential to find out the appropriate strategies for the players. The payoff of a given player is affected by both the actions performed by him and the other player (Rajbhandari and Snekkenes, 2011). Using game theory, the risk analysis can be based on priority or values related to benefit which users can provide rather than the probability. In addition, it can be used in situations where no actuarial data is available. This may increase the quality and suitability of the overall risk analysis operation (Hamdi and Abie, 2014).

Game theory has been used in the risk-based access control. Rajbhandari and Snekkenes (2011) presented a risk analysis approach that based on preferences or values of benefit which the subjects can provide rather than subjective probability using the game theory. Moreover, a simple privacy scenario between a user and an online bookstore is introduced to provide an initial perception of the concept.

4.4 Decision Tree

A decision tree model is used to simplify decision making based on a set of rules presented as a tree. It uses the attributes of objects for classification and decision. To develop a decision tree model, data are divided into training and validation sets. Training data are used to identify appropriate rules and find the best partition for certain attributes using techniques such as recursive partitioning. While validation data are used to validate the decision tree and make necessary adjustments to the tree (Shang and Hossen, 2013).

Decision tree paradigms are easy to understand

and valuable for classification. They can work well with insufficient data if all the rules can be determined by experts. However, in a classical decision tree model, the partition of attribute values is based on classical set theory. A small change in the value of an attribute could lead to a different conclusion due to the discreteness of the partition. Moreover, when the scale of the decision tree becomes large, it will be difficult to understand and more data will be needed to identify and validate the rules (Wang et al., 2016).

4.5 Monte Carlo Simulation

The Monte Carlo Simulation (MCS) is a very powerful method for estimating risks of a system by calculating risks of hundreds or thousands of possible scenarios. It produces a complete probability distribution associated with risks and can provide very realistic results. In the MCS method, the system random behaviour is represented by performing a set of experiments on the system in the form of simulations (Goerdin et al., 2015a). The MCS method requires high computing power and have become increasingly interesting due to the availability of high-speed computers. An advantage of the MCS is that it can work with large complex systems. Moreover, it can process the probabilistic behaviour of multiple inputs to the system which in the analytical technique are supposed to be constant values (Goerdin et al., 2015b).

4.6 Expert Judgment

Expert judgment is an important source of information in risk estimation in risk-based decision-making processes that rely significantly on a quantitative risk assessment that requires numerical data describing the event frequencies and conditional probabilities in the risk model (Kahneman et al., 1974). In some cases, it will be very difficult to quantify the risk value using traditional methods but with an expert judgment, a correct value regarding a specific scenario can be specified. Security experts are asked to define a weight for the potential damage regarding a specific security breach associated with risk factors. Experts should be selected from diverse fields to provide different points of views. In order for the risk-based access control model to be valuable, a larger number of experts in each field would need to be interviewed (Pluess et al., 2013).

This section provides a summary of the risk-based access control models that mentioned earlier as shown in Table 1. It contains the risk estimation technique that has been used, risk factors used to estimate the risk value and the domain where the model is evaluated.

Table 1: Some of the risk-based access control models.

Risk models	Risk Estimation Technique	Risk factors	Domain
(Chen et al. 2007)	Fuzzy MLS Model	Difference between subject security level and object security level	IBM System
(Li et al. 2013)	Fuzzy Model	Data sensitivity, action severity, and user risk history	EHealth
(Ni et al. 2010)	Fuzzy Inference	Object security level and subject security level	Numeric Example
(Khambhammettu et al. 2013)	Risk Assessment	Object sensitivity, subject trust, and Difference between object sensitivity and subject trust	Numeric Example
(Diep et al. 2007)	Risk Assessment	Outcomes of actions	A case study of a hospital
(Rajbhandari & Snekkenes 2011)	Game Theory	Access benefits of the subject	Scenarios of online bookstore

5 RISK ESTIMATION TECHNIQUE FOR THE IoT

The distributed and dynamic nature of the IoT system demands many requirements that should be taken into consideration when choosing the appropriate risk estimation technique of the risk-based access control model for the IoT system. These requirements include:

- *Dynamic interaction*: The access control model required for the IoT should not be static and predefined. It should be adjustable, predictable, and specified in a dynamic and continuous way by considering context changing during the access control process (Fremantle et al., 2014). Hence, the risk estimation technique should have the ability to adapt to environment changes and uses real-time contextual information.
- *Scalability:* The IoT system connects billions of devices. The increasing rate of newly connected objects should be taken into

consideration when selecting the risk estimation technique. Also, the performance should not be affected.

