Testing a Trust Management System for Cloud Computing Using Simulation

Norah Farooqi
Umm Al-Qura University
Makkah, Saudi Arabia

Abstract

Cloud computing is a central topic in computing systems due to its importance in daily life. Although it has been developed to provide services to consumers for storing and manipulating data quickly at low cost, it still suffers from various problems from a security perspective. Security concerns in the cloud environment still require further investigation and development. This paper presents a dynamic security management system for cloud computing based on electronic trust. The system studies and evaluates the relations in two directions between end users, the data owner, and the provider, and it manages data security by updating trust values for access permissions and authentication purposes. Developing the proposed system can evaluate trust relations between entities, show flexibility in its calculations and provide dynamic access control while monitoring the entities' interactions over time. The simulation experiments show the efficiency of this proposed approach.

1. Introduction

Cloud computing is an active research area due to the recent improvements in its usability. Huge volumes of data can be stored and transferred via cloud environment that needs to be managed in a secure manner. Thus, security issues are one of the major topics in cloud management that requires more investigation. Hundreds of studies have proposed different models in order to improve security issues in cloud platform. However, gaps remain which need to be developed further. Developing an applicable access control system can be considered to be one of the main approaches guaranteeing data security in cloud computing.

The research paper proposes a data security management system in cloud computing, to provide a secure environment for managing all data and especially sensitive information. The system is designed as a monitoring system to control the access to data and evaluate the relations among three main entities in cloud; it depends on trust value. These entities are the end user, system provider, and data owner. The system studies the relations among these participants to improve trust value and provide a secure platform. The proposed system is based on trust based access control to manage privileges in cloud network. It illustrates the flexibility of trust values and how they will be affected in these relations by different factors. The future results will explain how the proposed system will be designed to improve security in cloud environment from the perspectives of functionality and performance.

The remainder of this paper is structured as follows. Section 2 discusses the related work for this topic. Section 3 points out the main contributions for the proposed system that is explained in section 4. Section 5 discusses the system's testing through running some simulation experiments. Section 6 forms the conclusion.

2. Related Work

Cloud computing is currently considered as one of the most important technologies for internet computing due to its services and features that include scalability, functionality, and low cost [1-4]. It provides a powerful environment for data storage and access processing, to meet the needs of consumers [2, 18, 19, 20]. Data and information are the central keys in the cloud; thus, this technology should concentrate on how to deal with these features in a secure and protective manner [5, 6, 20].

The security topic is the main issue in cloud management that requires further investigation and development [2, 5, 6, 7, 18, 19, 20]. Many areas can be considered to improve security in cloud computing including authentication, confidentiality, and integrity. As a result, managing data security in the cloud is critical and essential [2, 7]. The task suffers from several concerns: privileges, data segregation, and recovery [2 , 19, 20].

In order to improve security in any computing system, access control can be applied as a major tool to protect data from misuse and to prevent unauthorised access to data [1, 8, 20]. The access control system can capture threats from both insiders and outsiders [1]. Different systems have been developed to enhance access control in cloud security using traditional methods or new models [1, 8, 18, 20]. The traditional access control types suffer

from limitations, and they are static [1, 18, 20]. To match the cloud computing features that are dynamic, the most reasonable access control types need to be dynamic and responsive. Thus, many proposed systems have employed trust-based access control with different developments to fit in with the cloud environment [1, 8, 18, 20].

Trust-based access control has been applied in different security fields of networks and databases to control system permissions and provide a dynamic secure environment for users [9-13]. It depends mainly on monitoring users' behaviours, histories, accomplishments, and interactions over a period of time to calculate trust values and update permissions [13-16]. Trust-based access control includes trust management models that are responsible for calculating processes and updating users' privileges [9, 10, 14, 15].

Trust relations between entities can be measured internally by direct methods or externally by indirect methods. The direct methods include monitoring the direct operations between entities and studying their histories. The indirect methods usually depend on third-party or external factors that affect the calculations, such as recommendations [9, 13, 17]. In general, direct methods are more reliable than indirect methods to evaluate users' operations and behaviours [9, 10, 17].

