Thesis no: MSCS-2016-09

User Behavior Trust Based Cloud Computing Access Control Model

Qin Jiangcheng

Faculty of Computer
Blekinge Institute of Technology
SE - 371 79 Karlskrona Sweden

This thesis is submitted to the Faculty of Computing at Blekinge Institute of Technology in partial fulfillment of the requirements for the degree of Master of Science in Computer Science. The thesis is equivalent to 20 weeks of full-time studies.

Contact Information:
Author(s):
Qin Jiangcheng
E-mail: jiqi14@student.bth.se

University advisor:
Dr. Lawrence Henesey
DIDD Department of Computer Science and Engineering

Faculty of Computing
Blekinge Institute of Technology
SE - 371 79 Karlskrona, Sweden

Internet : www.bth.se
Phone : +46 455 38 50 00
Fax : +46 455 38 50 57

ABSTRACT

Context. With the development of computer software, hardware, and communication technologies, a new type of human-centered computing model, called Cloud Computing (CC) has been established as a commercial computer network service. However, the openness of CC brings huge security challenge to the identity-based access control system, as it not able to effectively prevent malicious users accessing; information security problems, system stability problems, and also the trust issues between cloud service users (CSUs) and cloud service providers (CSPs) are arising therefrom. User behavior trust (UBT) evaluation is a valid method to solve security dilemmas of identity-based access control system, but current studies of UBT based access control model is still not mature enough, existing the problems like UBT evaluation complexity, trust dynamic update efficiency, evaluation accuracy, etc.

Objective. The aim of the study is to design and develop an improved UBT based CC access control model compare to the current state-of-art. Including an improved UBT evaluation method, able to reflect the user's credibility according to the user's interaction behavior, provides access control model with valid evidence to making access control decision; and a dynamic authorization control and re-allocation strategy, able to timely response to user's malicious behavior during entire interaction process through real-time behavior trust evaluation. Timely updating CSUs trust value and re-allocating authority degree.

Methods. This study presented a systematical literature review (SLR) to identify the working structure of UBT based access control model; summarize the CSUs' behaviors that can be collected as UBT evaluation evidence; identify the attributes of trust that will affect the accuracy of UBT evaluation; and evaluated the current state-of-art of UBT based access control models and their potential advantages, opportunities, and weaknesses. Using the acquired knowledge, design a UBT based access control model, and adopt prototype method to simulate the performance of the model, in order to verify its validation, verify improvements, and limitations.

Results. Through the SLR, two types of UBT based access control model working structures are identified and illustrated, essential elements are summarized, and a dynamic trust and access update module is described; 23 CSU's behavior evidence items are identified and classified into three classes; four important trust attributes, influences and corresponding countermeasures are identified and summarized; and eight current state-of-art of UBT based access control models are identified and evaluated. A Triple Dynamic Window based Access Control model (TDW) was designed and established as a prototype, the simulation result indicates the TDW model is well performed on the trust fraud problem and trust expiration problem.

Conclusions. From the research results that we obtained from this study, we have identified several basic elements of UBT evaluation method, evaluated the current state-of-art UBT based access control models. Towards the weaknesses

of trust fraud prevention and trust expiration problem, this paper designed a TDW based access control model. In comparing to the current state-of-art of UBT models, the TDW model has the following advantages, such as it is effectively preventing trust fraud problem with “slow rise” principle, able to timely response to malicious behavior by constantly aggravate punishment strategy (“rapid decrease” principle), effectively prevent malicious behavior and malicious user, and able to reflect the recent credibility of accessing user by expired trust update strategy and most recent trust calculation; finally, it has simple and customizable data structure, simple trust evaluation method, which has good scalability.

Keywords: User Behavior Trust, Access Control Model, Cloud Computing Security, Triple Dynamic Window

ACKNOWLEDGMENTS

On the completion of my thesis, I should like to express my deepest gratitude to all those whose kindness and advice have made this work possible.

I am greatly indebted to my supervisor Dr. Lawrence Henesey, who gave me valuable instructions and advice during the entire thesis time. His effective advice, shrewd comments have kept the thesis in the right direction; and also his “wicked” humor, made this difficult and tiring journey more vivid and enjoyable.

Secondly, I thank all the professors that gave the lessons to me, their knowledge sharing made me in a higher level in the field of Computer Science.

Thirdly, I would like to express gratitude to my friends, Jian Gao and Yuan Zhou, and the other friends I met in Sweden. Their friendship is my precious fortune in my two years study in Sweden.

And last, I would like to thank my parents, without their constantly encouragement and support, I won’t be able to have the opportunity to study here, and able to finish the master study.

CONTENTS

ABSTRACT I

ACKNOWLEDGMENTS III

CONTENTS IV

LIST OF TABLES VII

LIST OF FIGURES VIII

CHAPTER 1. INTRODUCTION 1

1.1 PROBLEM DEFINITION 2

1.2 RESEARCH QUESTIONS 4

1.3 AIM AND OBJECTIVES 4

1.4 THESIS STRUCTURE 4

1.5 ACRONYMS 5

CHAPTER 2. BACKGROUND 6

2.1 CLOUD COMPUTING AND SECURITY 6

2.1.1 The Definition of Cloud Computing 6
2.1.2 The Features and Architecture of Cloud Computing 7
2.1.3 Cloud Computing Security 8

2.2 ACCESS CONTROL TECHNOLOGY 9

2.2.1 Introduction of Access Control Technology 9
2.2.2 Mandatory Access Control Model 10
2.2.3 Discretionary Access Control Model 10
2.2.4 Role-Based Access Control Model 11
2.2.5 Trust Based Access Control Model 11

2.3 TRUST AND TRUST MECHANISM 12

2.3.1 Basic Concept of Trust 13
2.3.2 Trust Classification 13

CHAPTER 3. RESEARCH METHODOLOGY 15

3.1 SYSTEMATICAL LITERATURE REVIEW 15

3.2 PROTOTYPE 16

CHAPTER 4. SYSTEMATICAL LITERATURE REVIEW 17

4.1 INTRODUCTION 17

4.2 PLANNING SLR 17

4.2.1 The Need of Systematical Literature Review 17
4.2.2 Identify Research Questions 17
4.2.3 Keywords Selection 18
4.2.4 Review Protocol 18

4.2.5 Study Quality Assessment 18
4.2.6 Selection Criteria and Procedures 19

4.3 CONDUCTING SLR 19

4.3.1 Identification of Research 19
4.3.2 Database Selection 20
4.3.3 Study Selection Criteria 20
4.3.4 Study Selection Procedure 21
4.3.5 Data Extraction and Primary Data Synthesis 22

4.4 RESULTS OF SLR 22

4.4.1 Answer of Research Question 1 22
4.4.2 Answer of Research Question 2 26
4.4.3 Answer of Research Question 3 28
4.4.4 Answer of Research Question 4 33

CHAPTER 5. TDW BASED ACCESS CONTROL MODEL 37

5.1 BASIC PRINCIPLE 37

5.1.1 Basic Design Principle 37
5.1.2 Basic Definition and Constraint of Trust 37

5.2 TDW BASED BEHAVIOR TRUST EVALUATION METHOD 38

5.2.1 The Triple Dynamic Windows 38
5.2.2 BTRs Classification 38
5.2.3 Windows Initialization and Workflow 39

5.3 BTRS UPDATE STRATEGY 40

5.3.1 Malicious BTRs Update Strategy 40
5.3.2 Expired BTRs Update Strategy 41

5.4 TRUST EVALUATION PRINCIPLE 42

5.4.1 Comprehensive UBT Evaluation 42
5.4.2 Most Recent UBT Evaluation 42
5.4.3 Actual UBT Evaluation in Trust Establish Window 42
5.4.4 UBT Update Strategy 42

CHAPTER 6. PROTOTYPE & SIMULATION 44

6.1 PROTOTYPE ENVIRONMENT SETTING 44

6.1.1 Prototyping Tool 44
6.1.2 Simulation Environment 44
6.1.3 Prototype Configuration 45

6.2 SIMULATION RESULT AND ANALYSIS 46

6.2.1 Verification 46
6.2.2 Comparison 47
6.2.3 Discover the Unknown 49

CHAPTER 7. DISCUSSION 51

CHAPTER 8. VALIDITY THREATS 53

8.1 INTERNAL VALIDITY 53

8.2 EXTERNAL VALIDITY 53

8.3 CONSTRUCT VALIDITY **53**
CHAPTER 9. CONCLUSION & FUTURE WORK **54**
9.1 CONCLUSION **54**
9.2 FUTURE WORK **55**
CHAPTER 10. REFERENCE **56**
APPENDIX A – SELECTED STUDIES **59**
APPENDIX B – PRIMARY DATA SYNTHESIS **61**
APPENDIX C – SIMULATION RESULT **62**

LIST of TABLES

Table 4-1 Study Quality Assessment Checklist 19
Table 4-2 Selection Criteria 19
Table 4-3 Database Selection 20
Table 4-4 Data Extraction Form 22
Table 4-5 Data Synthesis for *RQ1* (● YES, – No) 23
Table 4-6 Security Evidence Collection 27
Table 4-7 Reliability Evidence Collection 27
Table 4-8 Performance Evidence Collection 27
Table 4-9 Data Synthesis for *RQ3* 28
Table 4-10 Model Performance Evaluation Synthesis Table 35
Table 6-1 External Simulation Environment 44
Table 6-2 Prototype Configuration 46
Table 6-3 Trust Degree Distribution Comparison 47
Table B-1 Primary Data Synthesis Overview 61

LIST of FIGURES

Figure 2-1 CC Environment Simplified Model 6
Figure 2-2 CC Architecture 7
Figure 2-3 Standard RBAC Reference Model [22] 11
Figure 2-4 Trust Role Based Access Control Model [26] 12
Figure 2-5 Trust Classification 14
Figure 4-1 Study Selection Procedure 21
Figure 4-2 Authority Based Access Control Model Working Structure 24
Figure 4-3 Role Based Trust Access Control Model Working Structure 25
Figure 4-4 Dynamic Trust and Access Update Strategy 26
Figure 4-5 Dynamic Trust Ontology Model [38] 29
Figure 4-6 AHP Method Decompose UBT 30
Figure 4-7 Trust Record Time Range 31
Figure 5-1 Triple Dynamic Windows Method 38
Figure 5-2 Initialization of Trust Establish Window 39
Figure 5-3 Most Recent Trust Window 39
Figure 5-4 Squeeze out Expired BTRs 40
Figure 5-5 Malicious BTRs Update Strategy 41
Figure 5-6 Expired BTRs Update Strategy 41
Figure 6-1 Established Prototype and Simulation Environment in NetLogo 45
Figure 6-2 Trust Value of Good users, Bad Users, and Random Users in TDW Model 46
Figure 6-3 (d) Honest Users, (e) Malicious Users, (f) Random Users [S3] 46
Figure 6-4 Trust Evaluation Comparison on Fraud User 48
Figure 6-5 Trust Evaluation Comparison on Intermittent User 49
Figure 6-6 Trust Evaluation Performance on Misoperation User 50
Figure C-1 Fraud User Trust Value Simulation on Study S3 Provided Model 62
Figure C-2 Fraud User Trust Value Simulation on TDW Model 62
Figure C-3 Intermittent User Trust Value Simulation on Study S3 Provided Model 62
Figure C-4 Intermittent User Trust Value Simulation Result on TDW model 63
Figure C-5 Comprehensive User Trust Value Simulation Result on TDW model 63

CHAPTER 1. INTRODUCTION

The Cloud Computing (CC) is an emerging computing technology, it is integrated and developed with parallel computing, distributed computing, network storage, virtualization technologies, embodies the basic idea of the 'network is the computer'. The CC is centralized and connects massive network resource together to form a virtualized computing resource pool (also is known as the 'Cloud'), provides the user with a large scale of cloud services [1].The CC provides the user with three type of service model, Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a service (IaaS) [2]. This flexible service greatly reduces the users' cost and enable individuals and small businesses to use super-powerful computing service, through a variety of ways to obtain universal cloud services follow their own demand. According to the series advantages of CC, recently, the development of CC become a research hotspot in the computer network and information technology domain. The application of CC is very extensive, no matter the size of the companies, firms, such as Google, Amazon, Alibaba, or even small IT Technology Company, take CC into their future development strategy. Research and analysis company Gartner pointed out in their research paper that the CC will replace the current virtualization technology, and become the most important technology trends [3].

The advantages of CC has been recognized by the information technology industry, but the extensive using of CC is facing great challenges. To store confidential information and important business data into the CC platform requires a lot of courage, as the user aware the security risk of the current CC environment. The initial design of CC within a narrow range, the resource access, and resource sharing is under a closed environment, the basic security protections like firewall and traditional access control technology are able to satisfy the security requirement. But, with the development and expansion of CC, the cloud resources are more and more exposure on the Internet, the number and the scale of attacks are exponential increasing [1]. The security requirement was upgraded from traditional closed security access control into a dynamic, open security access control. Security problems of CC in data security and user privacy protection directly related to the further development of CC.

To truly implement a safe and reliable CC environment, we need to improve its *stability*, *integrity*, and *credibility*. Especially credibility is known as the trust between cloud service providers (CSPs) and cloud service users (CSUs), which is a critical factor in the expansion of CC [4]. The CC trust issues involve two aspects:

For CSUs, as lack of control of the remote data and equipment, lead to distrust of CSPs. Unwilling to store important confidential data, business information, and daily processing environmental into the cloud platform, the risks like data disclosure, data being investigated by unauthorized parties, data loss, cloud server collapse, etc. will seriously damage the information security and data

integrity, causing inestimable economic loss [5]. If there is no user trust CSPs, the business of CSPs will not able to expand much, like a bank without a customer to open an account and deposit money. Therefore, it is necessary to make CSUs trust CSPs, and it is currently a very important research content in cloud security.

On the other hand, for CSPs, the trust to authorize a user access, assign service degree to a user. The CC can be accessed by every single Internet-linked device, and provides authorized user with high degree of freedom inside of CC platform, CSUs can directly use and operate the CC software, operating system, infrastructure like virtual machine, server, and even able to deploy their own program and execute on cloud [6]; therefore, it is very vulnerable to attacks, the attacker could be a malicious user, hackers, and even identified user may be hijacked, misoperation, or a potential competitor [7]. The impact of an attack can cause huge disaster, for instance, a malicious user deployed a malicious program on the cloud server by using the PaaS, user's malicious program may take control the virtual machine configuration, occupy the hardware like CPU, memory, network stream, and may also attack the other users' client machine. Therefore, timely detect and prevent the malicious and risk user accessing is an important research content, and it is the objective of this research study.

1.1 Problem Definition

Currently, CSPs are mainly using IAM (Identity and Access Management) technology as access control to manage user authorization [8], but the IAM has three major disadvantages:

First of all, the IAM does not consider the multi-domain characteristics of CC, cannot well settle the cross-domain access control and authorization issues;

Secondly, the IAM only verifies user's identity trust, test username, password, and IP address to identify user's identity, without verifies the user's behavior trust according to its historical interaction evidence [8], it cannot detect and prevent potential malicious user; for instance, today's digital library using CC to build large-scale book and thesis data resource warehouse, the visitor can read the resource online, and the authorized user like the school students or paid account can access the resource and legally download the resource. We can use identity authorization to identify user's identity, and provide with proper authority; but we the IAM cannot detect and prevent malicious users, which might use tools or set proxy to download large quantities digital resource to obtain illegal profit. In this case, the user's identity is legal but his behavior is malicious and not trusted.

And the last, the IAM assigns authority to the user before the beginning of interaction without monitoring user's actual behavior during the entire interaction, malicious action, misoperation and risk behavior cannot be effectively detected and prevented.

With these three disadvantages, the IAM cannot effectively solve the CC security issues, especially the CSP's trust problem we mentioned above.

Therefore, expand and update the traditional access control technology is urgent to solve the trust issues and improve the security problem of CC.

The concept of 'Trust' was first introduced into computer science in 1996 by Blaze M [9], the basic idea is admitting the imperfection of security information in an open system, the system's security decision requires to depends on a reliable third party to provide additional security information. The theory of trust management mechanism provides a new solution to solve CC security problems.

The UBT is a branch of trust management theory, is the comprehensive evaluation of user's interaction behavior, by using quantized evaluation result to represent the user's friendly degree to the system, and identify risk users and malicious user [10]. Provide access control system with a valid basis for decision making, improves the reliability of authority allocation.

The purpose of UBT evaluation mechanism is similar to the bank credit systems. For example, they assign a bank client with different grades of credit based according to the client's salary, job stability, social record (whether have criminal records), and the behaviors, such as whether they pay loans on time, and maintain a reliable deposit amount. High credit clients are able to borrow more loans from banks, receive improved financial services, and are considered as valuable clients by the bank. Correspondingly, the bank will refuse to provide loans to low credit clients, or issue a few loans, and also will keep an eye on these clients.

In recent years, scholars utilize the UBT evaluation method and access control technology, expected to solve the CC security problem. Tian Liqian et al [11], established three-level user behavior evaluation principle, proposed a Bayesian network based user behavior trust prediction and game control theory, but the evaluation system cannot solve the problem of uncertainty and fuzzy of trust measurement. Chen Yarui et al [12], proposed a dynamic game control based user behavior trust model, through a multi-stage game control of incomplete information principle to analyze the type of cloud end-user, examine potential untrusted cloud end-users in the system, but the main study is real-time analysis of user behavior, failure to establish specific cloud security access control mechanism. Lv Yanxia proposed an FANP (Fuzzy Analysis Network Process) based user behavior trust evaluation method in cloud computing environment [13]. However, the evaluation process of the method is complex, the computation is difficult, and the evaluation efficiency is low.

The UBT based access control technology is the technology trends to address the CSUs trust issues, but there remain problems and weaknesses; identify those potential weaknesses and design a solution to improve the performance of UBT based access control model is the research problem of this research project.