- *Limited resources:* The resources associated with IoT devices such as energy, memory, and processing power are limited due to the small size of these devices (Adda et al., 2015). Therefore, the risk estimation technique should support efficient solutions.
- *Data availability:* In order to accurately calculate the risk associated with a particular factor, data is needed. Once real world data is collected, it can be used in various probability distributions to calculate a much more accurate risk value. So the availability of the proper data will allow to analytically determine the appropriate risk estimation technique for the IoT.

6 CONCLUSIONS

The IoT has become the current technology revolution that is intended to convert the existing environment into a more pervasive and ubiquitous domain. The successful deployment of the IoT in our environment is related to conquer security and privacy issues specifically authentication and access control issues. Risk-based access control model provides a dynamic and efficient way to make the access decision depending on the risk estimates of each access request. Risk estimation is a complex operation that requires the consideration of a variety of factors in the access control domain. Selecting the appropriate risk estimation technique for the IoT is not an easy task. In this paper, we provided an overview of different risk estimation techniques that are used in existing risk-based access control models. Also, we have presented some of the IoT requirements for selecting the appropriate risk estimation technique. Our future direction would be to empirically compare among these risk estimation techniques to select the most appropriate technique for the IoT system. However, the lack of the proper data will be a big issue.

ACKNOWLEDGEMENTS

We acknowledge Egyptian cultural affairs and mission sector and Menoufia University for their scholarship to Hany Atlam that allows the research to be undertaken.

REFERENCES

Abul-Haggag, O.Y. & Barakat, W., 2013. Application of Fuzzy Logic for Risk Assessment using Risk Matrix. *International Journal of Emerging Technology and Advanced Engineering*, 3(1), pp.49–54.

Adda, M. et al., 2015. Toward an Access Control Model for IOTCollab. *The 6th International Conference on Ambient Systems, Networks and Technologies*, 52(Ant), pp.428–435.

Chen, P. et al., 2007. Fuzzy Multi – Level Security : An Experiment on Quantified Risk – Adaptive Access Control. *2007 IEEE Symposium on Security and Privacy(SP'07)*, pp.222–227.

Diep, N.N. et al., 2007. Enforcing Access Control Using Risk Assessment. *the Fourth European Conference on Universal Multiservice Networks*, pp.419–424.

Fremantle, P. et al., 2014. Federated Identity and Access Management for the Internet of Things. *2014 International Workshop on Secure Internet of Things (SIoT)*, pp.10–17.

Goerdin, S.A. V, Smit, J.J. & Mehairjan, R.P.Y., 2015a. Monte Carlo simulation applied to support risk-based decision making in electricity distribution networks. *2015 IEEE Eindhoven PowerTech, PowerTech 2015*.

Goerdin, S.A. V, Smit, J.J. & Mehairjan, R.P.Y., 2015b. Monte Carlo simulation applied to support risk-based decision making in electricity distribution networks. *2015 IEEE Eindhoven PowerTech*.

Habib, K. & Leister, W., 2015. Context-Aware Authentication for the Internet of Things. *The Eleventh International Conference on Autonomic and Autonomous Systems fined*, pp.134–139.

Hamdi, M. & Abie, H., 2014. Game-based adaptive security in the Internet of Things for eHealth. *2014 IEEE International Conference on Communications, ICC 2014*, pp.920–925.

Kahneman, D., Slovic, P. & Tversky, A., 1974. Judgment under uncertainty: heuristics and biases. *Science*, 185(4157), pp.1124–1131.

Khambhammettu, H. et al., 2013. A framework for risk assessment in access control systems. *Computers & Security*, 39(Sec 2012), pp.86–103.