The trust based access control model is known for its flexibility in defining factors and calculation processes. Each system can select affected factors according to organisational needs and design the trust access model's structure based on organisational policies. Trust-based access control models can calculate trust values, based on different techniques using mathematical approaches [13, 14, 17].

Some proposed models have applied numerous different access control models with different techniques to provide secure environments in cloud computing [1, 8, 18, 20]. Tan et al. (2011) [8] applied trust-based access control to cloud platform, using both direct and indirect trust by considering different factors. Lin et al. (2013) [1] proposed a trust-based policy for access control in multi-domain cloud network. The proposed system categorises the access control, through local domain and cross-domain. The majority of the proposed systems that have applied trust-based access control in cloud computing, have studied the trust relationships between users and resources without considering the role of the data owner, the system provider, and the whole platform.

The system will study the trust relationship by considering three entities: end users, data owner, and system providers. It then evaluates the trust relationship in two directions in order to find the trust value, which it will then use to update permissions. In addition, the proposal will apply trust-based access control in some directions between entities to manage the access processes for resources. The proposed system is a dynamic data management system to improve security in cloud environment.

3. Contributions

Considering issues and limitations in existing security management in cloud computing, this paper aims to:

1. Evaluate the relationships between entities in a cloud environment and measure the trust values among them.
2. Design the proposed data management system using trust-based access control to improve the security environment in cloud computing.
3. Provide a secure and dynamic data management system for the cloud.

4. The System Relations

In this section, relations between entities are evaluated individually and then the proposed data security management system is described. The system studies relations between actors in cloud management who are the system provider, data owner and end user. The system evaluates different factors in these relations to calculate an appropriate trust value. Figure1 explains relations in two directions between entities.

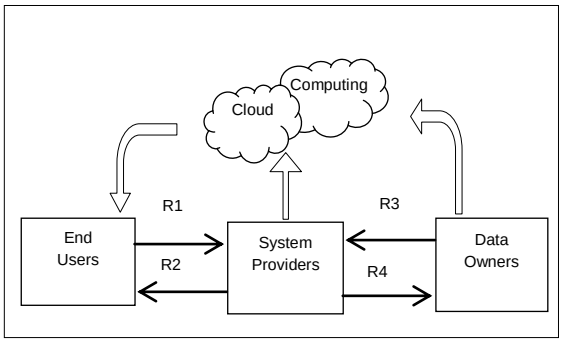

Figure 1. Entities' relations in cloud computing.

In general, there are four relations that require investigation and evaluation considering different factors in order to generate trust values.

4.1. Relation between end users and system providers (R1)

The relation (R1) shows to what extent the end user can trust the system provider to use its services. Technology Acceptance Model (TAM 3) can be used to evaluate this relationship plus adding other factors like: social factors, cultural factors and feedback from other users about the services. These factors

can be used to evaluate the trust relation between end user and system provider. When users trust the system providers, they start using their services. Since, this relationship is dynamic; it will be always be evaluated over actions and time. The generated trust value for R1 will be calculated continuously. R1 is less important than the relation in the second direction.

4.2. Relation between system providers and end users (R2)

The relation (R2) reflects to what extent the system provider trusts users to give them the access privileges to data. To evaluate this relation, Trust Based Access Control system (TBAC) is applied. TBAC evaluates the end users' interaction continuously by detecting bad transactions and errors. The calculated trust value is updated over time and is used to manage the end users' privileges.

4.3. Relation between data owner and system provider (R3)

The relation (R3) explains to what extent the data owner can trust the system provider to use their services and store data on it. R3 is affected by system provider history and advertisements in the market. Technology Acceptance Model (TAM 3) can also be used to evaluate R3 by adding other factors. The evaluation for trust factor can depend on list of big customers who work with the system provider company and feedback from other data owners about the system provider's services.

4.4. Relation between system provider and data owner (R4)

R4 is a relation which considers the trust value between system providers and data owners to allow them use their services. The relation R4 requires Trust Based Access Control system (TBAC). The applied access control evaluates the data owner's interaction continuously and checks the data types which are used. Also, the system provider can benefit from the end user's feedback to evaluate data owner activities. The trust value is updated over time according to the data owner's behaviours. In the cloud computing environment, sometimes the data owner can be the end user depending on the services.