1.2 Research Questions

In this research project, the following questions are attempted to be answered:

Part1. Identify Essential Elements

RQ1: *What is the working structure (essential elements) of UBT based CC access control model?*

RQ2: *What kinds of cloud user behavior can be collected as evidence for trust evaluation?*

Part2. Identify Potential Weaknesses

RQ3: *What attributes of trust can affect the performance of UBT based access control model?*

RQ4: *What is the currently state-of-art of UBT based CC access control model?*

Part3. Verify the Improvements

RQ5: *How can a prototype be built to evaluate user behavior trust?*

RQ6: *How to verify and validate the improvements?*

1.3 Aim and Objectives

The main aim of this research is to gain a better understanding of UBT based access control technology in CC and to improve any weaknesses. To achieve this main aim, two sub-objectives are defined:

- Understand the basic elements of UBT evaluation based access control technology in CC, summarized the state-of-art and identify the potential weaknesses that able to be improved.
- Design a solution to overcome the identified the weaknesses, model the design and conduct a simulation to verify the improvements.

To clear define the research range, we list excluded research area below:

- This research does not consider user's identity authorization as it's already a mature technology, the improved cloud access control model will focus on the UBT of CSUs that already passed identity authorization.
- This research does not consider cross-domain authorization problem, the method to handle cross-domain authorization is in another research domain.

1.4 Thesis Structure

We summarized the background and relative knowledge of CC security, access control technology, and trust mechanism in Chapter 2. An introduction of adopted research methodologies explained in Chapter 3. And we present the detailed work process of systematical literature review and the result in Chapter 4. Chapter 5 present the design of TDW based Access Control model. And the

chapter 6 present the work process of prototype establishment, and simulation result. In Chapter 7, we discussed and explained the findings in this research study. Then we discuss the validity threats in Chapter 8. Finally, we present the conclusion and the future work of the research in Chapter 9.

1.5 Acronyms

CC	Cloud Computing
CSP	Cloud Service Provider
CSU	Cloud Service User
UBT	User Behavior Trust
BTR	Behavior Trust Record
SLR	Systematical Literature Review

CHAPTER 2. BACKGROUND

This chapter introduced the basic definition of CC, and CC security issues; summarized the current research status of access control technologies; and the trust management theory as the foundation for later research. To deeply understand the design of CC environment oriented access control model and its security problems.

2.1 Cloud Computing and Security

This section introduced the basic definition of CC, explained basic features of CC, illustrated its architecture, and the current security problems of CC.

2.1.1 The Definition of Cloud Computing

The major purpose of CC is to realize the computer resource's publicity for commercialization. CC provides various users with fast and convenient data storage, network computing, and other specific services. A simplified CC environment is illustrated as figure 2-1. However, CC is unlike simple network calculation. In network computing, the user only accesses to a specified server through the network, but the CC is composed by a group of numerous interconnected computers.

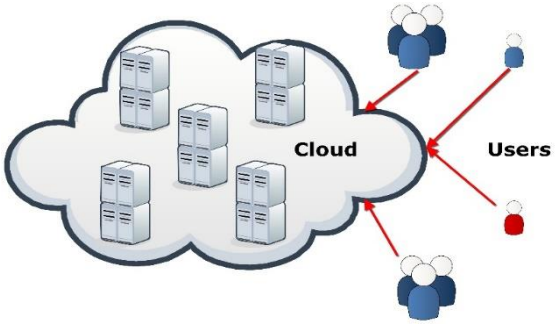


Figure 2-1 CC Environment Simplified Model

We summarized some scholars' research work on CC, obtained the following two CC definitions:

- The W. Li et al [14] considered that CC is a kind of computing, providing dynamically extendible virtualization resource service through the Internet, and providing universal services. This definition emphasizes that CC uses virtualization and other technologies to provide computing resources as a service to a demanded user.
- The X. Sun et al [15] considered the CC is an expanded computing model based on parallel computing, distributed computing, and grid computing; and also the commercial realization of the above computing models, promoted the concepts like virtualization, utility computing, IaaS, SaaS,

and PaaS, etc.

2.1.2 The Features and Architecture of Cloud Computing

Based upon the NIST description, CC has three different type of service models [16]:

- **Software as a Service (SaaS):** the software service provided through Internet, users do not need to purchase software and install it on the local computer, but leased the Web-based software from the service provider to manage business activities.
- **Platform as a Service (PaaS):** Delivered to the user with rich "the cloud" resources, development environment as a kind of service provided to the user, application run-time environment, sharing service, and the automation management service, etc. users can develop their applications in the development environment.
- **Infrastructure as a Service (IaaS):** The cloud provider infrastructure such as server, network and storage devices as a service provide to users. Users can directly development their own platform and application on the cloud infrastructure (the service layer) instead of purchasing additional hardware, system software maintenance, and relevant system software.

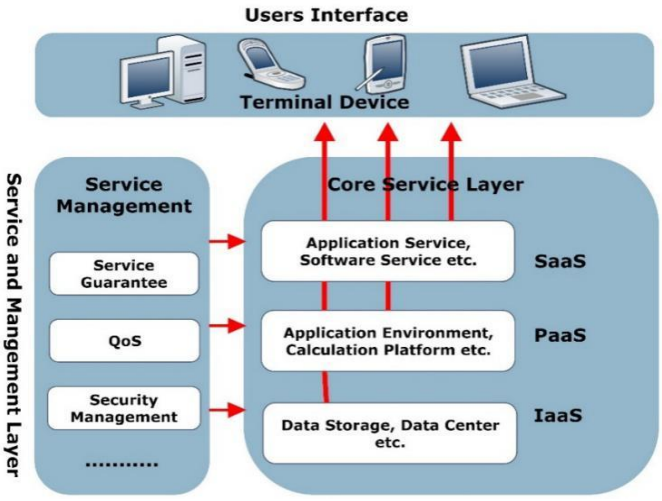


Figure 2-2 CC Architecture

The CC architecture is illustrated as figure 2-2. Users interface layer provides CC user with available access interface; Service management layer manage the service relationship between CSUs and CSPs, control the service quality and service security problem; Core service layer is the collection of available CC services and applications.

CC environment has many different characteristics compare with other traditional computing models, including the following aspects:

- Limitless resource: in the cloud environment, the resources are almost

infinite, which depends on resource virtualization technology, also requires the background resource pool must have a considerable size.

- Virtualization and packaging: in the CC environment, resources are virtualized and encapsulated into services, which provides users with the convenience of use, and is conducive to the protection of resources and user privacy.
- Customized service: CC service system can provide customized service type and service level according to the needs of users.
- Open service access and management interface: CC provides a standardized interface, facilitate the developers to development and construction of new services by SOA (Service-Oriented Architecture) or Web interface.
- Pay-as-demand: user can pay by their own demand, and chose different service combination.

2.1.3 Cloud Computing Security

The CC is a business computing model which service is its purpose. CC represents the information technology domain is now developing forward to intensive, large-scale and specialization direction. But extensive use of CC still facing challenges, the security issues is one of the biggest blocks for CC daily use.

The CC security problem has been widely concerned by both academic circle and IT industry. According to the statistics from IDC[1], the rating of the challenges or issues of the CC development, the security problem is top concerned with 87.5% among the other challenges.

Fox et al summarized the top ten CC security challenges at the Berkeley CC white papers [17], the data security, service availability, performance unpredictability, large-scale distributed system security vulnerabilities, and reputation crisis, are related to the confidentiality and reliability of CC. Based according to cloud computing services and cloud data center security problems, many companies and users still concern about whether to adopt CC.

The research study of CC security is still immature but is gradually developing. K Ren et al [18] consider the study of CC security can be divided into three aspects:

1. The problem of CC system and network security issues.
2. The problem of CC in data privacy protection.
3. The problem of trust issues among entities in CC environment.

The first two aspects are the premise of CC popularization, involve the realization of CC core techniques. The third aspect, as known as the credibility of

[1] IDC: International Data Corporation, a market research, statistics analysis, and advisor company, specialized in information technology, software development area.

CSPs and CSUs, which refers to two aspects:

- **The credibility of CSPs:** CSUs whether to trust the use of cloud services published by CSPs.
- **The credibility of CSUs:** CSPs, whether to trust the accessing users, will comply with the service requirements, and properly behave during the interaction.

At present, to solve the security problem of CC is to establish a feasible cloud security framework for specific security risks, and use this framework to study the key security technology. Access control policy based on trust mechanism provides a possible solution to solve the trust issues of CC.

2.2 Access Control Technology

This section introduced the basic concept of access control technology, four different types of access control technologies, including mandatory access control model, discretionary access control model, role-based access control model, and trust-based access control model are summarized and described in sub-sections.

2.2.1 Introduction of Access Control Technology

Access control is considered to be one of the most important elements in the field of information security. The so-called access control, which is to determine whether a user has permission to access, use or modify a resource. Access control systems generally include *object*, *subject,* and *access control strategy*. Basic description as follows [19]:

- **Object:** the object is a passive entity that can be accessed by other entities. Information, files, and resources, any objects that can be manipulated can be considered an object.
- **Subject:** the subject is the active entity that can exert their action to other entities, sometimes referred to users or visitors. A Subject can be the user's organizations or users itself, can also be any user's accessing terminal, or even application service program or process.
- **Access Control Policy:** Access control policy is an action-constrained set of subject to the object. Simply speaking, access control policy is set of subject to object access rules, the rule set defined the subject's action constraints to the object and object conditions constraints to the subject. Access control strategy represents the behavior of authorization, also is a permission from object to the subject, this permission is not able to go beyond the rules set.

Currently, the research of access control technology is already very mature, in the course of nearly four decades of development, has emerged many important access control technologies: *Discretionary Access Control* (DAC), *Mandatory Access Control* (MAC), *Role-Based Access Control* (RBAC), *Task Based*

Access Control (TBAC), and *Attribute-Based Access Control* (ABAC), etc. The traditional access control technologies include DAC and MAC.

2.2.2 Mandatory Access Control Model

The MAC is based according to the security attributes of subject and object to decide whether to grant access. The basic idea of MAC is: each subject and object have a label to represent their security attributes. The security attributes of the subject reflect the authority level that can be obtained by subject; the security attributes of the object represents the object sensitivity [20]. MAC determine whether users can obtain access authority by comparing the security attributes of subject and object.

The advantage of MAC is, in the authorization process, not only need to check whether the subject having the operation authority to the object, but also need to check if the security attributes of the object and subject meet the requirements, which makes the authorization process much more secure. Thus, the MAC is suitable for high security required system, for instance, the military authorization system.

The disadvantages of MAC is, the authorization management system must assign security attributes for each subject and object, and need to carefully define the correspondence security attributes between subjects and objects, thereby preventing legitimate subject cannot operate on authorized objects, and illegal subject able to operate on unauthorized object phenomenon. Therefore, MAC authorization management is difficult and complex.

2.2.3 Discretionary Access Control Model

The working principle of DAC is to confirm the identity of the subject, authorize the subject based on the corresponding relationship between its identity and authority. The basic idea of DAC is the owner of the subject determine the authority of other accessing subjects, the subject that obtained the accessing authorization can further grant the privileges to other subjects [21]. In this way, the authorization of DAC become a chain structure, for instance, there exist an authorization relation among subjects A, B, C, and D: A→B→C→D, which means the subject A grant an access authority of object O to the subject B, and subject B grant the authority to the subject C, and finally subject C grant the authority to the subject D. In this case, subjects A, B, C, and D all have the same access authority to the object O. In this authorization chain structure, every subject can only manage the authority of their successor node, but not able to manage the second level subject's authority.

The advantage of DAC is subject to the authorization process with great flexibility, but the drawback is authorization process exist chain structure, the authority management only valid on those directly granted subject, it cannot control the subject indirectly obtained access authority, which leads to low-security performance. Also, in terms of authority management, the system needs to maintain the relationship between different subjects with different access

rights to different objects, authority management complexity is high.

2.2.4 Role-Based Access Control Model

Most traditional access control mechanism grant authority directly to the subject, which leads to high complexity of authority management. To solve this problem, R. Sandhu et al [22] introduced "role" concept into the access control technology, developed RBAC. In RBAC, the system defines a series of roles, first assign access permissions to these roles, and then assign the appropriate roles to the subject, so the subject has the access authority as same as the role. Compared with the authority granted directly to the subject, grant role to users is much more flexible, but also simplifies the management of the system.

Standard RBAC reference model as shown in figure 2-3. The model defined basic functions of role, the model includes five basic factors: Users, Roles, Sessions, Objects, Operations, and Permission Role Assignment (PRA), User Role Assignment (URA), Role Assignment Constraint (RAC). The basic idea of RBAC is to establish many to many relationships between users and access authority by role.

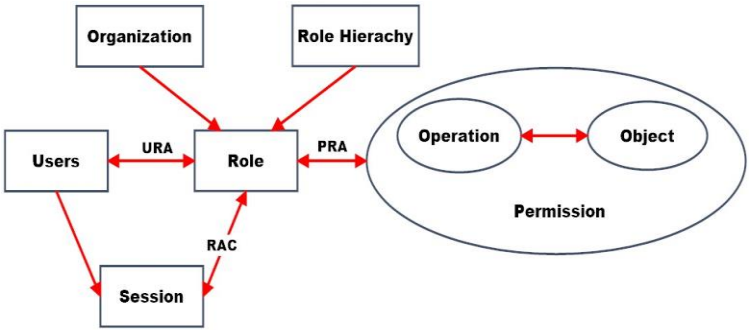


Figure 2-3 Standard RBAC Reference Model [22]

The advantage of RBAC is avoiding the direct mapping of users and authority in DAC and MAC, to build a hierarchical indirectly mapping relation. RBAC effectively reduce the authority management complexity, and with high flexibility. The drawback of RBAC is it only verify user's identity before grant role to the user, without considering user's behavior trust. And RBAC adopt the pre-assign strategy to assign access permission, it doesn't monitoring and control user's behavior during the interaction, malicious operation and user cannot be discovered timely.

2.2.5 Trust Based Access Control Model

Access Control Model not only the system security solution, but also the key technology to ensure system confidentiality, integrity, and availability. Therefore, the research of access control technology become research hot-spots in computer security domain. However, the traditional access control model is based on large-scale resource host access control, not able to apply in CC environment, and overcome the current security challenge in CC.

Aim at the feature of CC, J. Chen et al [23] analysis the CC dynamic

requirements to the access control, expanded RBAC model and make it suitable for the CC complex access control and management requirements. However, RBAC only fits in closed and centralized network environment, not able to apply in large-scale, open distributed network, in particular, cannot meet the security requirements of the multi-domain environment in CC.

To overcome the drawbacks of RBAC model, some researchers introduced trust management mechanism into the access control model.

Tang et al [24] expanded on the shortage of RBAC model, based on "trust management" concept proposed by Blaze, introduced trust concept into the access control mechanism, proposed the TRBAC (Trust Role Based Access Control Model), a trust-based access control model. The model identified specific requirements for user's authority, comprehensively calculate user's multiple trust feature, and achieved fine-grained, flexible authorization mechanism, which is more safe and reasonable for assigning users required authority. The model illustrated as in figure 2-4.

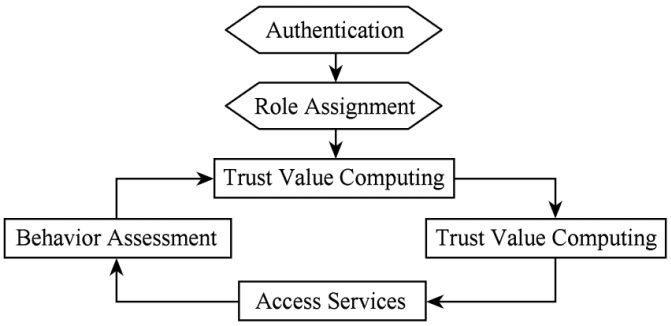


Figure 2-4 Trust Role Based Access Control Model [26]

Tan et al [25] and Wenhui et al [26] improved the weaknesses of TRBAC model, proposed trust based dynamic RBAC model in CC environment. Thesis [25] provided detailed user trust degree calculation procedure, assign users with different access authorities according to user's role information and trust degree, which will reduce the security threat in the CC environment. Thesis [26] is theoretical analysis, it doesn't provide trust degree calculation method.

2.3 Trust and Trust Mechanism

The concept of Trust is first proposed by German sociologist Georg Simmel, Simmel argued in his monograph 'The Philosophy of Money', it mentioned that the social behavior is formed according to the interaction between peoples, and the interaction is based on the trust among peoples. Thus, from the original concept, the trust is a sociology theory, but as peoples' connection can easily refer to the interaction between machines, computers, and internet entities, the concept of trust was lead into computer science domain. In 1972, J.P.Anderson [27] proposed the trust concept in computer domain. In 1994, Marsh [28] firstly start to analysis trust model to overcome the trust issues in the agent system, describe the formalization problem. In 1996, to handle the Internet security

problem, M. Blaze et al [29] firstly used the Trust Management concept, bring the trust model study into the distributed system area in order to solve its security problems. At the same time, A. Abdul-Rahman et al [30] proposed the trust metric mathematical model with the same purpose.

2.3.1 Basic Concept of Trust

As a concept of social engineering, trust was introduced into the field of computer security due to the network security consideration. CC rely on the network to achieve a certain kind of business service, the network is the epitome of human society, and trust relationship between the network entities is similar to the real society. Due to the openness and dynamism of the CC environment, the trust relationship among CC entities become much more complex and difficult to be defined than a traditional network. Recently, many scholars proposed the trust definition in computer science domain, but they are not unified.

- G. Xiaolin et al [31] consider the trust as a subjective probability prediction from subject to the object whether can accurately and non-destructively completed collaborative activities; and the trust is a subjective concept that related to honesty, competitive and reliability. This idea comes from the social psychological level analysis of trust, emphasize the subjectivity of trust, with strong uncertainty.
- X. Sun et al [32] consider the trust as a rational trust from subject to the object, an entity could only be credible, or not credible. Thesis designed a model to accurate describe and analysis trust relationship. This concept emphasized on trust rational factors, used a mathematical method to express the trust relationship, well performed on trust information expression, provides corresponding trust values for the upper application development, but not able to completely describe the trust relationship between entities.
- X. Wang et al [33] consider that trust is the subjective probability of an entity to execute a specific activity, the activity is not able to be monitored in advance. The developed trust model generally considers subjective factors of trust, trust feedback, and the corresponding trust updating factor, the model can effectively express the true relationship between entities. This theory combined the above two trust concepts, considers the subjective and rational aspects of trust, and provides good expression of trust, so this paper adopts this trust concept.

2.3.2 Trust Classification

Trust can be classified into identity-based trust and behavior-based trust from the access control perspective; meanwhile, behavior trust can be classified into behavior process based trust and behavior result based trust [34]. The classification illustrated as figure 2-5.