Kulk, G.P., Peters, R.J. & Verhoef, C., 2009. Quantifying IT estimation risks. *Science of Computer Programming*, 74(11–12), pp.900–933.

Langaliya, C. & Aluvalu, R., 2015. Enhancing Cloud Security through Access Control Models : A Survey. *International Journal of Computer Applications*, 112(7), pp.8–12.

Li, J., Bai, Y. & Zaman, N., 2013. A fuzzy modeling approach for risk-based access control in eHealth cloud. *Proceedings - 12th IEEE International Conference on Trust, Security, and Privacy in Computing and Communications, TrustCom 2013*, pp.17–23.

Liu, J., Xiao, Y. & Chen, C.L.P., 2012. Authentication and access control in the Internet of things. *Proceedings - 32nd IEEE International Conference on Distributed Computing Systems Workshops, ICDCSW 2012*, pp.588–592.

Ni, Q., Bertino, E. & Lobo, J., 2010. Risk-based access control systems built on fuzzy inferences. *in Proceedings of the 5th ACM Symposium on Information, Computer, and Communications Security, ser. ASIACCS 10. New York, NY, USA: ACM*, pp.250–260.

Pluess, D., Groso, A. & Meyer, T., 2013. Expert Judfgement in Risk Analysis: A Strategy to Overcome Uncertainities. *Chemical Engineering Transactions*, 31, pp.307–312.

Pokorádi, L., 2002. Fuzzy logic-based risk assessment. *Academic and Applied Research in Military Science*, 1(1), pp.63–73.

Rajbhandari, L. & Snekkenes, E.A., 2011. Using game theory to analyze risk to privacy: An initial insight. *Privacy and Identity Management for Life, Springer Berlin Heidelberg*, pp.41–51.

Ricardo dos Santos, D., Westphall, C.M. & Westphall, C.B., 2013. Risk-based Dynamic Access Control for a Highly Scalable Cloud Federation. *Proceedings of the Seventh International Conference on Emerging Security Information, Systems and Technologies (SECUREWARE 2013)*, pp.8–13.

Dos Santos, D.R., Westphall, C.M. & Westphall, C.B., 2014. A dynamic risk-based access control architecture for cloud computing. *IEEE/IFIP NOMS 2014 - IEEE/IFIP Network Operations and Management Symposium: Management in a Software Defined World*, pp.1–9.

Shaikh, R.A., Adi, K. & Logrippo, L., 2012. Dynamic risk-based decision methods for access control systems. *Computers and Security*, 31(4), pp.447–464.

Shanbhag, R. & Shankarmani, R., 2015. Architecture for Internet of Things to minimize human intervention. *2015 International Conference on Advances in Computing, Communications, and Informatics, ICACCI 2015*, pp.2348–2353.

Shang, K. & Hossen, Z., 2013. Applying Fuzzy Logic to Risk Assessment and Decision-Making. *Casualty Actuarial Society, Canadian Institute of Actuaries, Society of Actuaries*, pp.1–59.

Stoneburner, G., Goguen, A. & Feringa, A., 2002. Risk Management Guide for Information Technology Systems. *Nist Special Publication Sp*, 30(30).

Stoneburner, G., Goguen, A. & Feringa, A., 2002. Risk Management Guide for Information Technology Systems. *Nist Special Publication*, 19, p.58.

Wang, S. et al., 2016. A Vertical Handoff Method via Self-Selection Decision Tree for Internet of Vehicles. *IEEE Systems Journal*, 10(3), pp.1183–1192.

Ye, N. et al., 2014. An efficient authentication and access control scheme for perception layer of internet of things. *Applied Mathematics and Information Sciences*, 8(4), pp.1617–1624.

Yin, J. et al., 2006. On estimating the security risks of composite software services. *In First Program Analysis for Security and Safety Workshop Discussion (PASSWORD 2006).*

Zhi, L., Jing, W. & Xiao-su, C., 2009. Research on Policy-based Access Control Model. , (1), pp.164–167.