5. The System Architecture

After understanding the relations between entities that affect security aspects in cloud platform, the proposed system structure and its contents are explained in Figure 2. The system consists of three modules: evaluation module, calculation module and management module.

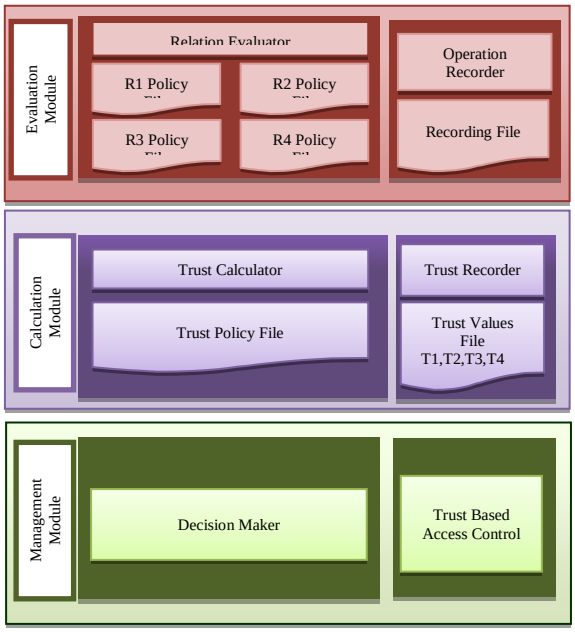

Figure 2. The system's architecture.

5.1. Evaluation Module

The evaluation module is constructed of two main parts that work simultaneously to evaluate the relations between entities. These parts are the relation evaluator and operations recorder. The relation evaluator works in light of the R1 policy file, R2 policy file, R3 policy file and R4 policy file. Each file of these policy files has the related rules of evaluating trust and selects certain factors that affect the specific relation. The relation evaluator evaluates each relation between entities over time according to its related policy file. The operation recorder records the actions and behaviours of related entities in a recording file depending on specific defined rules in the relation evaluator. The recording file is kind of log files that used for a certain security aspect.

5.2. Calculation Module

The second module in the proposed system is calculation module that consists of a trust calculator and trust recorder. The trust calculator uses data recorded by evaluation module to calculate trust values for relations between entities. The trust calculator depends on the rules and equations which are defined in the trust policy file. The file contains the calculation equations for all relations R1, R2, R3 and R4. It also defines the weights for related factors in each equation according to the importance of that factor. The importance of a factor reflects how much this specific factor affects the final trust value. The main goal of this trust calculator is calculating trust

values for each relation between entities. The trust recorder records the generated trust values in a trust value file. The trust value file thus contains all trust values for entities dealing with the system. Each relation has trust values such as T1, T2, T3 and T4.

5.3. Management Module

Management module includes decision maker and trust based access control. Both these parts work to improve security in the cloud. The decision maker handles trust values and then either permits or denies this relation between entities. It deals with trust values in multiple ranges. Trust Based Access Control works on relation classified, as R2 or R4. TBAC manages the access to data depending on the trust value that is updated over time

6. Experimental Testing

The proposed system was tested using a simulation environment. NetLogo simulator was used to run experiments because there is no standard simulator for the cloud environment, which NetLogo is a multi-agent simulator that is used to model and simulate different systems. The variety in agents' type in Netlogo leads to effective simulations for dynamic systems, and it includes four main types of agents: turtles, patches, links, and observers.

The evaluation process for the system were run in two levels. The first level includes simulations for each relation in the developed system. There were four experiments: R1 simulation experiment, R2 simulation experiment, R3 simulation experiment and R4 simulation experiment. Then, the second level of evaluation process focusses on system's functionality and simulated entire system experiment.

The trust values for all relations were calculated per different rules. All trust values were generated between 0 and 1, while 0 reflects no trust in the relation, and 1 shows that the trust reaches the maximum level in the relation. The rule of creating or denying all relations was as follows:

If Trust Relation (TR) > 0.5, then R is created
Else, R is denied

This rule can be modified depending on the applied security level in the system. Each experiment is discussed in following sections.