Lots of access control models adopt identity-based trust as trust value, the advantages of this type of trust are easy to calculate, store and operate [35]. But

the identity trust is not appropriate to be applied in open systems, as the user's identity is easy to be stolen or forged, becomes an access security vulnerability.

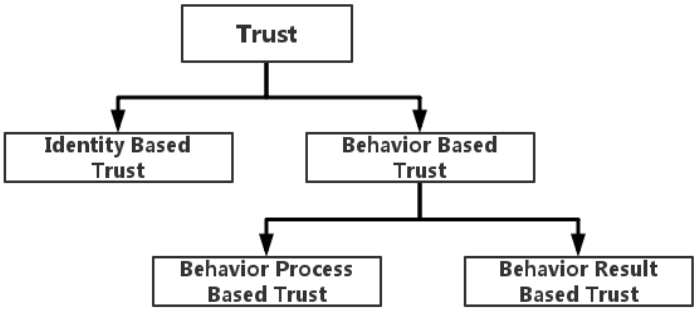


Figure 2-5 Trust Classification

The behavior trust based access control mechanism can avoid the above security vulnerability to a certain extent. It can timely detect and control the malicious user through real-time user behavior monitoring and analysis; even the user with correct identity, but admitted to a malicious behavior, the system will reduce their authority degree or denial their accessing.

Behavior process based trust evaluation depends on the type of entity's behavior (what kind of behavior), the evaluation system will assign different trust value to the entity according to entity's different behavior.

Behavior result based trust evaluation depends on the output of the entity's behavior (what kind of result), the evaluation system will assign different trust value to the entity according to the different system environmental changes.

CHAPTER 3. RESEARCH METHODOLOGY

Research methodology provides tools and means to discover a new phenomenon, new things, or put forward new theories, to reveal the inherent law of things during the research study. Help researchers to strengthen problem understanding, gain valid knowledge, obtain theory evidence and answer research problems.

"*A research project either has a pre-defined object and has to select valid methods to achieve it or has fixed methods and need to find the optimal result. Sometimes, during the research procedure, both the research aim and research methods have to be modified*". *- Dr. Lawrence Henesey*

In this research study, the objectives are to identify the weak spots of current trust-based access control technology and improve it to obtain a better performance and overcome the current CC security problem, which needs to select available and effective means (research methodologies) to achieve it.

According to Creswell [36], using diverse methodology approaches to collecting data for answering research question can provide better research result. The research strategy that adopted in the research study combines the systematical literature review (SLR) and prototyping method, which are both answers the research questions qualitatively and quantitatively.

3.1 Systematical Literature Review

The systematic literature review is a means to collect and survey available relevant research papers that focus on a similar research problem, research domain, or research phenomenon [37]. The purpose of SLR is to conduct an impartial assessment of a research topic by rigorous academic attitude, trustworthy survey methods, and auditable research procedure. The SLR should have a pre-defined research strategy, and the research strategy should be strictly executed during the study period. Both supportive and unsupported research evidence should be discovered and reported.

The SLR is suitable to summarize the advantages and disadvantages of a specific method or technology. The result of systematic literature review can help the researcher to discover the existing gaps of current research status, and valid research basement to support new research activities.

In this paper, we adopt the SLR guidelines by Kitchenham [37], executed the SLR in following three steps:

1. **Planning:** Identify the need for the SLR, develop and evaluate the review protocol.
2. **Conducting:** Research paper selection, study quality assessment, data extraction, and data synthesis.

3. **Reporting:** Report and document the study result.

3.2 Prototype

A prototype is an early software sample, function sample, or experimental demo of a new algorithm, a new model in computer science domain [38]; the purpose of building a prototype is to test whether the software function, model or algorithm has achieved the design goal.

The aim of building a prototype in this paper is to verify the validation of our model design, compare the performance of the current state-of-art model, and quantitatively observe the contribution and limitation; answer the ***RQ5*** and ***RQ6***.

This paper executed the prototype methodology in following three steps:

1. **Verification:** verify the validation of designed model by testing it with same prototyping method, environment setting, and data input as selected state-of-art model; Check if the model achieved the basic requirements.
2. **Comparison:** compare the performance of the current state-of-art model; check if the performance is better or worse in different cases, and verify the design object.
3. **Discover the unknown situation:** test the model with hypothetic scenarios; check if the model could handle the situation or not, acquire effective improvement advice as the limitation and future work.

CHAPTER 4. SYSTEMATICAL LITERATURE REVIEW

In this chapter, we present the work process and the results of SLR. The aim of adoption SLR is to identify the main elements of UBT based access control model in CC, summarized the current state-of-art, and identify potential weaknesses, in order to support the later solution design.

4.1 Introduction

According to the guidelines proposed by Kitchenham [37], we made some revisions and conducted this systematical literature review through following steps which are repeatable.

1. Identification of need for a systematical literature review;
2. Identification of search strategy;
3. Selection of primary studies;
4. Study quality assessment;
5. Data extraction and monitoring;
6. Data synthesis;
7. Report result.

4.2 Planning SLR

The planning procedures of SLR are presented in the following sub-sections. Including the need of SLR, the research questions that are attempted to be answered, the keywords selection, review protocols, study assessment protocol, study quality assessment, and study selection criteria.

4.2.1 The Need of Systematical Literature Review

Prior study is used here to identify the need of the systematical literature review, we selected following databases: *ACM*, *IEEE*, *ISI Web of Science*, *Springer link*, *Inspect*, *Scopus*, and search with following search string:

(Cloud Computing) AND ((Access Control) OR (Access Control Model) OR (Authorization)) AND ((Trust Evaluation) OR (Behavior Evaluation)) AND ((SLR) OR (Systematical Literature Review) OR (Literature Review))

The result indicates that there are no related result and relevant work retrieved. Therefore, we can conclude that there is a need for the systematical literature review of this research project.

4.2.2 Identify Research Questions

During the SLR, the following four research questions are attempted to be answered:

RQ1: *What is the working structure of UBT based CC access control model?*

RQ2: *What kinds of cloud user behavior can be collected as evidence for trust evaluation?*

RQ3: *What are the attributes of trust that can affect the performance of UBT based access control model?*

RQ4: *What is the currently state-of-art UBT based CC access control model?*

4.2.3 Keywords Selection

We followed the suggestion from Petticrew and Roberts, used the PICOC (Population, Intervention, Comparison, Outcome, and Context) criteria [39] to select research keywords.

- **Population:** in this research context, the population refers to an application area, we chose "Cloud Computing" as the population in this research project.
- **Intervention:** in this research paper, "access control model" is considered as a technology that addresses the CC security issue. So we chose "access control model" as the intervention.
- **Comparison:** in this research paper, the key methodology within access control model that being compared is "UBT evaluation method". So we select "UBT evaluation method" as the comparison.
- **Outcomes:** in this research paper, we want to assign good behavior CSUs with high authority, and bad behavior user with low authority to access the cloud service. So the outcomes we concerned is the authority assign accuracy. So we select "evaluation accuracy" as outcomes.
- **Context:** the comparison is under the academic environment, so the context of this research is "academia".

4.2.4 Review Protocol

The aim of having review protocol is to ensure the comprehensiveness of the systematical literature review, by pre-defined review protocol to reduce the subjective bias [37], the collected and primarily reviewed papers should fully relevant with research objectives, and qualified to support the research answer. According to the Kitchenham's guideline, we defined the study quality assessment, the selection criteria, and selection procedure in the following sections.

4.2.5 Study Quality Assessment

The study quality assessment checklist is shown in table 4-1. To ensure the quality of the paper we selected after inclusion and exclusion study procedure, we defined the following checklist to evaluate each selected papers.

Table 4-1 Study Quality Assessment Checklist

No.	Quality Assessment Criteria	Value
1	Does the study answered the research questions?	Yes/No/Partly
2	Does the research method are scientifically described?	Yes/No
3	Does the research validity threats are discussed?	Yes/No
4	Do the contributions and limitations are discussed?	Yes/No
5	Does the method defects are discussed?	Yes/No
6	How many times the paper has been cited?	Number

4.2.6 Selection Criteria and Procedures

In addition, to ensure the relevance of the papers that we selected during the primary study, we here list the selection criteria and procedure in advance. The aim of this procedure is to filter the papers that not able to cover the research objectives or not qualified to be surveyed. The selection criteria as shown in table 4-2.

Table 4-2 Selection Criteria

Item	Criteria
Search Constrain	• Journal, Conference paper, and Article • Publication year between (2010-2016) • Computer science domain • Language in English
Abstract/ Introduction	• Research gap is related to CC security • Mentioned UBT or similar keywords • Experiment or empirical study is mentioned as research methodology
Full Text	• Was well written, in good thesis structure. • Tables and figures are clearly stated and described with text • Experiment procedure and result are clearly described and supported by rational evidence. • Limitation discussed • The Contribution is produced by rational comparison.
Reference	• Well documented reference list

4.3 Conducting SLR

In this section, we presented the procedure of SLR conducting. Including the research identification, database selection, study selection procedure, and study extraction and primary data synthesis.

4.3.1 Identification of Research

The aim of having this systematical literature review is to comprehensively

research and review as many primary studies that related to the research questions as possible [37]. To satisfy above requirement, we developed a severe research strategy which will be described in the following sections.

According to the research keywords we have identified in section 4.2.3, we defined the following research keyword string:

(Cloud Computing) AND (Trust* OR Reputation* OR Credibility) AND (Access Control)

4.3.2 Database Selection

Six computer science literature database were selected for this study project, the selected databases are shown in table 4-3. The selection of those databases is based on the recommendation in Kitchenham's guideline, each of those databases is cover the computer science domain, and famous for the quality of the articles.

Table 4-3 Database Selection

No.	Database
1	*Scopus*
2	*ACM Digital Library*
3	*IEEE Xplore Digital Library*
4	*Springer Link*
5	*Inspect (Engineering Village)*
6	*ScienceDirect*

4.3.3 Study Selection Criteria

The inclusion and exclusion criteria are applied to the papers that collected after primary studies, review the full text of the paper and identify if the paper is relevant to the research topic and research questions.

- Inclusion Criteria
  1. The article described and illustrated a UBT evaluation method.
  2. The article aims to overcome the CC security problems or the distributed open access network security problems.
  3. The article provides the structure and working procedure of the behavior trust identification.
  4. The article discussed the trust attribution that affects the trust evaluation.
  5. The article discussed and provide the user behavior evidence for the trust evaluation.
- Exclusion Criteria
  1. The trust evaluation method in the article does not evaluate CSU's trust.

2. The article doesn't provide either theoretical evidence or experiment evidence to support the validation of the trust evaluation method.
3. The article is part of a book.
4. The article is not written in English

4.3.4 Study Selection Procedure

The study selection procedure and result are as illustrated in figure 4-1.

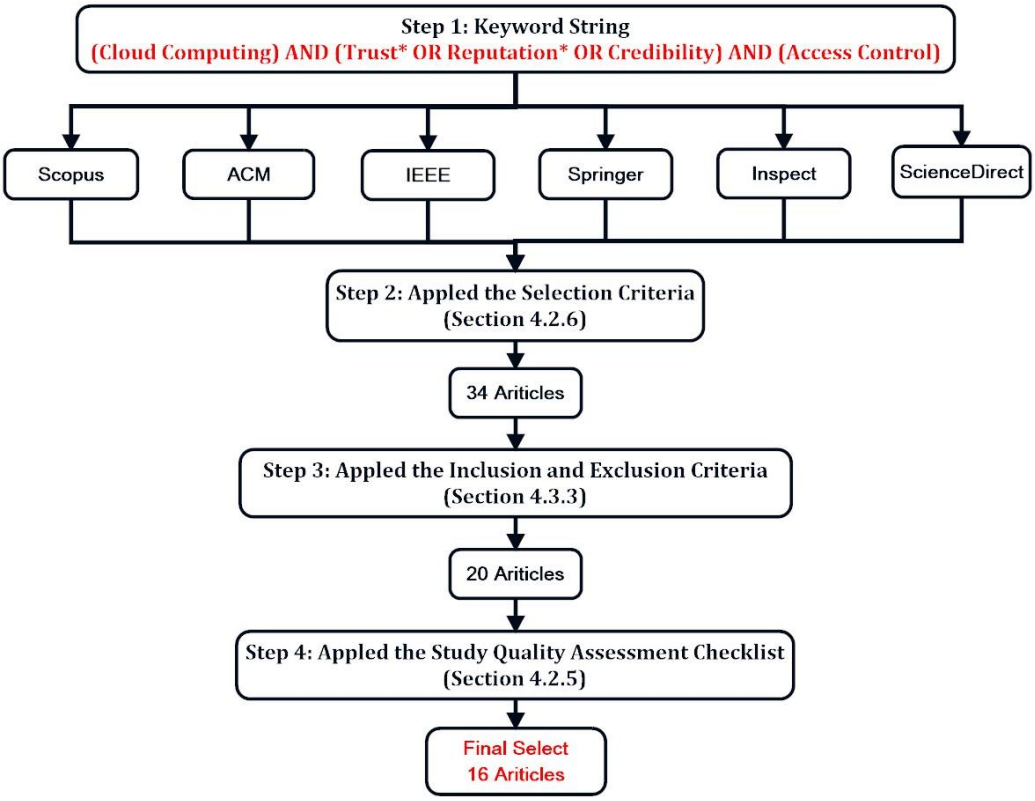


Figure 4-1 Study Selection Procedure

Step 1: we applied the research keyword string in each database, get an initial set of papers.

Step 2: following the selection criteria we defined in section 4.2.6, we first applied the research constraint, set the articles' publish year range between 2010 and 2016, select journal, conference paper and article as content type, set the article language with English, and research domain within computer science. Then, review the paper's abstract and introduction, identify if the paper is meet the criteria, and review the full text and reference section roughly if the paper's abstract is meet the criteria. After this step, 34 articles are selected.

Step 3: 34 articles are carefully full text reviewed with inclusion and exclusion criteria we defined in section 4.3.3. After this step, 20 articles are selected.

Step 4: 20 articles are reviewed with study quality assessment checklist we defined in section 4.2.5, four articles are excluded in this step as they are not able to provide any topic relevant knowledge and information.

Finally, we obtained 16 articles that meet all the requirements.

4.3.5 Data Extraction and Primary Data Synthesis

The selected studies are presented in Appendix A. and here we present the data extraction procedure and primary data synthesis result. Each selected study was reviewed with data extraction form as illustrated in table 4-4.

Table 4-4 Data Extraction Form

Data Item	Value
Selected reference ID	S. ID
Source Database (SD)	Database
The Published Year (PY)	Year
Provide Trust Evidence? (TE)	Yes/No
Discuss Trust Attributes? (TA)	Yes/No
Illustrate Working Structure? (WS)	Yes/No
Provide Trust Evaluation Methods? (EM)	Yes/No
What's the name of the EM? (MN)	Name
Experiment Environment (EE)	Real Cloud (RC)/ Simulated (SL)

The primary data synthesis is illustrated as table B-1 (Appendix B). 10 articles come from IEEE, three articles come from ScienceDirect, two from Springer, and one from ACM.

Eight articles designed and illustrate the working structure and procedure of UBT based access control model, the data of these articles are able to answer the ***RQ1***. Eight articles discussed the collection of trust evidence and provide the collection item, which available to answer the ***RQ2***. Seven articles discussed the trust attributes and their affections on the trust evaluation, the data of these articles are able to answer the ***RQ3***. And eight articles illustrated the UBT evaluation based access control model, aim to answer the ***RQ4***.

Among these articles, only one study obtained the simulation data from real CC environment, while nine studies conducted the experiments or prototypes in simulated CC environment.

4.4 Results of SLR

We present the SLR results in the following sub-sections, each sub-section is attempted to answer one research questions.

4.4.1 Answer of Research Question 1

RQ1: *What is the working structure of UBT evaluation based access control model?*

The data synthesis for the ***RQ1*** is shown in table 4-5. Eight articles that

selected by primary data synthesis are reviewed in this section. We identified and classified two type of access control model working structures in these papers, one is the authority based access control model, and another is the role-based access control model. We also identified whether the paper considered dynamic trust updating during the user interaction.

Table 4-5 Data Synthesis for *RQ1* (● YES, - No)

S.ID	Authority Based	Role Based	Dynamic Update
S1	-	●	●
S4	●	-	-
S5	●	-	●
S6	-	●	●
S7	●	-	-
S9	-	●	-
S11	●	-	●
S13	-	●	-
Total	**4**	4	**4**

■ **Authority Based Trust Access Control Working Structure**

The selected studies **S4**, **S5**, **S7**, and **S11** are using authority based trust access control working structure. The authority based access control model illustrate as shown in figure 4-2. The model composed of four modules.

1. **Authorization Module:** grant CSU with corresponding operation authority and service degree according to the user's trust value.
2. **Behavior Monitoring Module:** real-time monitoring user's behavior during the entire interaction process. Collect the required behavior evidence and go through data pre-processing, standardized the collected evidence, and store the data in user's behavior evidence database.
3. **Trust Evaluation Module:** apply the trust evaluation methods on user's behavior evidence that stored in evidence database, get the user's behavior trust value, and store the trust value in the user's trust database.
4. **Trust Dynamic Management Module:** acquire the user's trust value when a user request access and have passed identity verification. Real-time verifying user's trust value updating, dynamic change the user's service degree and operation authority accordingly.

The working procedure of authority based model is marked with the red number in figure 4-2.

(1) User request access, the CSP first check the user's identity, if the user failed the identity verification will be directly denied by the CSP.

(2) If the user passed the identity verification, the trust dynamic management module will acquire the user's current trust value from trust database. Compare the user's trust value with minimum acceptable trust degree, if lower than minimum trust degree, the CSP will be denied

the accessing request.

(3) If the user's trust value is accepted by the CSP, the authorization module will grant the user with corresponding service degree and operation authority.

(4) During the entire accessing process, the behavior monitoring module will real-time monitoring user's behavior, collect and standardized the behavior evidence, and store in user's behavior database.

(5) Meanwhile, the trust evaluation module will also real-time calculate the user's behavior trust and store in the user's trust database.

(6) Trust dynamic management module will detect the updating of trust value, dynamically control the user's operation authority and service degree.

(7) Trust value will also feedback to the user, to guide and regulate access behavior, establish a long-term trust mechanism.

