Building On/off Attacks Detector for Effective Trust Evaluation in Cloud Services Environment

SALAH T. ALSHAMMARI
salahtshammari@gmail.com
Department of Computer Science
College of Computing and Information Technology
King Abdul-Aziz University
Jeddah, Saudi Arabia

DR. AIIAD ALBESHRI
aaalbeshri@kau.edu.sa
Department of Computer Science
College of Computing and Information Technology
King Abdul-Aziz University
Jeddah, Saudi Arabia

DR. KHALID ALSUBHI
aaalbeshri@kau.edu.sa
Department of Computer Science
College of Computing and Information Technology
King Abdul-Aziz University
Jeddah, Saudi Arabia

Abstract
Cloud computing is a widely used technology that has changed the way people and organizations store and access information. This technology is quite versatile, which is why extensive amounts of data can be stored in the cloud. Furthermore, businesses can access various services over the cloud without having to install applications. However, the cloud computing services are provided over a public domain, which means that both trusted and non-trusted users can access the services. Though there are several advantages of cloud computing services, especially to business owners, various challenges are also posed in terms of the privacy and security of information and online services. A kind of threat that is widely faced in the cloud environment is the on/off attack. In this kind of attack, a few entities exhibit proper behavior for a given time period to develop a highly a positive reputation and gather trust, after which they exhibit deception. A viable solution is provided by the given trust model for preventing the attacks. This method works by providing effective security to the cloud services by identifying malicious and inappropriate behaviors through the application of trust algorithms that can identify on-off attacks.

Keywords
Trust Model, Reputation Attacks, Cloud Computing, On/off Attack, Cloud Services.

1. INTRODUCTION

A large number of threats are consistently faced by the users of cloud computing services, which include trust and reputation attacks. These threats are experienced because of the extremely dynamic, non-transparent and distributed nature of cloud computing services [1][2]. This is why cloud service providers and customers face significant challenges in preserving and handling trust in the cloud system [3]. The threats also emerge due to the reason that the provision of cloud computing services is on a public domain, which means that a large number of users have access to it [4]. The risks are clear from the actions of malicious users towards other cloud service consumers, who often given feedback with respect to their experiences.

Noor, Sheng, and Alfazi [1] have asserted that the feedback of service providers is an effective means of obtaining information that helps in examining the trustworthiness of cloud service customers. It has also been noted by Varalakshmi, Judgi, and Balagi [5] that a vital part is played by the feedback of service providers in generating trust for a cloud-based service. Cloud computing providers and customers use trust management systems and detection systems for reputation attacks to a large extent to provide improved protection and security to online data.

Though trust management and reputation attack detection systems are available, cloud computing systems continue to face targeted attacks from different sources [6][7]. It was found in the literature that there are shortcomings in the number of detection strategies that aim to prevent on/off attacks. Hence, vital information will be provided by this study regarding the way reputation attack detection mechanisms can be used for successful detection in cloud services. In addition, it will address the on/off attacks that decrease trust assessment in cloud computing. A major contribution will be made by this study to the existing literature regarding how the security and privacy of the cloud services can be improved by the providers and users of such services, which would provide an enhanced experience to the users on the whole.

Another major challenge emerges from authorization concerns regarding access to cloud computing. The issue is quite concerning because of the significant numbers of users and the big data of cloud computing linked to high data sensitivity [8][9]. In majority of the cases, this has led to the application of access controls within the cloud computing server application platforms. However, it has been found that the access controls related to the distributed systems are not reliable [10]. This is mainly because of the dynamic and complicated nature of consumers and the ineffectiveness of determining their identity beforehand [11]. To adequately handle these

Manuscript received July 5, 2024
Manuscript revised July 20, 2024
https://doi.org/10.22937/IJCSNS.2024.24.7.12

concerns, a better option for decentralized systems should be to integrate control models with trust models [12]. This solution has been attained following various attempts by developers of trust models to create new trust models that had the ability to solve the most complex and sophisticated issues linked to authorization [13][14]. Various proposals have been presented on the integrated trust models with access controls that face significant threats from attacks [15][16]. This paper aims to design a Trust Model System for curtailing reputation attacks on cloud services and providing high security to the cloud storage systems. A major security challenge experienced by reputation systems is the on/off attacks.