6.1. R1 Simulation Experiment

This experiment simulates the R1 in the proposed system. As described before in section 4, R1 is a relation that reflects the trust value from the end user to the system provider. The calculation of trust can depend on many factors. This evaluation used feedback from users as the main factor to calculate trust and then make decisions.

The parameters in R1 simulation dashboard were four users with random feedbacks. TR1 is the average of other users' trust values. Table 1 presents some readings of random trust values and the calculated TR1. Figure 3 shows case study one when the R1 is created from end user to system provider and case study two when R1 is denied per the decision maker because the trust value was less than the required level.

Table 1. Case studies for TR1

Users' Feedback				End User	
User 1	User 2	User 3	User 4	TR1	R1
0.8	1.0	0.9	0.7	0.85	Created
0.6	0.5	0.1	0.2	0.35	Denied

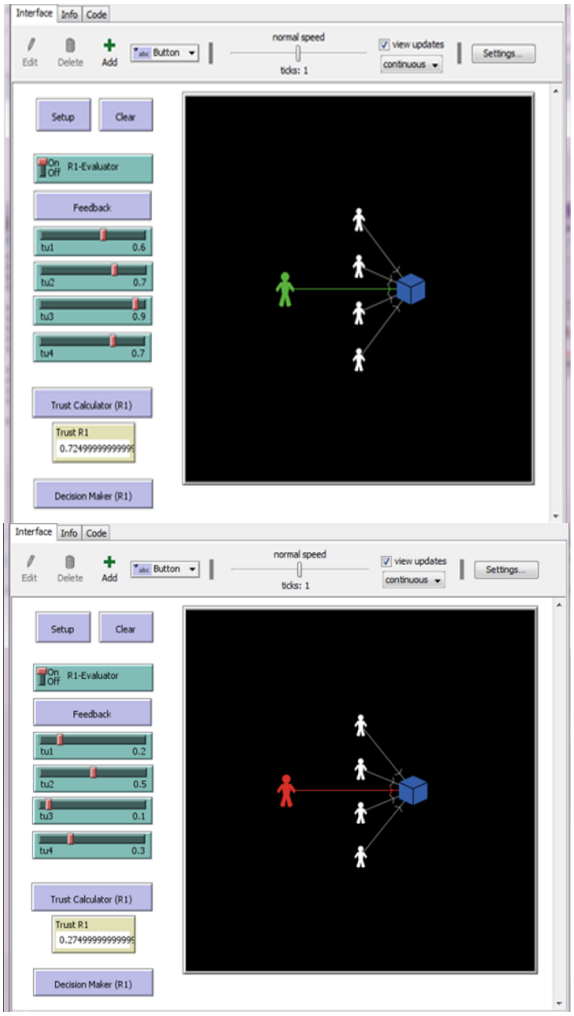

Figure 3. Case studies of R1 from the end user to the system provider

6.2. R2 Simulation Experiment

In this second experiment, the trust relation from the system provider to the end user was simulated and tested. Additionally, the evaluation of R2 applied access control techniques that recorded bad transactions over time, and calculated trust values per the bad transaction variable. The rules used were as follows:

If Bad Transaction (BT) < 5, then Trust Relation (TR2) =1

Else, If Bad Transaction (BT) < 10, then Trust Relation (TR2) =0.75

Else, If Bad Transaction (BT) < 15, then Trust Relation (TR2) =0.5

Else, If Bad Transaction (BT) < 20, then Trust Relation (TR2) =0.25

Else, Trust Relation (TR2) =0

These rules can easily be changed per system requirements. The parameters in R2 simulation dashboard were four users with different numbers of bad transactions in the system. Table 2 presents some readings of random values of bad transactions and the calculated TR2. Figure 4 shows the case studies of R2 from the system provider to the end user.