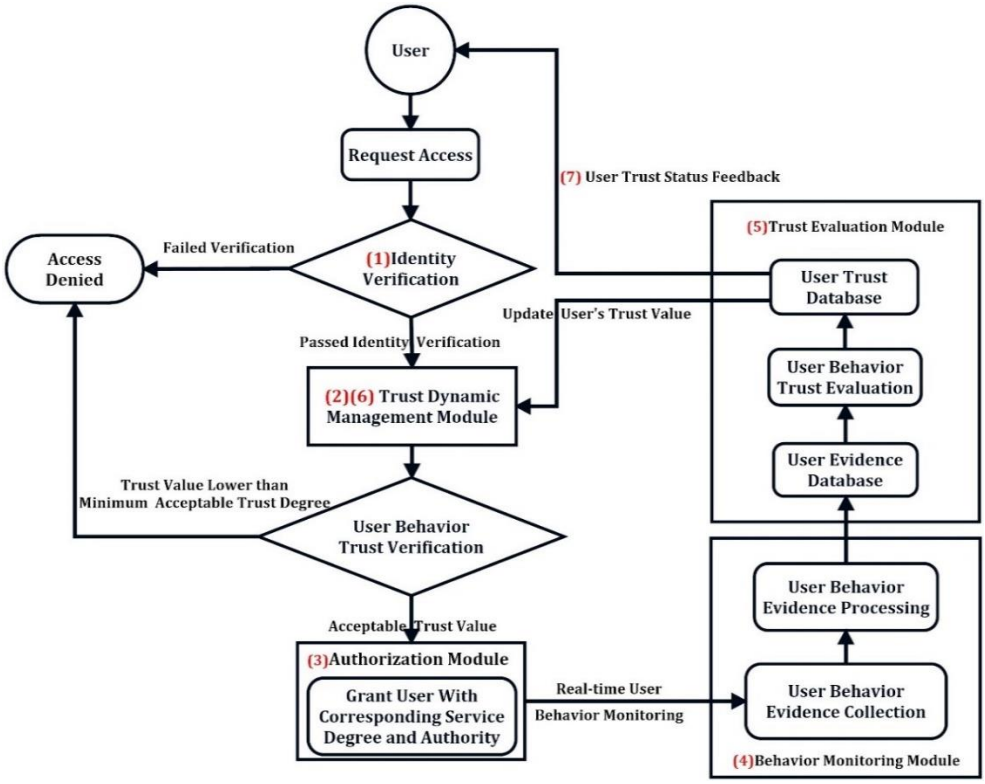


Figure 4-2 Authority Based Access Control Model Working Structure

■ Role-Based Trust Access Control Working Structure

The selected studies **S1**, **S6**, **S9**, and **S13**, utilized role-based trust access control working structure. The structure is illustrated as figure 4-3.

The role-based working structure including three important modules:

1. **Request Access Analysis Module:** verifying user's identity, identify user's ID and requested resource. The system will then bring the user's session history to calculate the trust value of the user.
2. **Trust Evaluation Module:** evaluate the trust value of the accessing user,

it will bring the user's session history, which is the interaction history record of the user and the system. Behavior evidence will be collected among the session history, the trust evaluation will be based on the behavior evidence data.

3. **Dynamic Access Control Module:** assign the accessing user with roles according to the user's trust value, constraints are pre-defined to control the correspondence of the role assignment. The module should also respond to the new request of the user during the interaction of a session, inform the trust evaluation module to re-calculate the trust value, and assign new roles to the user.

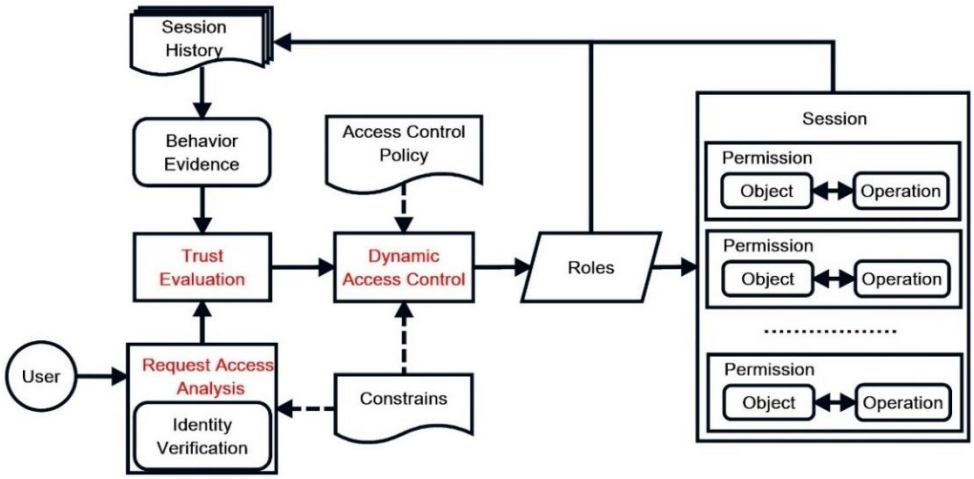


Figure 4-3 Role Based Trust Access Control Model Working Structure

The user obtains authority by inheriting pre-defined roles, the roles is a series operation permission on a specific object (data resource or resource node). The role based access control model assign user with different roles and corresponding priority according to the user's trust value, which depends on how good behavior the user had in the previous interaction history. Based upon this strategy, the cloud system can provide flexible access control.

Compare with authority based working structure, the role-based trust access control model assign trust verified user with pre-defined roles instead of service degree. In general, role-based trust access control model assign user with operation constraints on a specific object, like read, write, revise a documents, data, or configure virtual machines, etc. (Fine-grained), while authority based trust access control model assign user with operation constraints in the entire service system, like deploy a software, uploading data, obtain different levels of software service, etc. (Coarse-grained).

Thus, the role-based trust access control model is suitable for the massive data resourced based CC system, and the authority based trust access control model is suitable for the service based CC system. They both able to help improve the system security of CC.

- **Dynamic Trust and Access Update Strategy**

During the review of the selected research studies, studies **S1**, **S5**, **S6**, **S11** deployed dynamic trust update strategy in their trust-based access control model, which dynamically change the user's operation authority, service degree, or roles according to their current interaction behavior. The trust dynamic management module in the authority based trust access control model and dynamic access control module in the role-based trust access control model inherits this strategy. As illustrate in figure 4-4.

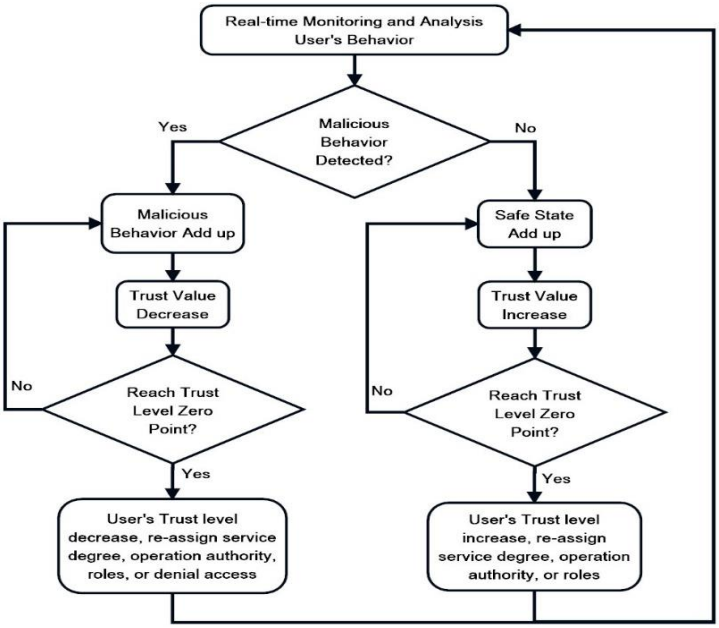


Figure 4-4 Dynamic Trust and Access Update Strategy

Dynamic trust and access update strategy prevent the security problem caused by assign user with authority before the interaction. Access control system will real-time monitoring accessing users, if a user enters the system with high-level operation authority, but continuing to make malicious behavior, the system will decrease his trust value, re-assign the user with lower service level and service degree according to the change of trust value, avoid the user cause greater harm to the system.

4.4.2 Answer of Research Question 2

RQ2: *What kind of cloud user behavior can be collected as evidence for trust evaluation?*

8 studies (**S1**, **S2**, **S5**, **S6**, **S8**, **S12**, **S14**, **S15**, and **S16**) are reviewed to conduct the answer of ***RQ2***, according to the studies **S6**, **S8**, **S14**, and **S15**, user behavior evidence can be divided into three categories.

1. **Reliability Evidence:** the evidence to present CSUs reliability characteristic during the interaction with the CSP. For instance, if the CSU's IP packet loss frequently, it reflects the user is on a non-secure network or not steady state; on the one hand, reduces the efficiency of cloud services; and on the other hand, brings potential virus attacks and risks to the on cloud resources and other CSUs.

2. **Performance Evidence:** the evidence to present CSUs performance characteristic, it has important significance to take full advantages of cloud service capability. CSUs with low-performance evidence will occupy the same cloud resource for a long period, lead to long time service waiting, and other CSUs are not able to acquire the service in time.
3. **Security Evidence:** the evidence to present CSUs security characteristic, including the user's likely risky behavior during the accessing. For instance, the malicious attack behavior, which will bring huge damage on the cloud resources and services.

Based on the upon classification principle, we collected user behavior evidence as shown in the following tables:

Table 4-6 Security Evidence Collection

	ID	Evidence Item	S.ID
Security Evidence	E1	The number of times user exceed authority attempt	**S1, S2, S5, S6**
	E2	The number of times user illegal connections	**S5, S6, S14**
	E3	The number of times user scan important resource ports	**S15, S16**
	E4	The number of times user carrying virus	**S15, S16**
	E5	The number of times malicious attack attempt	**S1, S2, S16**
	E6	Whether the IP address of accessing is unusual	**S16**
	E7	Whether the accessing time is unusual	**S16**
	E8	Whether user entered overflowed username or password	**S16**
	E9	Whether user inputs security sensitive keywords	**S14, S15**
	E10	Whether the user using proxy	**S14, S15**

Table 4-7 Reliability Evidence Collection

	ID	Evidence Item	S.ID
Reliability Evidence	R1	User data error rate	**S6, S15**
	R2	User IP packet loss rate	**S1, S2, S5, S14**
	R3	Connection establishment failure rate	**S2, S6, S8**
	R4	The number of logins failures	**S14, S15**
	R5	The number of trouble-free services	**S14, S15, S16**

Table 4-8 Performance Evidence Collection

	ID	Evidence Item	S.ID
Performance Evidence	P1	CPU occupancy rate	**S14, S16**
	P2	User's throughput capacity	**S5, S6, S15**
	P3	User's IP packet transmission delay	**S15, S16**
	P4	User's bandwidth occupancy rate	**S15, S16**
	P5	User's IP packet response time	**S15, S16**
	P6	User's threads occupancy rate	**S14**
	P7	Time of accessing duration	**S15, S16**
	P8	User's storage resource occupancy rate	**S1, S5**

The **S15 and S16** provide the behavior trust evidence acquirement methods. The above user behavior evidence items can be captured by network flow detection tools (Bandwidth[2], Cisco's CALIGARE[3]), intrusion detection tools (TCPDUMP[4]), and system recorded system event logs, auditing logs, network management logs etc. CSPs can also develop their own user behavior evidence collection software based on the service protocol standard, obtain customized user behavior evidence data to satisfy the system's security requirement.

During the phase we answering the research question2, we obtained following important discoveries.

1. The evidence items we summarized in this study is basic items that can be collected for UBT evaluation.
2. Different CC systems or applications can develop their own evidence collection standard according to their own security requirements and service protocol.
3. We are not able to acquire these behavior data due to the time and resource limitation.
4. Even we obtained the actual datasets, the calculation result will be meaningless if we don't consider the CC system security standards and requirements.

The above research discoveries made us concentrate on the trust management process and comprehensive trust evaluation instead of single trust evaluation that based upon collected user behavior evidence.

4.4.3 Answer of Research Question 3

RQ3: *What attributions of trust will affect the trust evaluation?*

Table 4-9 Data Synthesis for *RQ3*

ID	Attribution	S.ID	Solution	Solution Reference
A1	Subjective	**S6, S8, S12, S15**	AHP	**S6, S8, S12**
			Fuzzy-ANP	**S15**
A2	Trust will expire over time	**S6, S8, S10**	Time-Flag	**S6**
			Three-level Interaction Range	**S8**
A3	More interaction data, more accurate	**S3, S16**	Uncertainty indication	**S3**
A4	Trust can be forged	**S3, S16**	Trust Record Stack	**S3**
			Slow Rise Rapid Decrease	**S16**

[2] Bandwidth: http://bandwidthd.sourceforge.net/
[3] Cisco CALIGARE: http://www.caligare.com/netflow/caligare_flow_inspector.php
[4] TCPDUMP: http://www.tcpdump.org/#documentation

Seven studies (**S3**, **S6**, **S8**, **S10**, **S12**, **S15**, and **S16**) were selected and reviewed in order to answer the ***RQ3***, the data synthesis as illustrated in table 4-9. For each selected study, we not only summarized the trust attributions that mentioned in the study but also capture the corresponding method that possible to address the affection.

A1. Nature of Trust – Subjective

The concept of trust has its roots in social science, it is subjective as a nature characteristic. In the human society, trust judgment is influenced by internal factors, such as emotions, confidence, cognitive ability, etc. and external factors, such as social relations, recommendation, historical data, context etc. Generally speaking, the generation of human trust is a subjective judgment on a subjective action.

In Viljanen et al [40], they proposed a comprehensive ontology model of dynamic trust that is illustrated in figure 4-5. The model integrated different input factors of different trust models, and comprehensively described the influence factors of trust evaluation.

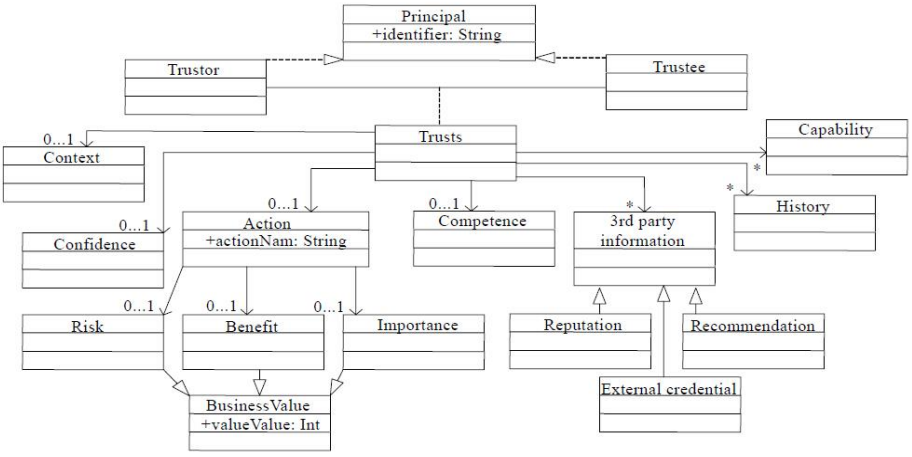


Figure 4-5 Dynamic Trust Ontology Model [38]

The evaluation of UBT is based on the user's behavior evidence (Actions). In the CC environment, user's behavior is complicated and changeable, the trust evaluation method has to consider the weight (risk, benefit, importance) of each behavior evidence item in a given context, and also decide which evidence will be a major impact on the final evaluation result. During above procedure, system have to make a subjective judgment on given context and user actions, inaccurate evaluation result will be produced if the system fails to identify the major influence factor, and the access control system will not able to assign right authority to the user accordingly.

S6, S8, and S12 adopted AHP (Analytic Hierarchy Process) method to handle the subjectivity of trust evaluation. AHP is an analysis method for decision science (divide and treat theory), the main idea of AHP is through the analysis of complex systems-related factors and their mutual relations, simplify the system

into an ordered hierarchical structure, so that these elements are incorporated into different layers, and form a multi-layered analysis model, the final analysis problem comes down to the relative importance comparison (weight determination) between lower level of the system (evidence, measurements) and the highest level (overall goal) [41].

The AHP based UBT evaluation procedure as follow: Firstly, developed a top-down hierarchy to decompose the trust evaluation problem, a three-level hierarchical structure is illustrated in figure 4-6 (we here used the behavior evidence we summarized in section 4.4.2). Secondly, pairwise compare the importance of every evidence under each characteristic. For instance, pairwise compare the importance of evidence P_1 to P_n under performance evidence, assign higher weight on the evidence that have higher impact among the other performance evidences. Finally, after every evidences have been assigned with weight, pairwise compare the importance of every characteristics. For instance, pairwise compare the importance of performance evidence, reliability evidence, and security evidence, decide which characteristic has major impact among the other characteristics in the given context, and assign higher weight.

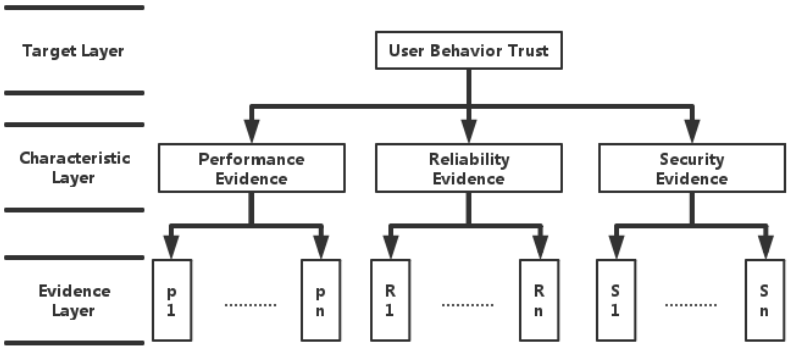


Figure 4-6 AHP Method Decompose UBT

In this way, we can identify which evidence item has the highest impact on current trust evaluation by multiply the evidence weight and the characteristic weight. With the identification of major influence factor, the trust value calculation will produce more accurate and objective result. The significance comparison and weight allocation are supported by an expert system with pre-defined decision protocol.

In study **S15**, they adopted Fuzzy-ANP (Analytic Network Process) method to handle the problem. According to the study description, the **S15** identified the AHP evaluation method described above very depends on the expertise of expert system, the weight value judgment on the impact factor is still with strong subjectivity. ANP is developed based on the idea of AHP, but with more complex network structure than hierarchy structure, using more profound mathematical knowledge. Overall, the ANP is more scientific and more comprehensive than AHP.