Table 2. Case studies for TR2

#	Bad Transactions	System provider	
		TR2	R2
User 1	4	1	Created
User 2	8	0.75	Created
User 3	14	0.5	Denied
User 4	23	0	Denied

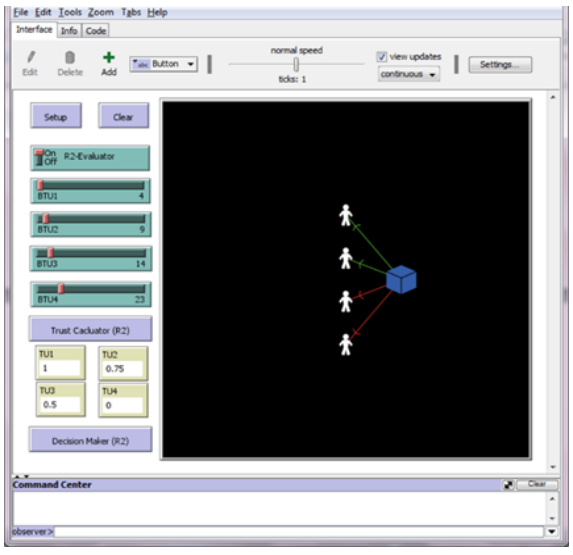

Figure 4. Case studies of R2 from the system provider to the end user

6.3. R3 Simulation Experiment

The third experiment simulated the relation from the data owner to the system provider. Various factors can be used to calculate trust for R3. In this experiment, feedbacks from other data owners were used as the basic factors in the calculation.

Parameters in the R3 simulation dashboard were four data owners with random values of feedbacks. TR3 was calculated as the average value of all feedbacks, and Table 3 illustrates some readings of random trust values and the calculated TR3. The case study when the decision maker created R3 from data owner to system provider and the case study when the data owner trusts system provider less than requirement level are shown in Figure 5.

Table 3. Case studies for TR3

Data Owners' Feedback				System Provider	
Data Owner 1	Data Owner 2	Data Owner 3	Data Owner 4	TR3	R3
0.7	0.9	1.0	0.5	0.775	Created
0.5	0	0.6	0.7	0.45	Denied

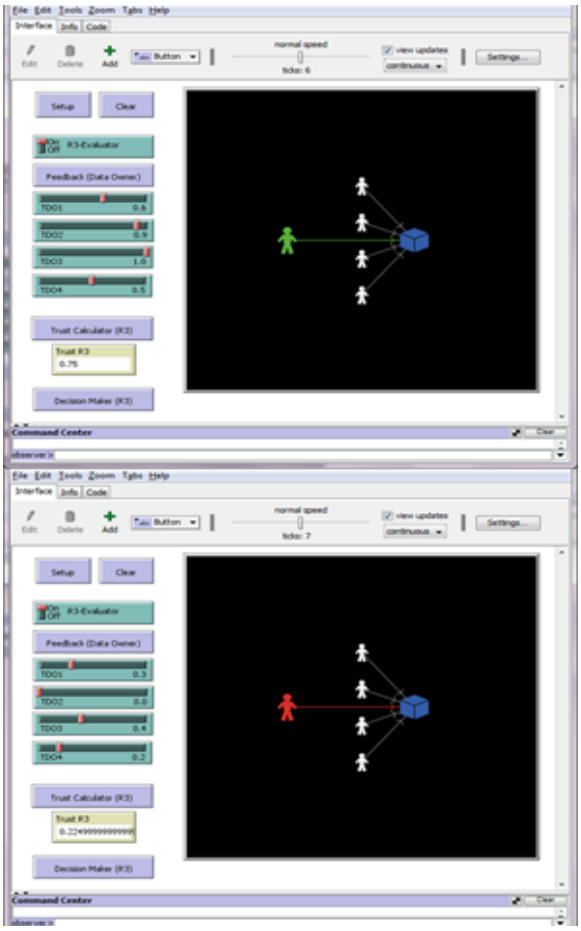

Figure 5. Case studies of R3 from the data owner to the system provider

6.4. R4 Simulation Experiment

The final experiment to test relations in the system simulated R4 that reflects to what extent the system provider trusts the data owners to allow them to use the cloud services and handle data sources. The access control in R4 depends on recording bad transactions for each data owner and automatically updates trust for R4. The rules used to evaluate bad transactions in the system were as follows:

If Bad Transaction (BT) < 5, then Trust Relation (TR4) =1
Else, If Bad Transaction (BT) < 10, then Trust Relation (TR4) =0.75
Else, If Bad Transaction (BT) < 15, then Trust Relation (TR4) =0.5
Else, If Bad Transaction (BT) < 20, then Trust Relation (TR4) =0.25
Else, Trust Relation (TR4) =0

The access control can be extended to relate with other factors that can be used easily in calculations. Table 4 includes some case studies for four data owners with different behaviours in the system and the generated TR4. Figure 6 describes the trust in R4.

Table 4. Case studies for TR4

#	Bad Transactions	System provider	
		TR4	R4
Data Owner 1	10	0.5	Denied
Data Owner 2	6	0.75	Created
Data Owner 3	14	0.5	Denied
Data Owner 4	3	1	Created

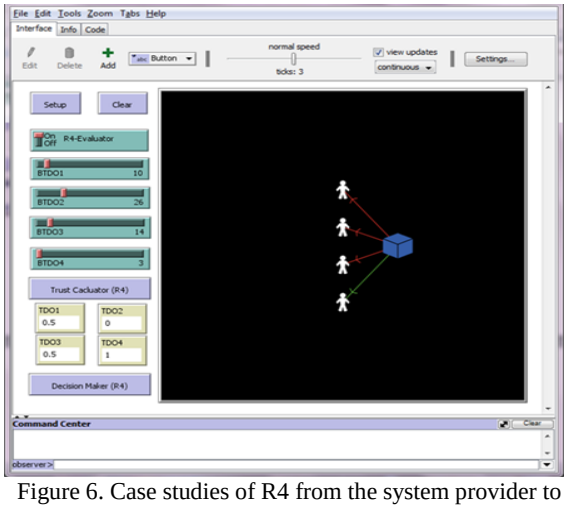

Figure 6. Case studies of R4 from the system provider to the data owner

6.5. Simulation entire system experiment

This simulated experiment tests the entire system and evaluates all the relations. The simulation system includes three main modules: evaluation module, calculation module, and management module. The three modules were integrated and the four relations were represented to run the whole system. Figure 7 shows the simulation of the entire system and presents the world view for the proposed system in Netlogo.

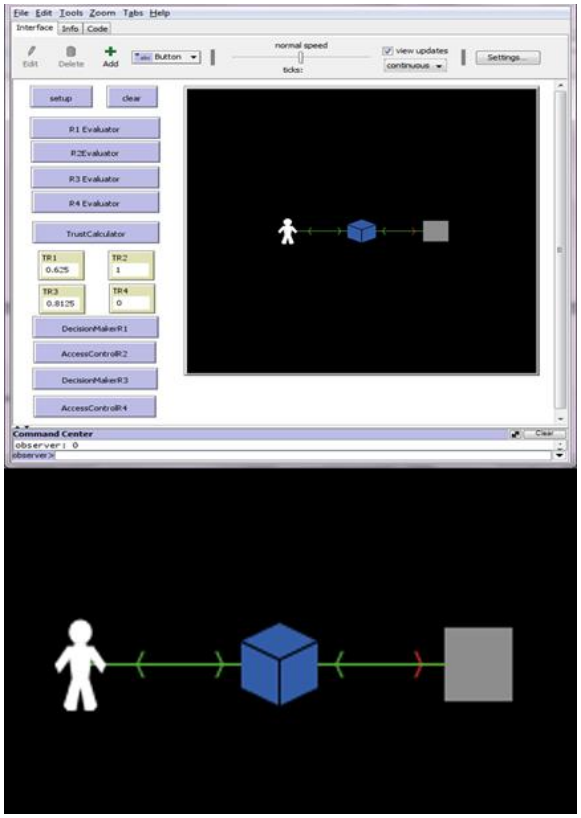

Figure 7. Simulation dashboard for the entire system

7. Conclusion

The paper highlights main issues in security management in the cloud, and presents valuable case studies to improve security management in cloud computing. Additionally, the paper proposes and designs a dynamic secured data management system to evaluate trust relations in the cloud and improve the security level. The system monitors the interactions and behaviours between entities over time, which are dependent on defined rules, to calculate related trust values and make decisions on access permissions to make the system dynamic, responsive and productive.