The study **S15** also used the triangular fuzzy number to replace the 1-9

weight scale, developing fuzzy comparison matrix, which overcomes the uncertainty problem of weight value representation.

A2. Trust Will Expire Overtime

The trust record can be compared to the "best before date" of the food in the supermarket. If the record of trust was generated in very old time and out of date, the value of the trust will gradually decrease with the time, and finally invalid.

For instance, if a user stop contact with the system for a long time, even though he maintain a good behavior in the past, and with good trust record, when the time the user re-connected with the system, the expired the trust record will no longer available for the trust evaluation, the system have to consider the user as stranger user, and re-calculate trust value according to his current interaction behavior.

If a trust-based access control system doesn't consider the trust expiration, the system might make the misjudgment on the user's current trust status.

In study **S6**, they assign each trust record with a time flag, during the trust evaluation process, a weight value (scale between 0-1) will assign to each trust record, the older the trust record, the lower the weight. It also pre-defined a valid time range of trust record, expired trust record will be deleted from the system trust database.

In study **S8**, they defined the trust record positive interaction range, negative interaction range, and uncertainty interaction range.

The BTRs in the negative interaction range is far from the current time, and will not participate in the trust evaluation. The BTRs in the uncertainty interaction range is passed for a period of time but not expired, the system considers this part of BTRs as uncertain records, and assigned with uncertainty weight during the trust calculation. The BTRs in the positive interaction range are fresh BTRs, provide comprehensive trust evaluation with most valuable evidence, assign with higher weight on these BTRs during the trust calculation accordingly. The method illustrated as figure 4-7.

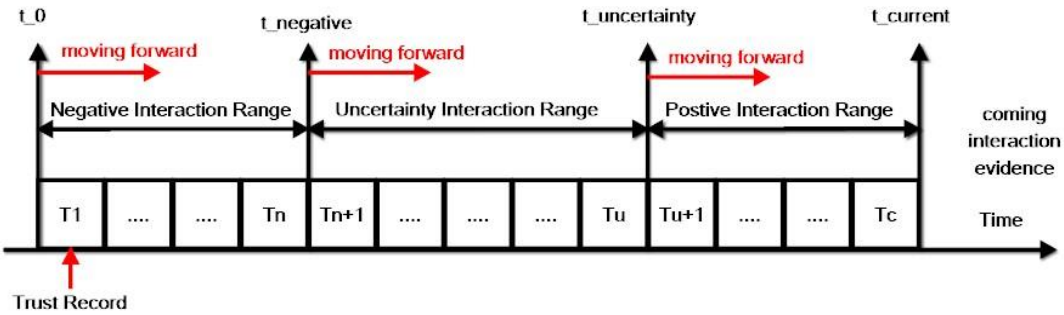


Figure 4-7 Trust Record Time Range

A3. Accurate Trust Evaluation rely on Constantly Accumulating Interaction

In the social interaction, stable trust is established based on long-term interaction history, people tend to conduct negative trust judgment on brief

interaction, people are not able to trust the person they met for the first time and even with serval time interaction, they will also doubt their trust judgment (trust evaluation uncertainty). Thus, valid and stable trust evaluation result relies on long-term constant interaction record.

In general, the credibility of trust evaluation result is in proportion to the user's access times and access duration.

In study **S3**, they used a variable called "Trust Uncertainty (T_Uncertainty)" to indicate the user with a few amount of interaction records. A stranger user will be assigned with initial T_Uncertainty=1, with the gradual accumulation of interaction record, the T_Uncertainty gradually reduce and eventually tends to 0. When the access control system identified a user with high T_Uncertainty, the system will reduce the authority degree assign to the user according to the T_Uncertainty. Avoid uncertain trust evaluation brings risk to the system.

A4. Trust can be forged

Fraud behavior exists in the social environment and trust management system at the same time. In a social environment, scammers through forged documents, setting environment, role-playing etc. to perform high-quality good behavior within a short period of time to get high trust from the target, in order to achieve the ultimate Fraud. In trust management system, a malicious user can cheat the system with a period of time good behavior to obtain high trust evaluation, after obtaining superior service degree and authority, they can cause greater damage to the system.

In study **S3**, they proposed "trust record stack" method to overcome this problem. Every new accessing user will have a trust record stack full of stranger trust record (for instance, 0.5 for the trust value range [0, 1]), the size of the stack depends on the application scenario. Each time the stranger user produce a new trust record and replace one strange trust record in the stack. The trust evaluation of the user will be based on all the records in the stack, even the user have good behavior records in the first few times, the comprehensive trust value of this user will remain low as the strange BTRs in the stack dilute a few good BTRs. Therefore, a stranger user cannot achieve high behavior trust value by a small number of good interaction behaviors. The disadvantage of this method is not able to prevent a long-term user fraud, a long-term user's identity might be stolen, or other potential reason become a malicious user, and after the trust record stack has been full of real interaction records, the method will not able to prevent short-term trust fraud.

In study **S16**, they mentioned when a trust evaluation system detected a fraud user, who maintain a period of time good behavior and then conducted a malicious behavior, should be given severe punishment.

In general, to overcome the problem of trust fraud, the trust evaluation system should keep "Slow rise, Rapid decrease" principle, avoid user's trust value rapid growth in a short period of time, and punish malicious behavior with rapid

trust decrease.

4.4.4 Answer of Research Question 4

RQ4: *What is the currently state-of-art UBT based CC access control model?*

Eight studies each provided their own design of UBT based CC access control model. An evaluation of each study is presented as follows:

In study **S1**, they towards the complexity and inaccuracy of role based access control model in CC system, **S1** proposed a flexible RBAC model based on trust. The FRBAC model evaluation the direct trust between CSP node and CSU node according to CSU's behavior; at the meantime, obtain recommendation trust from other CSP nodes, combined the direct trust and recommendation trust to produce comprehensive trust value of accessing CSU. Based on the evaluation result, FRBAC model assigns the user with different roles and corresponding authority. FRBAC model adopts AIMD (additive-increase, multiplicative-decrease) algorithm in order to punish the malicious CSU node. And finally, introduced the notion of accuracy concept into the FRBAC model to ensure the evaluation result is reasonable and objective.

- **Advantages:** FRBAC model well considered the recommendation trust, multi-platform trust computing collaboration can avoid the subjective of trust evaluation to a certain extent. And the AIMD algorithm can improve the trust fraud resistance capability of the system.
- **Disadvantage:** FRBAC model not able to prevent the synergies cheating, no effective screening capability towards recommendation trust.

In study **S2**, they present a UBT evaluation model based on Fuzzy-Mathematics in CC. The trust evaluation combined direct trust from the local domain, recommendation trust from the same CSP but different domain, and indirect trust from other CSPs but familiar with. The evaluation based on Fuzzy-Mathematics theory, the aim is to reduce the subjectivity of trust evaluation by a fuzzy representation of trust degree.

- **Advantages:** the model is able to prevent the synergies cheating by using domain trust concept. According to the trust degree of collaboration CSP entities, assigns different weight on recommendation trust and indirect trust, in order to avoid too much influence receiving from outside.
- **Disadvantages:** the trust evaluation method not considered the BTRs expiration, and also the BTRs time affection, therefore, not able to reflect the actual behavior trust of CSU. And the model doesn't consider trust fraud situation, not able to prevent malicious user obtain high trust value within a short-term good behavior.

In study **S3,** they designed a UBT evaluation method based on D-S theory (Dempster–Shafer theory), the basement of D-S theory is the Bayesian theory of subjective probability [42], in order to overcome the subjective of trust evaluation. The method takes recommendation trust as assistant evidence to improve the accuracy of comprehensive trust evaluation; and also adopt an

improved fusion approach to eliminate the conflict recommendation, in order to handle synergies cheating problem.

- **Advantages:** the model well considered the trust expiration problem by using trust record time range structure we described in section 4-3. Actual reflect the user's most recent behavior trust. The evaluation accuracy on good users and malicious users is high.
- **Disadvantages:** the model doesn't consider the trust fraud problem, and also no correspond punishment strategy on malicious behavior.

In study **S5**, they proposed a DTBAC (dynamic trust based access control) model, target to solve the problem of malicious user error authorization problem in CC environment.

- **Advantages:** DTBAC is well considered the identification of malicious behavior, able to fast response to the user's malicious behavior and take countermeasures on the authorization.
- **Disadvantages:** DTBAC doesn't consider the BTRs expiration problem, and doesn't consider the closer the time of behavior, the higher the impact.

In study **S6**, they proposed a MTBAC (mutual trust based access control model) model, assign different user with different available CSP according to the user's behavior trust and the credibility of CSP.

- **Advantages:** MTBAC model solved the trust uncertainty problem by using recommendation trust, and also the evaluation method adopts AHP theory to reduce the subjective of trust evaluation.
- **Disadvantages:** MTBAC model doesn't consider the BTRs expiration problem, and doesn't consider the closer the time of behavior, the higher the impact. Therefore, not able to actual reflect users' actual behavior pattern and behavior trust.

In study **S7**, they proposed a CC trust based dynamic access control model inspired by GTRBAC model. The main idea is to combine the evaluation of user behavior trust and recommendation trust, generate the comprehensive user behavior trust value as the decision basis for role assignment, and overcome the CC security problem.

- **Advantages:** the model clearly defined the role assignment protocol according to different user trust degree, achieve the dynamic role assignment.
- **Disadvantages:** not well defined the utilization of recommendation trust, not able to solve synergies cheating problem. Also, no any strategy provided to deal with user's malicious behavior, no identification method defined and no countermeasures proposed. Is a theoretical ideal model.

In study **S11**, they proposed a role based access control model incorporate with the notion of UBT. The model defined different contexts of trust evaluation and adopt the idea of trust model as evaluation theory. The system is able to

provide flexible and scalable authorization strategy.

- **Advantages:** the model defined the different trust evaluation context, and the trust evaluation method borrows the idea of trust model, which help to reduce the subjective of trust evaluation, improve the credibility of trust evaluation result.
- **Disadvantages:** the evaluation process is too complex, and it didn't have specific measurements toward the trust characteristic; therefore, it is difficult to practice in real CC environment.

In study **S14**, they proposed a dynamic UBT evaluation method to solve the CC security problem. Adopt AHP method to obtain a subjective weight of each user behavior evidence, and entropy method to obtain objective weight; solve the subjectivity of trust evaluation.

- **Advantages:** able to reflect essential behavior pattern of CSU through the combination of entropy method and AHP method, the evaluation result are objective and valid.
- **Disadvantages:** no corresponding strategy to solve trust fraud problem, and didn't consider the trust records expiration problem. The evaluation method is too complex to apply in practice.

According to the above evaluation, we defined the following model performance evaluation synthesis table (table 4-10) to evaluate the performance of each identified study. The evaluation item is based on the study of ***RQ3*** and the recommendation from L. Tian et al [43]. (The notation ● means the model performs well at this item; ○means the model performs badly at this item; - means not mentioned in the paper, or the model is not related to this problem.)

Table 4-10 Model Performance Evaluation Synthesis Table

S.ID	Subjectivity Weakening	Trust Expiration	Trust Fraud	Time Impact	Synergies Cheating	Practicability	Score
S1	●	○	●	○	○	●	3
S2	●	○	○	○	●	●	3
S3	●	●	○	○	●	●	4
S5	-	○	●	○	-	●	2
S6	●	○	○	○	-	○	1
S7	●	○	○	○	●	○	2
S11	●	●	○	●	○	○	3
S14	●	○	○	●	-	○	2
Total	7	2	2	2	3	4	

According to the performance evaluation synthesis, most of the current UBT based access control model fulfilled the trust subjectivity weakening, but have the weaknesses, such as trust expiration problem, trust fraud problem, and time impact problem. Therefore, the UBT based access control model proposed in this paper will focus on solving the weaknesses mentioned above. As the model provided by study **S3** has the highest score among the others, we extract the model from study **S3** as a comparison object in the later prototype simulation.

CHAPTER 5. TDW BASED ACCESS CONTROL MODEL

In this chapter, we designed our own UBT based access control model called Triple Dynamic Windows based Access Control Model (TDWACM). In addition, this chapter introduced the basic design principle, model features, trust update strategy, and trust evaluation method.

5.1 Basic Principle

In this section, we defined the basic design principle of our model and present the trust definitions and constraints we adopted in the design.

5.1.1 Basic Design Principle

According to the trust attributes and the influence we summarized in section 4.4.3, we defined the basic UBT evaluation principle as follow:

1. Expired BTRs will not participate in the trust evaluation.
2. In trust evaluation, the affection of valid BTRs is inversely proportional to their age.
3. The credibility of trust evaluation is in proportion to the size of user's BTRs.
4. Trust slow rise to prevent the user with fewer interactions to quickly obtain high trust value.
5. Trust rapid decrease to punish the user carry out malicious behavior.

5.1.2 Basic Definition and Constraint of Trust

The UBT evaluation result (Trust Value) is a double-precision floating point number between [0, 1). The evaluation is based on the user behavior evidence in BTRs.

The trust degree and corresponding service strategy classified as follow:

- If (0≤ Trust Value < 0.15), the trust degree is Strong Mistrust, access denied.
- If (0.15 ≤ Trust Value < 0.35), the trust degree is Mistrust, the service strategy provides a small quantity of basic services and low authority. High alert on this type of user.
- If (0.35 ≤ Trust Value < 0.65), the trust degree is General Trust, the service strategy provides basic services and general authority.
- If (0.65 ≤ Trust Value < 0.85), the trust degree is Trust, can provide with a large quantity of services and high authority.
- If (0.85 ≤ Trust Value < 1), the trust degree is Very Trust, can provide with core services and superior authority.
- User's initial trust value as 0.5.
- Good behavior corresponding Trust Value > 0.5.
- Malicious behavior corresponding Trust Value < 0.5.

5.2 TDW Based Behavior Trust Evaluation Method

In this section, we present the structures of our designed model and the feature of designed elements.

5.2.1 The Triple Dynamic Windows

Three dynamic windows including valid trust window, trust establish window, and most recent trust window, illustrated as figure 5-1.

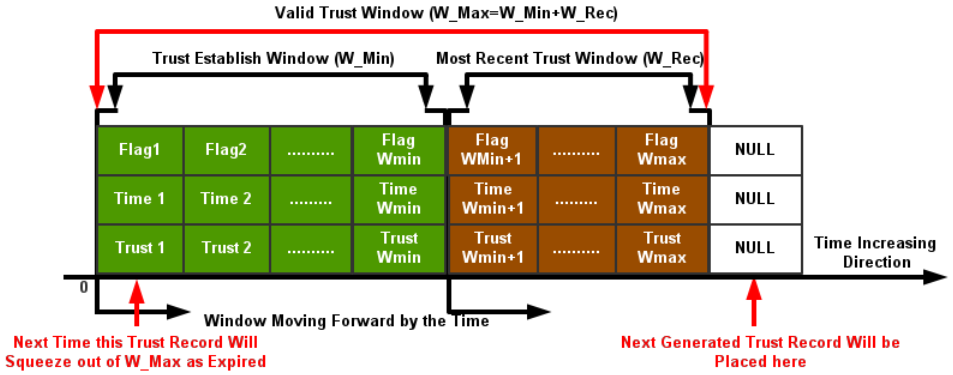


Figure 5-1 Triple Dynamic Windows Method

- **Valid Trust Window:** Defined the range of maximum preserved BTRs, if a trust record is expired, it will be squeezed out of the Valid Trust Window from the left side. (The size of window defined as W_Max.)
- **Trust Establish Window:** Defined the least number of access records during the trust establishing. (The size of window defined as W_Min). If a user's BTRs count less than W_Min, the actual trust evaluation adopts "slow rise" strategy to reduce the risk of trust uncertainty, and prevent trust fraud.
- **Most Recent Trust Window:** Defined the range of the most recent BTRs. (The size of window defined as W_Rec). The trust evaluation of the BTRs in W_Rec presents the user's most recent behavior trust, ensure the final evaluation result is able to reflect the current state of the user, timely adjust trust result.

The size relation of above three windows: W_Max = W_Min + W_Rec, and the size of each window can be adjusted in order to satisfy different system requirements.

5.2.2 BTRs Classification

There are three types of BTRs, we used Flag to indicate:

- **Strange User Record:** used in Trust Establish Window initialization, and as BTRs during the pause when a user stop interaction for a long period. (Marked as Strange)
- **Normal User Record:** the user's actual interaction generated BTRs during the valid period. (Marked as Normal)

- **Punishment User Record:** partial user's normal BTRs decreased due to the user's malicious behavior. (The punishment effected BTRs marked as Punish).

5.2.3 Windows Initialization and Workflow

The BTRs in Trust Establish Window will be initial with strange user records, the trust value mark as STR, and can be modified according to different system requirements.

As the user begin to access, the initial strange BTRs constantly being replaced by normal BTRs, and all the strange BTRs in Trust Establish Window will eventually be replaced by normal BTRs. The initialization and replacement process are illustrated as figure 5-2. The figure illustrated the situation when the system captured three user's BTRs. Three strange BTRs were replaced by normal BTRs.

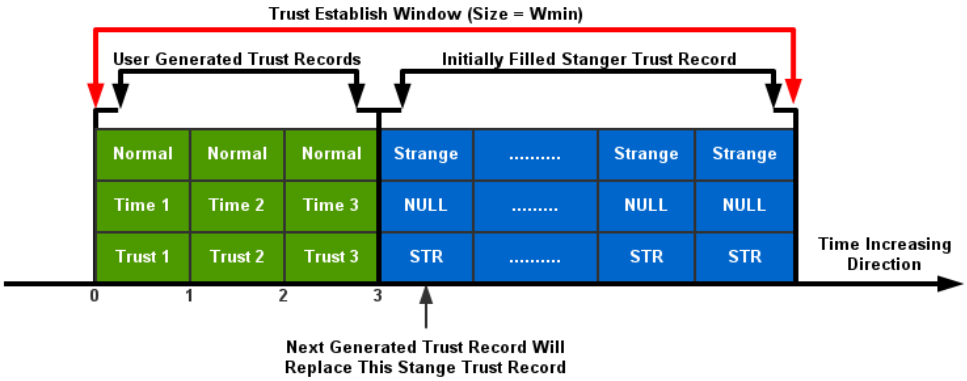


Figure 5-2 Initialization of Trust Establish Window

After the normal BTRs filled up Trust Establish Window, the Most Recent Trust Window will start to store the coming BTRs. The process illustrated as figure 5-3. In this way, the Most Recent Trust Window will always maintain the most recent collected BTRs.

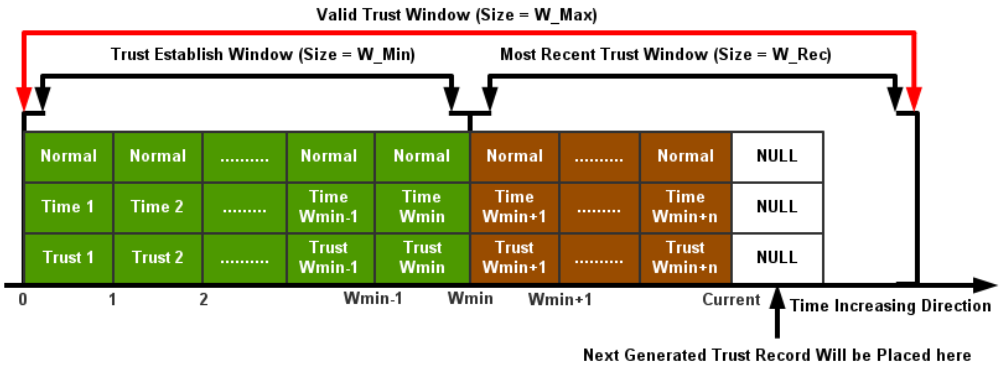


Figure 5-3 Most Recent Trust Window

When the total number of captured BTRs is larger than W_Max, the oldest trust record will be squeezed out of Valid Trust Window from the left side. The process

illustrated as figure 5-4. The borderlines of three windows will move one step right after the system receiving a new trust record each time. In this way, the system will only maintain time valid BTRs, the expired BTRs will be automatically deleted accordingly.

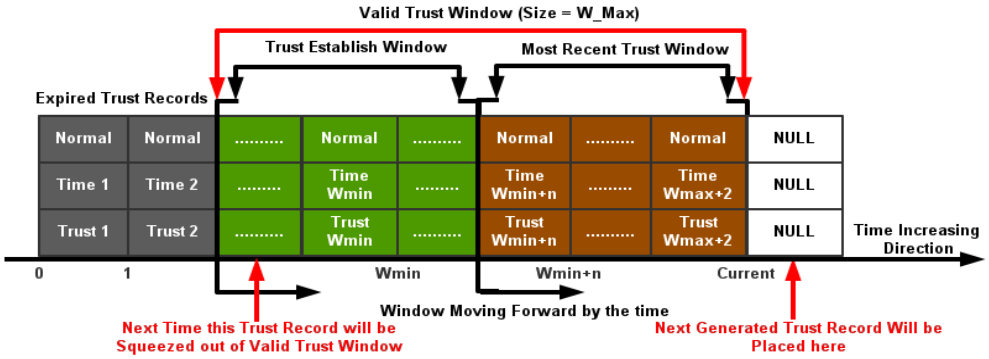


Figure 5-4 Squeeze out Expired BTRs

5.3 BTRs Update Strategy

In this section, the behavior trust records updating strategy is presented.

5.3.1 Malicious BTRs Update Strategy

If a BTR is evaluated as malicious behavior (Trust Value < 0.5), a part of (set as N) recently evaluated trust values will be reduced to mistrust value ($\text{mis}_{\text{trust}}$), so that the user's comprehensive trust value will be decreased rapidly, in order to punish the user's malicious behavior.

The trust punishment need to consider four aspects:

5. The malicious extent: the greater extent of malice, the greater the punishment. Assume the Trust Value of the detected malicious behavior is T_m, the lower the T_m, the greater the punishment.
6. The user's current comprehensive trust value (T_c): the higher user's current trust value, the greater the punishment. As the user's current trust value indicate the received service degree and authority, the higher the current trust value, the greater user's past authority, the greater damage can cause by current malicious behavior.
7. The number of malicious behaviors (N_m): more the number of malicious behavior, the greater the punishment. For a very small number of malicious behavior, it can be judged as possible misoperation. But for multiple times malicious behaviors, the intensity of punishment will continue to increase.
8. The actual system security requirements and application scenarios: defined penalty factor α.

According to the above analysis, we can calculate the n by formula (1), and $\text{mis}_{\text{trust}}$ by formula (2).

$$N = \min\left\{\left\lceil \alpha * \frac{T_c}{T_m} \right\rceil, m\right\} \quad (1)$$

$$\text{mis}_{\text{trust}} = \frac{0.5}{N_m} \quad (2)$$

The value m in formula (1) is the number of valid BTRs which excluded expired BTRs and strange BTRs, the punishment is only applied on the actual user's BTRs, the expired BTRs or strange BTRs will not get punish.

Assume we have α=10, T_m=0.3, T_c=0.6, N_m=2, m=30, with formula (1) we get the N= 20, and with formula (2) we get $\text{mis}_{\text{trust}}$ = 0.25. Which means the punishment is to decrease the 20 recent trust value to 0.25. The modified BTRs marked as punish. The process illustrated as figure 5-5.

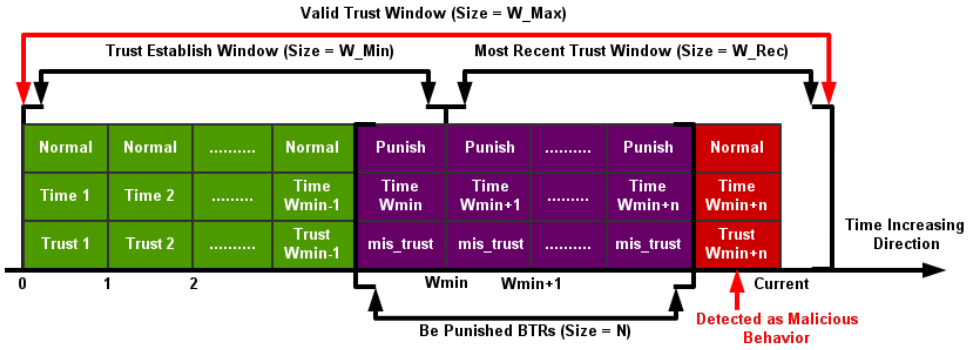


Figure 5-5 Malicious BTRs Update Strategy

5.3.2 Expired BTRs Update Strategy

When a user stops accessing the system for a long period, some BTRs farther away from the current time, and gradually expired, (Current Time – Time i > W_Max). However, as the user stop accessing the system, there are no new BTRs generated, the oldest BTRs will not get squeezed out from the Valid Trust Window, so here we need an expired BTRs update strategy.

We designed the update strategy by replacing the expired BTRs with Strange BTRs. When the system detect the user stop accessing the system, and some BTRs are out of date, it will replace these BTRs with Strange BTRs. The process illustrated as figure 5-6.

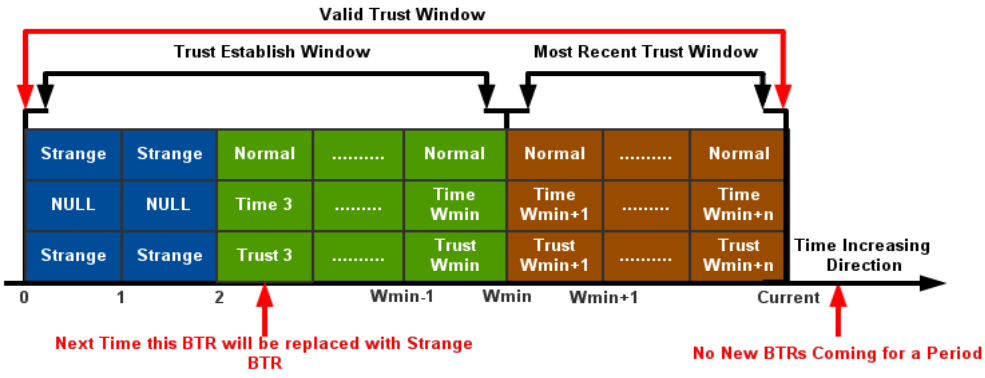


Figure 5-6 Expired BTRs Update Strategy

In this way, a user without access system for a long time, the user's trust value will gradually tend to be a strange user. Both the trusted user and the untrusted user will gradually tend to be strange users while stop accessing the system for a long time, this property coincides with the nature of trust of social reality.

5.4 Trust Evaluation Principle

In this section, the trust evaluation principle and trust update strategy are presented and explained.

5.4.1 Comprehensive UBT Evaluation

The basic idea of the comprehensive UBT evaluation is a more recent behavior has greater proportion impact in the evaluation. Therefore, we have the formula (3) to evaluate all the BTRs in Valid Trust Window.

S represent the total number of BTRs in Valid Trust Window.

$$\text{Trust}_{\text{valid}} = \sum_{i=1}^{S} \left[\frac{(time_i - time_0)}{\sum_{i=1}^{S} (time_i - time_0)} \right] Trust_i \tag{3}$$

5.4.2 Most Recent UBT Evaluation

Based on the same theory above, we also calculate the most recent UBT by formula (4). The most recent UBT can help system identify the most recent user behavior tendency, timely response to unexpected malicious behavior.

$$\text{Trust}_{\text{recent}} = \sum_{i=W_{min}+1}^{W_{Max}} \left[\frac{(time_i - time_{W\_Min})}{\sum_{i=W_{Min}+1}^{W_{Max}} (time_i - time_{W\_Min})} \right] Trust_i \tag{4}$$

5.4.3 Actual UBT Evaluation in Trust Establish Window

In order to avoid the user's malicious behavior be diluted by strange BTRs, we calculate actual UBT based on the BTRs generated by actual user interaction by formula (5).

$$\text{Trust}_{\text{actual}} = \sum_{i=1_{Flag=Normal}}^{W_{Min}} \left[\frac{(time_i - time_0)}{\sum_{i=1_{Flag=Normal}}^{W_{Min}} (time_i - time_0)} \right] Trust_i \tag{5}$$

5.4.4 UBT Update Strategy

This paper adopts a conservative strategy, the UBT update strategy divided into two cases discussed.

1. When (S < W_Min), which the number Normal BTRs less than the size of Trust Establish Window. Compare $\text{Trust}_{\text{actual}}$ and $\text{Trust}_{\text{valid}}$, the decision making as illustrated in formula (6).

$$\text{Trust} = \begin{cases} Trust_{actual}, & Trust_{actual} \le Trust_{valid} \\ Trust_{valid}, & Trust_{actual} > Trust_{valid} \end{cases} \tag{6}$$

2. When (W_Min < S < W_Max) and (S>W_Max), which the number of Normal BTRs more than the size of Trust Establish Window. Compare

$Trust_{recent}$ and $Trust_{valid}$, the decision making as illustrated in formula (7).

$$\mathbf{Trust} = \begin{cases} Trust_{\text{recent}}, & Trust_{recent} \le Trust_{valid} \\ Trust_{valid}, & Trust_{recent} > Trust_{valid} \end{cases} \quad (7)$$

In this way, the system can prevent malicious user obtain high trust value within a small number of good behavior interaction, and also reflect the actual trust value of mistrust user.

CHAPTER 6. PROTOTYPE & SIMULATION

In this chapter, we developed the prototype of TDW based Access Control Model and a simulation environment by NetLogo. We followed the research strategy we designed in Section 3.2, collected simulation result, and comparative analysis the result with a comparison object model extracted from study **S3**, in order to verify the contribution and limitation of TDW based Access Control Model.

6.1 Prototype Environment Setting

In this section, the prototyping tool is explained, the simulation environment is defined, and simulation configuration is presented.

6.1.1 Prototyping Tool

According to the recommendation of study **S3** and study **S5**, we chose NetLogo as our development tool, and simulation environment.

NetLogo is an agent-based programming environment used to simulate the natural and social phenomena [44]. NetLogo is a development platform inherited the Logo programming language. It improves the Logo language inadequate control of a single individual, it can control thousands of simulated individuals' behavior. Therefore, NetLogo can well simulate the microscopic behavior of the individuals and the macroscopic evolution. NetLogo is suitable for the simulation of natural and social phenomena, especially suitable for simulation of time-variation complex systems.

We used NetLogo to develop the TDWACM prototype and a simulation environment; we simulated the basic elements of CC network environment, including CSP, and different types of CSUs, assign different types of CSUs with different behavior pattern.

6.1.2 Simulation Environment

The simulation external environment setting as illustrated in table 6-1:

Table 6-1 External Simulation Environment

Item	Parameter
CPU	Intel Core i5-2430M 2.4GHz
RAM	8GB
Operating System	Windows 10 x64
Development Tool	NetLogo 5.3.1

The simulation internal environment elements setting as follow:

There are only one CSP in the simulated environment, represented by a gray

turtle.

CSUs are classified into 5 types: good users, bad users, cheat users, random users, and intermittent users.

- Good users: always carry out good behaviors, represented by green turtles, the number of good users can be modified by a slide bar, and set as 200.
- Bad Users: always carry out bad behaviors, represented by red turtles, the number of bad users can be modified by a slide bar, and set as 200.
- Fraud Users: keep very good behaviors for a period of time, and then carry out several times malicious behavior, and then return to good behavior; continue to cycle this process. Represented by yellow turtles, the number of cheat users can be modified by a slide bar, and set as 200.
- Random Users: carry out good behaviors and bad behaviors randomly. Represented by blue turtles, the number of random users can be modified by a slide bar, and set as 200.
- Intermittent Users: intermittent interact with the server, and always carry out good behaviors during the interaction period. The length of interaction time set as 30 and pause interaction time set as 60. Represented by violet turtles, the number of intermittent users can be modified by a slide bar, and set as 100.

The interface as shown in figure 6-1. The circles represent the different trust degree, closer to the center, the higher the trust value.

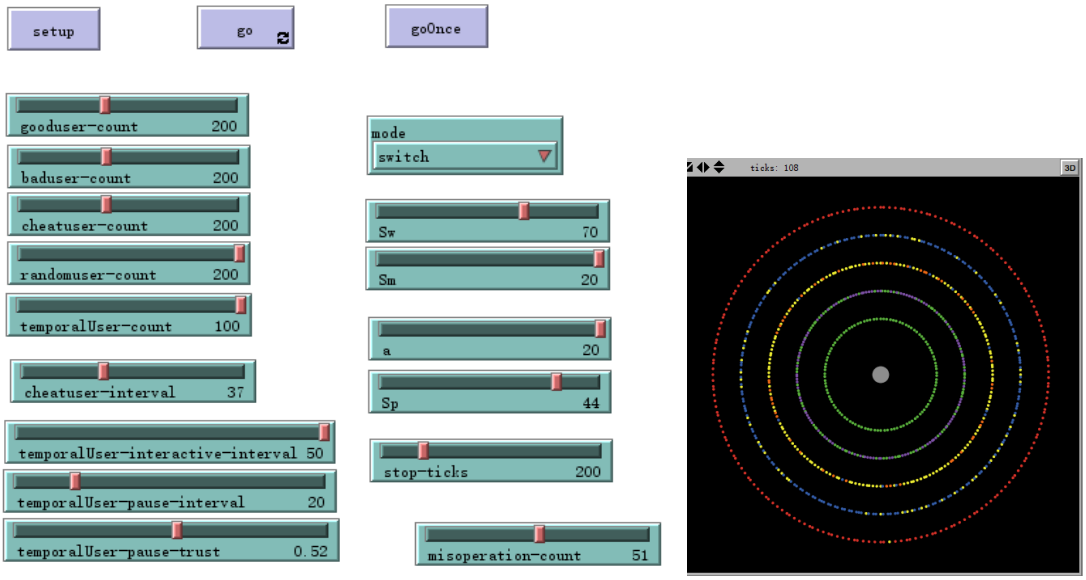


Figure 6-1 Established Prototype and Simulation Environment in NetLogo

6.1.3 Prototype Configuration

The prototype configuration is illustrated as table 6-2.

Table 6-2 Prototype Configuration

Item	Parameter
Valid Trust Window Size (W_Max)	100
Trust Establish Window Size (W_Min)	70
Most Recent Trust Window Size (W_Rec)	30
Initial User Trust Value (T_i)	0.5
Penalty Factor (α)	20
Strange Trust Value (T_s)	0.5

6.2 Simulation Result and Analysis

In this section, the simulation results are presented and evaluated.

6.2.1 Verification

In this section, we compare the basic UBT evaluation performance on good users, bad users, and random users with the model provide by **S3**, with same input datasets. Verify the basic functionality of TDW based Access Control Model. The performance as illustrated in figure 6-2, and figure 6-3.

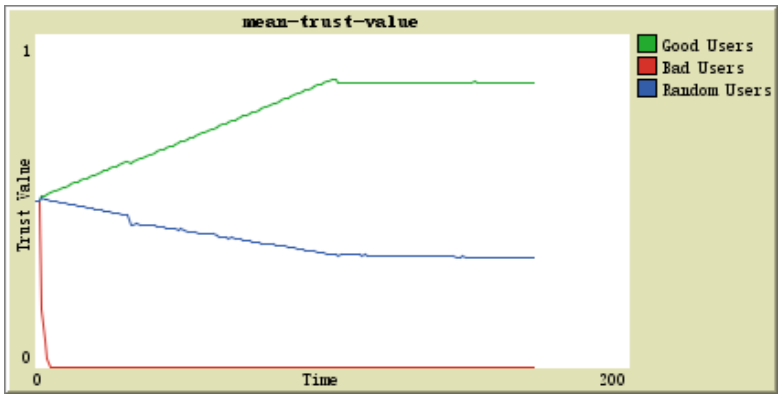
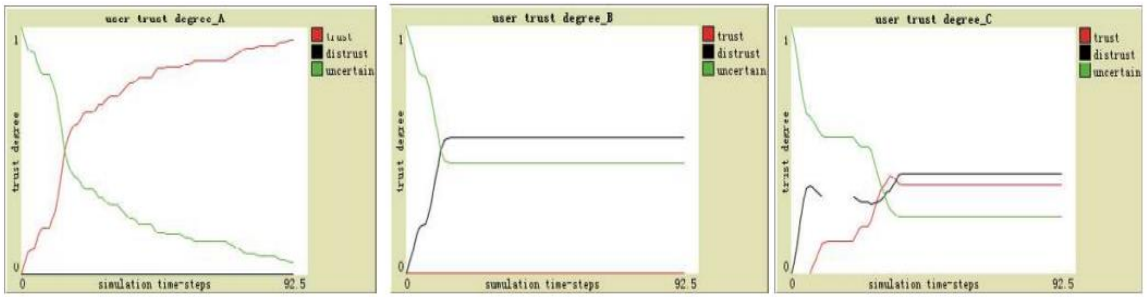


Figure 6-2 Trust Value of Good users, Bad Users, and Random Users in TDW Model



(d) the trust degree of the honest CU (e) the trust degree of the malicous CU (f) the trust degree of the random CU

Figure 6-3 (d) Honest Users, (e) Malicious Users, (f) Random Users [S3]

The trust value of good users is following the "slow rise" principle, reached the peak value at time 112 with mean value 0.866, and bad users is following the "rapid decrease" principle, reached the bottom line at time 6 (access denied); which similar to the performance of the **S3** model. The trust value of random users overall decline, which is accord with the evaluation requirement on this type of user. Besides, the "slow increase" growth rate can be adjusted by the size of Trust Establish Window, the bigger Window size, the smaller growth rate.