The proposed system was applied to test what extent the designed system meets the requirements and objectives while ensuring validity. The

experimental results for simulating systems can lead to improvements in data security and information systems in cloud management. The designed system may affect, directly and indirectly, the ways in which people can handle data in the cloud and may enhance the features for their options in cloud computing.

8. References

[1] G. Lin, Y. Bie and M. Lei, "Trust Based Access Control Policy in Multi-domain of Cloud Computing", *Journal of Computers*, vol. 8(5), 2013, pp. 1357-1365.

[2] S. Ramgovind , M. Eloff and E. Smith, "The Management of Security in Cloud Computing", *Information Security for South Africa (ISSA)*, 2010, pp. 1-7.

[3] F. Sabahi, "Virtualization-Level Security in Cloud Computing", *IEEE 3rd International Conference on Communication Software and Networks (ICCSN)*, 2011, pp. 250-254.

[4] Y. Younis, M. Merabti and K. Kifayat, "Secure Cloud Computing for Critical Infrastructure: A Survey", *Tech.Rep*., Liverpool John Moores University, Liverpool, UK, 2013.

[5] M. Ahmed, Y. Xiang and S.Ali, "Above the Trust and Security in Cloud Computing: A Notion towards Innovation", *IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, 2010, pp. 723-730.

[6] D. Meng, "Data Security in Cloud Computing", *The 8th International Conference on Computer Science and Education (ICCSE)*, 2013, pp. 810-813.

[7] J. Wang, C. Liu and G. Lin, "How to Manage Information Security in Cloud Computing", *IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 2011, pp.1405-1410.

[8] Z. Tan, Z. Tang, R. Li, A. Sallam and L. Yang, "Research on Trust-Based Access Control Model in Cloud Computing", *6th IEEE Joint International Information Technology and Artificial Intelligence Conference (ITAIC)*, 2011, pp. 339-344.

[9] J. Ma, L. Logrippo, K. Adi and S. Mankovski, "Risk Analysis in Access Control Systems Based on Trust Theories", *IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology (WI-IAT)*, 2010, pp. 415-418.

[10] F. Xing, L. Cui and L. Xu, "A Mixed Access Control Method Based on Trust and Role", *The Second IITA International Conference on Geoscience and Remote Sensing*, 2010, pp. 552-555.

[11] L. Zhang and R. Rao, "Trust Based Access Control Framework for R-Osgi". *The 2nd International Workshop on Database Technology and Applications (DBTA)*, 2010, pp. 1-5.

[12] L. Zhao, S. Liu, J. Li and H. Xu, "A Dynamic Access Control Model Based on Trust", *International Conference on Environmental Science and Information Application Technology (ESIAT)*, 2010, pp. 548-551.

[13] S.Singh, "Trust Based Authorization Framework for Grid Services", *Journal of Emerging Trends in Computing and Information Sciences*, vol. 2, 2011, pp. 136-144.

[14] F. Almenarez, A. Marin, D. Diaz and J. Sanchez, "Developing a Model for Trust Management in Pervasive Devices", *Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops*, 2006, pp. 52-71.

[15] A. Lin, E. Vullings and J. Dalziel, "A Trust-Based Access Control Model for Virtual Organizations", *Fifth International Conference on Grid and Cooperative Computing Workshops*, 2006, pp. 557-564.

[16] L. Jia, M. Collins and P. Nixon, "Evaluating Trust-Based Access Control for Social Interaction", *Third International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies*, 2009, pp. 277–282.

[17] H. Tran, M. Hitchens, V. Varadharajan and P.Watters, "A Trust Based Access Control Framework for P2p File-Sharing Systems", *The 38th Annual Hawaii International Conference on System Sciences*, 2005, pp. 302-312.

[18] U. Naushahi, "Profile-Based Access Control in Cloud Computing Environments with applications in Health Care Systems", *MSc Thesis*, Bishop's University, Quebec, Canada, 2016.

[19] X. Luo, L. Yang, D. Hao, F.Liu, and D. Wang, "On Data and Virtualization Security Risks and Solutions of Cloud Computing", *Journal of Networks*, 9(3),2014, pp. 571–581.

[20] N. Maghanathan, "Review of access control models for cloud computing". *Computer Science & Information Science*, 3(1), 2013, pp.77–85.