The trust degree distributions of these three type of users are shown in table 6-3. All the bad users are denied access with strong mistrust, the two models have the same performance. In TDW model, 179 random users are mistrusted and 21 are generally trusted while the **S3** model has 68 mistrusted and 132 general trusted random users, which indicate the TDW model is much more conservative than the **S3** mode. And the last, 53 good users are trusted, and 147 are very trusted in TDW model, has less user obtain very trust degree than the **S3** model, which indicate the "slow rise" principle has affected the trust value increasing speed. Overall, we conclude the TDW based Access Control Model is valid as an access control mechanism.

Table 6-3 Trust Degree Distribution Comparison

	User Type	Strong Mistrust	Mistrust	General Trust	Trust	Very Trust
TDW Model	Good User	0	0	0	53	147
	Bad User	200	0	0	0	0
	Random	0	179	21	0	0
S3 Model	Good User	0	0	0	21	179
	Bad User	200	0	0	0	0
	Random	0	68	132	0	0

6.2.2 Comparison

The comparison aim on the trust fraud problem and trust expiration problem.

- **CASE1. Trust Fraud**

The problem of trust fraud is a user obtain high trust value within fewer times high-quality behavior interaction, which a malicious user could cause more damage. The TDW based access control model adopt malicious BTRs update strategy described in section 5.3.1 to solve this problem. We obtain the simulation result on fraud user's trust as shown in figure 6-4, the actual simulation results are illustrated as figure C-1 and figure C-2 in Appendix C (due to the limitation of NetLogo, we can't put two simulation results at one plot in NetLogo).

The fraud user's trust in **S3** model is rapidly rising at the beginning (reach

peak value 0.84 at time 16); after the system detected malicious behavior, the decrease of trust value is small, as there no effective punishment method, and no awareness of the trust fraud problem.

The fraud user's trust in TDW model is slowly rising at the beginning (reach peak value 0.67 at time 36), and once the system detected a malicious behavior, the trust value is rapidly decreased, and with the accumulating malicious behaviors, the greater the punishment. After punishment, the trust value increase slower than before, cannot restore to the state before the punishment within a short-term. When the system detects malicious behavior to 4 times, the fraud users' trust value reached strong mistrust degree and be included in the list of denied access.

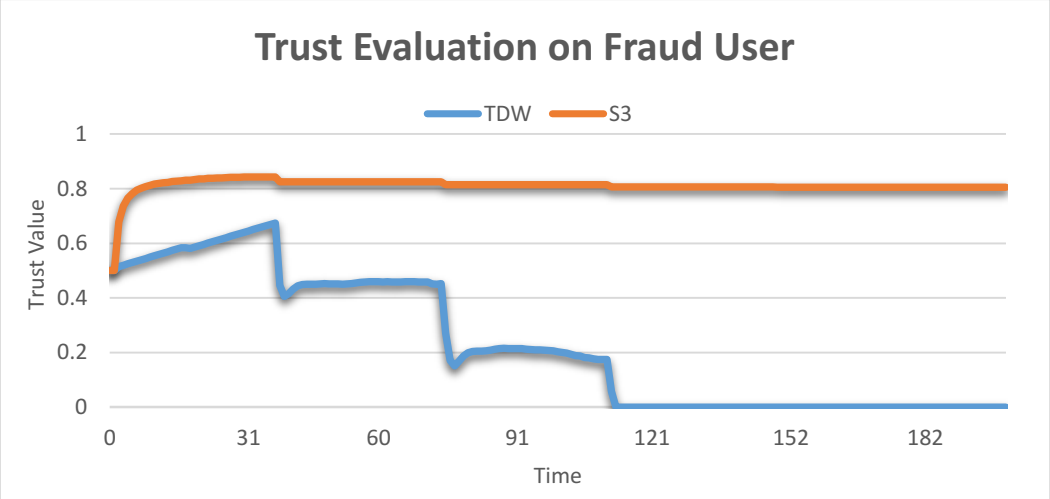


Figure 6-4 Trust Evaluation Comparison on Fraud User

From this comparison, we conclude the TDW is effective to solve the trust fraud problem; no only able to prevent fraud user obtain high trust value within a short-term high-quality interaction, but also have effective dynamic trust update strategy to against malicious behavior.

- **CASE2. Trust Expiration**

The system will increase uncertainty on the suspended user's trust value due to the trust expiration; normally, based on security consideration, the trust value of suspended user should tend to strange trust, the expired trust records should be deleted and no longer participate in the trust evaluation. If a system doesn't consider the trust expiration problem, the user identity lost and user behavior pattern change will bring huge risk to the system.

TDW based access control model adopts expired BTRs update strategy described in section 5.3.2 to solve this problem. We obtained the simulation result as illustrated in figure 6-5, the actual simulation plots are provided in Appendix C.

Both TDW model and S3 model fixed the trust value at time 30 while the intermittent users stop the interaction. TDW fixed the trust value as 0.65, and S3

fixed the trust value as 0.7.

The TDW model decreased the trust value from 0.65 to 0.55 when the intermittent user restart to accessing the system due to the expired BTRs were replaced with strange trust records. The S3 model continues to increase the trust value after the intermittent user restart to accessing the system.

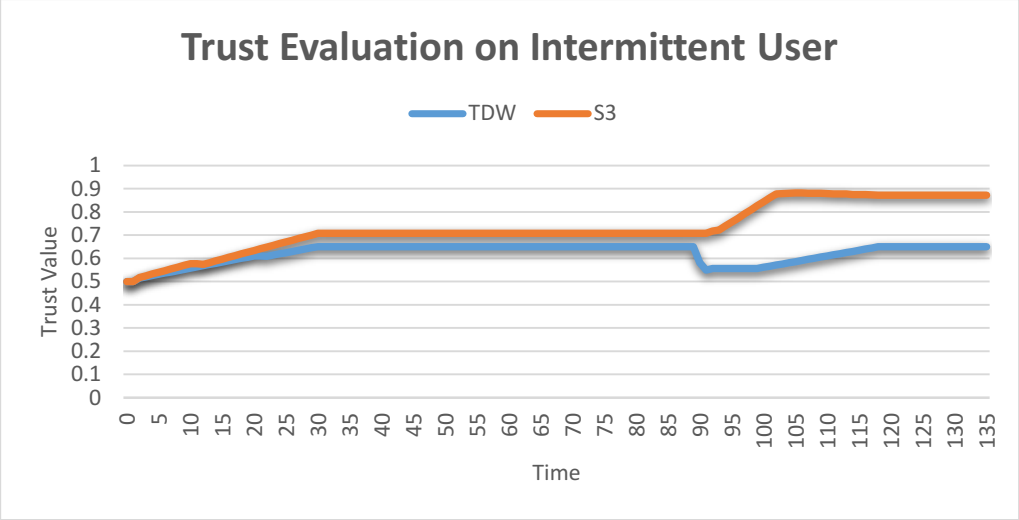


Figure 6-5 Trust Evaluation Comparison on Intermittent User

The simulation result indicates the expired BTRs replacement strategy accords with the attributes of trust expiration, stop access user's trust value has the tendency towards strange trust, reduced the risk arise due to the user identity lost and user behavior pattern change.

6.2.3 Discover the Unknown

We have proved the TDW based access control model is able to solve the trust fraud problem, and also has valid punishment strategy on malicious behavior; so, we wonder what will happen if a good user carries out a malicious behavior accidently as a misoperation.

- **CASE3. Misoperation**

To identify the trust evaluation performance of TDW in this case, we established a new type of user called misoperation user; the misoperation users will always carry out good behavior, but will carry out once malicious at a random time. The simulation result is illustrated as figure 6-6.

The trust value of misoperation user reach the peak point at time 60 with value 0.81, and at the same moment, the user carried out a malicious behavior, which leads to a trust value rapid decrease to 0.4; after the punishment, it took the user 120 tickets restored to the peak point, and then continue increase. The simulation result indicates the misoperation will lead to trust value rapid decrease, but after a long-term good behavior accumulation, the trust value will slowly recovering.

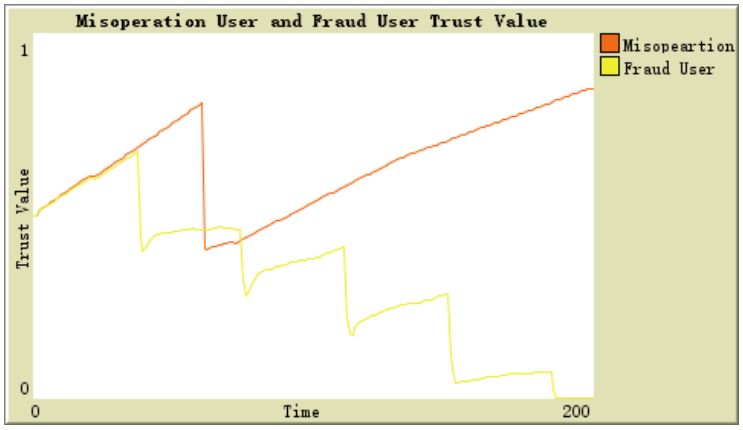


Figure 6-6 Trust Evaluation Performance on Misoperation User

We believe the punishment and recovery procedure is good to avoid the risk of malicious behavior; they are necessary to help distinguish the malicious user and misoperation user, is a conservative strategy to ensure the system security are not violated. However, from the user's perspective, accidental misoperation cannot be avoided, heavy punishment will affect the user's experience, and also affect the CSP's attractiveness to the beginner users.

Therefore, we conclude the TDW model should establish a user behavior distinguish strategy, utilized scientific computer science technology like machine learning method, to fine-grained distinguish malicious user and misoperation user through behavior pattern recognition; not only able to prevent malicious user from accessing, but also able to guarantee the smooth interaction of ordinary user's. This problem is considered as the study's limitation and future work.

CHAPTER 7. DISCUSSION

Information security is always a major challenge in computer network domain, researchers designed and established all kinds of security mechanisms, not matter internal or external, local or remote, software of hardware, personal or enterprise-level, universal or exclusive, to solving the endless network attacks, various and security vulnerabilities. Access Control Technology and Trust Mechanism are part of them.

Synthetic multiple mature technologies to facing new challenges is a technology trend. In this paper, in order to solve the CSUs trust problem and security problem of CC, utilized the combination of access control technology and trust mechanism. General access control mechanism based on user identity verification, which is not able to provide accurate authorization in open accessed CC; Trust mechanism is a theoretical model, which depends on practical technology to realize self-capability. Access control mechanism provides a mature authorization standard and working structure while the UBT theory provides a more accurate identity verification method based on user's actual interaction behavior. The combination of these two technologies meets the security and trust requirements of CC.

Based on the above research motivation, we conducted a systematical literature review in chapter 4 to identifying the key elements of trust-based access control model. The ***RQ1*** identified two type of working structures of trust-based access control model, obtained both fine-grained and coarse-grained access control strategy. We obtained the essential features and function modules while answering ***RQ1***, which is the knowledge foundation of our solution design. The ***RQ2*** classified the behavior evidence into three categories, and summarized the majority behavior evidence that can be collected by a CC system and valid for trust calculation. The ***RQ3*** identified the nature attributions of trust that can affect the evaluation accuracy, which provides us with valid path and tools to improve the current state-of-art UBT based access control model. The ***RQ4*** summarized the current study on the UBT based access control model, evaluated and compared their performance according to the standard we concluded in ***RQ1, RQ2, and RQ3***, and identified two major weaknesses of current UBT based access control model, trust fraud resistance and trust expiration problem; Based upon the research result of SLR, this paper designed a TDW based access control model aim to solve the weaknesses of current state-of-art UBT based access control model.

Unexpectedly, we found that it is very difficult to obtain real CSUs behavior evidence, neither from online database nor in practical ways; and even we obtained the actual datasets from a CC system, the calculation result will be meaningless if we don't consider the CC system security standards and requirements. Therefore, the study focuses on solving the impact of trust

attributes in comprehensive trust evaluation instead of guarantee the accuracy of UBT calculation in a unit time.

Meanwhile, we discovered that none of the current UBT based access control model has been adopted by any CSP, we believe the main problem is the complexity of behavior trust evaluation and the complexity of BTRs data structure. The above two discoveries changed the way we design the trust evaluation method and data structure in TDW based access control model; we abandoned the fine-grained Fuzzy ANP based UBT evaluation method, turn to a coarse-grained method as described in section 5.1.2 and section 5.4. And also simplified the data structure as three dynamic window structure.

After we completed the model design, a TDW based access control model prototype was established in NetLogo, three steps simulation procedure were conducted to verify the design validation, strength the knowledge we learned from this research and acquired the study limitation. The “slow rise, rapid decrease” principle is fulfilled the model design, and the simulation results verify the benefits of this principle.

The TDW model we designed could not satisfied both malicious user prevention and misoperation user smooth interaction, the recommendation for the future work is to adopt machine learning algorithm on the user behavior dataset to distinguish the behavior pattern of these two type of users, improve the division, and reduce the punishment on accidental misoperation user.

CHAPTER 8. VALIDITY THREATS

In this chapter, we summarized the validity threats to the research result. Three types of validity threats are identified and described in the following sections.

8.1 Internal Validity

The internal validity of this paper is to concern the relationship between collected studies and SLR results, simulation environment setting and simulation results [45].

The SLR results in this paper are affected by the study selection. In order to solve this problem, we identified the research keywords according to the PICOC criteria and clearly defined the study selection criteria based on the research questions.

The prototype performance is affected by the simulation environment and input data. The SLR result indicates that different studies using different simulation method to test the performance of their designed model; if we compare the performance of our prototype in a different simulation environment, the verification, and comparison results are invalid. In order to solve this problem, we developed our prototype in NetLogo with same environment setting as comparison object **S3**; the verification and comparison simulations are conducted on the same platform with same simulation environment and input data.

8.2 External Validity

The external validity of this paper is to concern if the simulation results can be generalized in other places by different researchers at different times [45].

In this research study, the prototype performance is affected by the input behavior of different types of users and the corresponding trust value of different behaviors. The input setting we adopted is following the recommendation of collected research studies **S3**, **S5**, and **S16**, which is a common way to carry out the UBT prototype performance simulation, and we clearly defined the input setting in the section 6.1.2 in order to reduce the chance of external validity.

8.3 Construct Validity

The construct validity of this paper is to concerns the relationship between the measurements of simulation and object [45].

In this research study, the users trust value and time tickets are two metric of prototype simulation, it is also used in **S3** and **S5** while they simulate their model in NetLogo. And this research paper clearly described the prototype environment setting and parameter setting, in order to reduce the chance of construct validity.

CHAPTER 9. CONCLUSION & FUTURE WORK

9.1 Conclusion

Towards the trust issues and security problems of CC, and the weaknesses of current state-of-art of UBT based access control technology, this research study designed and developed an improved UBT based Access Control Model; which according to the simulation result, compare to the current state-of-art UBT model, the TDW model has following advantages:

1. Effectively preventing trust fraud problem with "slow rise" principle.

2. Able to timely response to malicious behavior with constantly aggravate punishment strategy ("rapid decrease" principle), effectively prevent malicious behavior and malicious user.

3. Able to actual reflect the recent credibility of the accessing user by expired trust update strategy and most recent trust calculation.

4. It has simple and customizable data structure, simple trust evaluation method, which has good scalability.

In this paper, we have published the results from the research studies that were performed. Based on these results, we have been able to answer the following research questions:

RQ1: based upon the result of SLR, we identified two types of trust-based access control model working structure, authority based trust access control model, and role-based trust access control model; according to the different application scenarios and working pattern, classified as fine-grained and coarse-grained access control. Meanwhile, described the structure of dynamic trust and access update module.

RQ2: based upon the result of SLR, three types of user behavior evidence were identified, total 23 different behavior evidence items were identified and available to be collected by a CC system.

RQ3: according to the result of SLR, four trust attributes were identified and their impact on the trust evaluation accuracy were summarized; meanwhile, valid countermeasures were captured from the collected studies.

RQ4: according to the result of SLR, eight UBT based access control models were identified and evaluated as state-of-art, we explained the main features of each model, and identified the advantages and disadvantages of each model.

Based on the above knowledge we collected through SLR, we designed our own UBT based access control model called Triple Dynamic Window based Access Control Model. From the model design perspective, the TDW model provides a customizable data structure and lightweight trust evaluation methods.

RQ5: we established the prototype of TDW access control model on NetLogo platform according to the recommendation of **S3** and **S5**.

RQ6: according to the results of three steps simulation, the performance of TDW access control model was verified; the comparison result indicate the TDW access control model has better performance on the trust fraud problem and trust expiration problem than the model provided by study **S3**; the discover unknown procedure provided us a weakness of TDW access control model, which is not able to distinguish malicious user and misoperation user. In general, we verified the improvements and discovered the limitations.

9.2 Future Work

From the research that was performed and published in this paper, we have outlined a few pointers for future work that could be addressed by researchers. The following items are interesting for further research:

1. The TDW access control model is not able to well distinguish the malicious behavior and misoperation, in order to solve this limitation, we will adopt machine learning algorithm in the future to help distinguish the behavior pattern of malicious user and misoperation user, improve the recognition rate.
2. The prototype we built is in a simulated environment, and the behavior evidence is not collected from real CC system, is a practice in an ideal environment. To prove the practicability of our design, the further study needs to establish the TDW model in a real CC environment and develop a more fine-grained trust evaluation method according to the system security and service standard.
3. The TDW model provides a customizable data structure, but we are not sure which configuration is optimized in what kind of application scenario. As same as the future work 2, we will establish the TDW model in different types of CC systems and test with different scenarios, to acquire optimization configuration.

CHAPTER 10. REFERENCE

1. Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of-the-art and research challenges," Journal of internet services and applications, vol. 1, no. 1, pp. 7–18, 2010.
2. P. Mell and T. Grance, "The NIST definition of cloud computing," 2011.
3. J. Brodkin, "Gartner: Seven cloud-computing security risks," Infoworld, vol. 2008, pp. 1–3, 2008.
4. C. Cachin and M. Schunter, "A cloud you can trust," IEEE Spectrum, vol. 48, no. 12, pp. 28–51, Dec. 2011.
5. S. Pearson and A. Benameur, "Privacy, Security and Trust Issues Arising from Cloud Computing," in 2010 IEEE Second International Conference on Cloud Computing Technology and Science, 2010, pp. 693–702.
6. L. Tian, C. Lin, and Y. Ni, "Evaluation of user behavior trust in cloud computing," in Computer Application and System Modeling (ICCASM), 2010 International Conference on, 2010, vol. 7, pp. V7–567.
7. A. J. Choudhury, P. Kumar, M. Sain, H. Lim, and H. Jae-Lee, "A Strong User Authentication Framework for Cloud Computing," in Services Computing Conference (APSCC), 2011 IEEE Asia-Pacific, 2011, pp. 110–115.
8. S. A. Almulla and C. Y. Yeun, "Cloud computing security management," in Engineering Systems Management and Its Applications (ICESMA), 2010 Second International Conference on, 2010, pp. 1–7.
9. M. Blaze, J. Feigenbaum, J. Ioannidis, and A. D. Keromytis, "The role of trust management in distributed systems security," in Secure Internet Programming, Springer, 1999, pp. 185–210.
10. R. A. R. Shaikh and M. Sasikumar, "Trust model for a cloud computing application and service," in 2012 IEEE International Conference on Computational Intelligence Computing Research (ICCIC), 2012, pp. 1–4.
11. L.Q. Tian and C. Lin, "A kind of game-theoretic control mechanism of user behavior trust based on prediction in trustworthy network," Computer Science Journal, vol. 30, no. 11, pp. 1930–1938, 2007.
12. Y.R. Chen, L.Q. Tian, and Y. Yang, "Model and analysis of user behavior based on dynamic game theory in cloud computing," Electronica Journal, vol. 39, no. 8, pp. 1818–1823, 2011.
13. Y.X. Lv, L.Q. Tian, and S. Sun, "FANP based user behavior trust evaluation and control analysis in Cloud Computing environment," Computer Science Journal, vol. 40, no. 1, pp. 132–135, 2013.
14. W. Li, L. Ping, and X. Pan, "Use trust management module to achieve effective security mechanisms in cloud environment," in Electronics and Information Engineering (ICEIE), 2010 International Conference On, 2010, vol. 1, pp. V1–14–V1–19.
15. X. Sun, G. Chang, and F. Li, "A Trust Management Model to Enhance Security of Cloud Computing Environments," in 2011 Second International

Conference on Networking and Distributed Computing (ICNDC), 2011, pp. 244–248.
16. P. Mell and T. Grance, “The NIST definition of cloud computing,” 2011.
17. A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, “Above the clouds: A Berkeley view of cloud computing,” Dept. Electrical Eng. and Comput. Sciences, University of California, Berkeley, Rep. UCB/EECS, vol. 28, no. 13, p. 2009, 2009.
18. S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving secure, scalable, and fine-grained data access control in cloud computing,” in Infocom, 2010 proceedings IEEE, 2010, pp. 1–9.
19. R. S. Sandhu and P. Samarati, “Access control: principle and practice,” Communications Magazine, IEEE, vol. 32, no. 9, pp. 40–48, 1994.
20. B. Thuraisingham, “Mandatory access control,” in Encyclopedia of Database Systems, Springer, 2009, pp. 1684–1685.
21. N. Li, “Discretionary access control,” in Encyclopedia of Cryptography and Security, Springer, 2011, pp. 353–356.
22. R. Sandhu, E. Coyne, H. Feinstein. Role-based Access Control Models [J]. IEEE Computer, 1996, 29(2): 38-47
23. Chen Jincui, Jiang Liqun. Role-Based Access Control Model of Cloud Computing [J]. Energy Procedia, 2011, 13: 1056 – 1061.
24. Z. Tang, J. Wei, A. Sallam, K. Li, and R. Li, “A new RBAC based access control model for cloud computing,” in Advances in Grid and Pervasive Computing, Springer, 2012, pp. 279–288.
25. Tan Z, Tang Z, Li R, et al. Research on Trust-based Access Control Model in Cloud Computing[C]. Information Technology and Artificial Intelligence Conference (ITAIC), 2011 6th IEEE Joint International. IEEE, 2011, 2: 339-344.
26. Wenhui Wang, Jing Han, Meina Song, et al. The Design of a Trust and Role Based Access Control Model in Cloud Computing[C]. Information Technology and Artificial Intelligence Conference (ITAIC), 2011 6th International Conference on. IEEE, 2011: 330-334.
27. J. P. Anderson, “Computer Security Technology Planning Study. Volume 2,” DTIC Document, 1972.
28. Marsh S. “Formalizing Trust as a Computational Concept” [D].Scotland, UK: 1994.
29. M. Blaze, J. Ioannidis, and A. D. Keromytis, “Experience with the keynote trust management system: Applications and future directions,” in Trust Management, Springer, pp. 284–300, 2003.
30. A. Abdul-Rahman and S. Hailes, “A distributed trust model,” in Proceedings of the 1997 workshop on New security paradigms, pp. 48–60, 1998.
31. G. Xiaolin, X. Bing, L. Yinan, and Q. Depei, “Study on the behavior-based trust model in grid security system,” in 2004 IEEE International Conference on Services Computing, 2004. (SCC 2004). Proceedings, pp. 506–509, 2004.
32. X. Sun, G. Chang, and F. Li, “A Trust Management Model to Enhance Security of Cloud Computing Environments,” in 2011 Second International

Conference on Networking and Distributed Computing (ICNDC), pp. 244–248, 2011.
33. X. Wang, “A study of P2P access control strategy based on trust and security grade,” in 2011 International Conference on Computer Science and Service System (CSSS), pp. 126–128, 2011.
34. S. Ries, J. Kangasharju, and M. Mühl, “A classification of trust systems,” in On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, 2006, pp. 894–903.
35. B. Lee, “Unified Public Key Infrastructure Supporting Both Certificate-Based and ID-Based Cryptography,” in ARES ’10 International Conference on Availability, Reliability, and Security, pp. 54–61, 2010.
36. Creswell, J.W., 2009. The Selection of a Research Design. In Research Design Qualitative, Quantitative, and Mixed Methods Approaches. California: SAGE, pp. 16–18.
37. B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, “Systematic literature reviews in software engineering–a systematic literature review,” Information and software technology, vol. 51, no. 1, pp. 7–15, 2009.
38. “Prototype,” Wikipedia, the free encyclopedia. 24-Apr-2016.
39. Petticrew, Mark and Helen Roberts. Systematic Reviews in the Social Sciences: A Practical Guide, Blackwell Publishing, 2005, ISBN 1405121106
40. L. Viljanen, “Towards an Ontology of Trust,” in Trust, Privacy, and Security in Digital Business, S. Katsikas, J. López, and G. Pernul, Eds. Springer Berlin Heidelberg, pp. 175–184, 2005.
41. T. L. Saaty, “How to make a decision: the analytic hierarchy process,” European journal of operational research, vol. 48, no. 1, pp. 9–26, 1990.
42. A. P. Dempster, “Upper and lower probabilities induced by a multivalued mapping,” The annals of mathematical statistics, pp. 325–339, 1967.
43. L. Tian, C. Lin, and Y. Ni, “Evaluation of user behavior trust in cloud computing,” in Computer Application and System Modeling (ICCASM), 2010 International Conference on, 2010, vol. 7, pp. V7–567.
44. S. Tisue and U. Wilensky, “NetLogo: A simple environment for modeling complexity,” in International conference on complex systems, 2004, vol. 21.
45. M. B. Brewer, H. Reis, and C. Judd, “Research design and issues of validity,” Handbook of research methods in social and personality psychology, pp. 3–16, 2000.

Appendix A – Selected Studies

S1. W. Deng and Z. Zhou, "A Flexible RBAC Model Based on Trust in Open System," in Intelligent Systems (GCIS), 2012 Third Global Congress on, 2012, pp. 400–404.

S2. A. Mohsenzadeh, H. Motameni, and M. J. Er, "A New Trust Evaluation Algorithm between Cloud Entities Based on Fuzzy Mathematics," International Journal of Fuzzy Systems, pp. 1–14, 2015.

S3. X. Wu, R. Zhang, B. Zeng, and S. Zhou, "A trust evaluation model for cloud computing," Procedia Computer Science, vol. 17, pp. 1170–1177, 2013.

S4. H. Lin, L. Xu, X. Huang, W. Wu, and Y. Huang, "A trustworthy access control model for mobile cloud computing based on reputation and mechanism design," Ad Hoc Networks, vol. 35, pp. 51–64, 2015.

S5. R. K. Banyal, V. K. Jain, and P. Jain, "Dynamic Trust Based Access Control Framework for Securing Multi-Cloud Environment," in Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies, 2014, pp. 29.

S6. G. Lin, D. Wang, Y. Bie, and M. Lei, "MTBAC: A mutual trust based access control model in cloud computing," Communications, China, vol. 11, no. 4, pp. 154–162, 2014.

S7. Z. Tan, Z. Tang, R. Li, A. Sallam, and L. Yang, "Research on trust-based access control model in cloud computing," in Information Technology and Artificial Intelligence Conference (ITAIC), 2011 6th IEEE Joint International, 2011, vol. 2, pp. 339–344.

S8. J. Ma and Y. Zhang, "Research on Trusted Evaluation Method of User Behavior Based on AHP Algorithm," in 2015 7th International Conference on Information Technology in Medicine and Education (ITME), 2015, pp. 588–592.

S9. W. Wang, J. Han, M. Song, and X. Wang, "The design of a trust and role based access control model in cloud computing," in Pervasive Computing and Applications (ICPCA), 2011 6th International Conference on, 2011, pp. 330–334.

S10. R. Bose, X. R. Luo, and Y. Liu, "The roles of security and trust: Comparing cloud computing and banking," Procedia-Social and Behavioral Sciences, vol. 73, pp. 30–34, 2013.

S11. R. Yang, C. Lin, Y. Jiang, and X. Chu, "Trust based access control in infrastructure-centric environment," in Communications (ICC), 2011 IEEE International Conference on, 2011, pp. 1–5.

S12. J. Huang and D. M. Nicol, "Trust mechanisms for cloud computing," Journal of Cloud Computing, vol. 2, no. 1, pp. 1–14, 2013.

S13. F. Yue-Qin and Z. Yong-Sheng, "Trusted Access Control Model Based on Role

and Task in Cloud Computing," in 2015 7th International Conference on Information Technology in Medicine and Education (ITME), 2015, pp. 710–713.

S14. L. Jun-Jian and T. Li-Qin, "User's Behavior Trust Evaluate Algorithm Based on Cloud Model," in Instrumentation and Measurement, Computer, Communication and Control (IMCCC), 2015 Fifth International Conference on, 2015, pp. 556–561.

S15. N. Yang, T. Liqin, S. Xueli, and G. Shukai, "Behavior trust evaluation for node in WSNs with Fuzzy-ANP method," in Computer Engineering and Technology (ICCET), 2010 2nd International Conference on, 2010, vol. 1, pp. V1–299.

S16. L. Tian, C. Lin, and Y. Ni, "Evaluation of user behavior trust in cloud computing," in Computer Application and System Modeling (ICCASM), 2010 International Conference on, 2010, vol. 7, pp. V7–567.

Appendix B – Primary Data Synthesis

Table B-1 Primary Data Synthesis Overview

S.ID	Source	PY	TE	TA	WS	EM	Method Name	EE
S1	IEEE	2012	●	-	●	●	FRBAC	SL
S2	Springer	2015	-	-	-	●	Fuzzy Mathematics	SL
S3	ScienceDirect	2013	-	●	-	●	DS Evidence	SL
S4	ScienceDirect	2015	-	-	●	-	-	SL
S5	ACM	2014	●	-	●	●	DTBAC	SL
S6	IEEE	2014	●	●	●	●	MTBAC	SL
S7	IEEE	2011	-	-	●	●	GTRBAC	-
S8	IEEE	2015	●	●	-	-	AHP	SL
S9	IEEE	2011	-	-	●	-	-	-
S10	ScienceDirect	2013	-	●	-	-	-	-
S11	IEEE	2011	-	-	●	●	ICTRBAC	SL
S12	Springer	2013	●	●	-	-	-	-
S13	IEEE	2015	-	-	●	-	RTBTAC	SL
S14	IEEE	2015	●	-	-	●	Entropy AHP	RC
S15	IEEE	2010	●	●	-	-	-	-
S16	IEEE	2010	●	●	-	-	-	-
Total			8	7	8	8		

S.ID: Selected Reference ID (accordance with the ID in Appendix A).

PY: Published Year **TE:** Trust Evidence

TA: Trust Attributes **WS:** Working Structure

EM: Evaluation Method **EE:** Experiment Environment

SL: Simulated Environment **RC:** Real CC Environment

●: YES, mentioned in the paper - : NO, not mentioned in the paper

Appendix C – Simulation Result

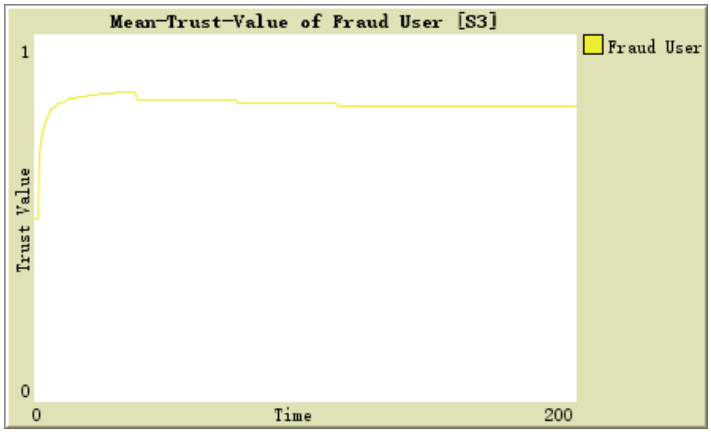


Figure C-1 Fraud User Trust Value Simulation on Study S3 Provided Model

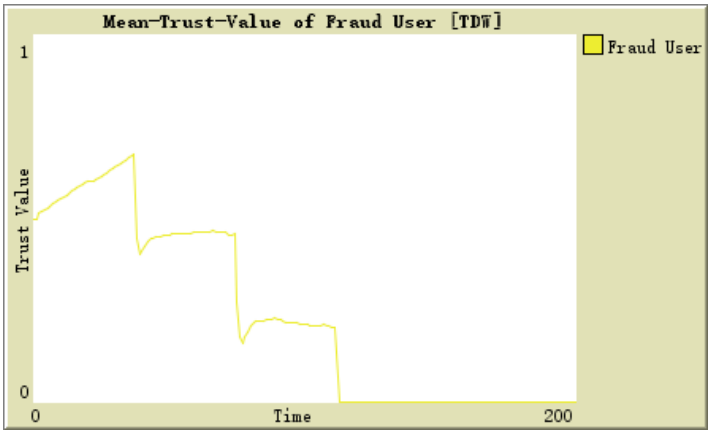


Figure C-2 Fraud User Trust Value Simulation on TDW Model

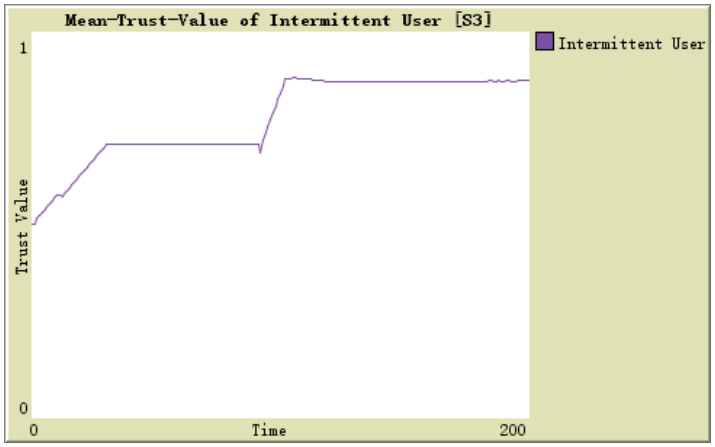


Figure C-3 Intermittent User Trust Value Simulation on Study S3 Provided Model

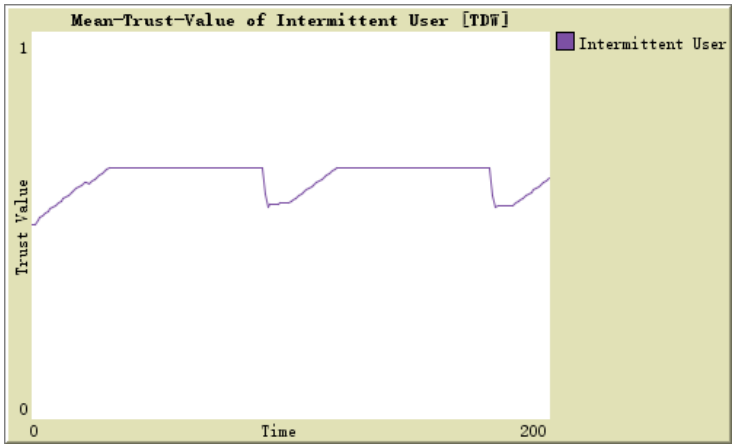


Figure C-4 Intermittent User Trust Value Simulation Result on TDW model

Figure C-5 Comprehensive User Trust Value Simulation Result on TDW model