A. Problem Statement

The on/off attack is a widely prevalent threat in the cloud environments. Here, there are a few entities that show proper behavior for some time to create a highly positive reputation. Once they have generated trust, they start their deception. Malicious bodies win the trust of the TMS by exhibiting good behavior during interactions that have small impacts. However, when they come across a suitable opportunity in major interactions, their malicious intentions become evident. For example, sellers on eBay carry out various small transactions to generate a positive reputation and then after gaining trust, they cheat buyers on a more expensive product. Since these entities change their transactional behavior suddenly, it becomes difficult for other entities to sufficiently decrease the attacker's reputation. This also consists of oscillatory transaction behavior, where an entity keeps shifting from honest to dishonest behavior, because of which the attacker's reputation cannot be updated in a timely manner.

B. Contribution

The objective of this study is to develop the Trust Model System to prevent reputation attacks of cloud services so as to increase the security of cloud storage systems. Reputation systems are highly affected by the on/off attacks. These attacks are carried out by entities that present themselves as good nodes on an online platform; however, once they have acquired the trust of the system, they become malicious nodes. Nodes that carry out the on/off attacks may give false information or feedback so as to cause damage to system's reputation. A solution for the trust model systems for preventing on/off attacks will be presented in this study. In this regard, we will put forward the strategies that should be considered when developing the trust evaluation process. This paper will try to determine the solution that is most appropriate for the trust issues regarding access control approaches and will then present trust models that can be used to increase information security in distributed storage frameworks that use cryptographic access control techniques. It was found during the investigation that accurate results should be offered by a trust model while assessing trustworthiness, which is what our plan for the recommended trust-based distribution storage framework is based on. In the plan, trust prototypes can be organized into a framework that uses the cryptographic access control approach. To ensure its effectiveness, a trust model that offers the following is put forward in this paper:

- ✓ Ensuring that the greatest security is provided to the customers of cloud services because they may be dealing with extremely sensitive data when using the trust management services.
- ✓ Securing cloud services by effectively detecting malicious and inappropriate behaviors through the use of trust algorithms that can identify on-off attacks.
- ✓ Making sure that trust management service availability is adequate for the dynamic nature of cloud services.
- ✓ Providing dependable solutions to avoid reputation attacks and increase the precision of customers' trust values by considering the significance of interaction.

2. RELATED WORKS

A targeted increment has been experienced in the number of methods employed for examining and handling the trust for online services. Noor, Sheng, and Alfazi [1]) asserted in 2013 that these methods are developed after taking into account the feedback of customers of cloud services. The drawback of this study, however, is that the methods do not stress on the occasional and periodic reputation attacks that often hamper the privacy and security of cloud computing.

It is because of the dynamic nature of cloud computing that there has been very little focus on the periodic and occasional reputation attacks experienced by cloud services. In addition, the fact that multiple accounts may be held by a single user for accessing a single service makes the issue more complex. Noor, Sheng, and Alfazi [17] explained an advantage of the study in 2013, which is that it offers vital information with respect to the efficiency of occasional attacks detection models in identifying occasional and periodic reputation attacks. However, the emphasis of the study was not on particular attacks like the on/off attacks.

In the same way, a study was carried out by Labraoui, Gueroui, and Sekhri [18] in 2015 to examine whether the trust and reputation networks were successful in preventing reputation attacks. The O2 Trust mitigation for trust systems that is employed in wireless sensor networks was presented in the study. The mechanism of the mitigation system is that it reprimands those with history of misbehavior on every network node. The trust value of every network node is influenced by these penalties; therefore, it is considered as being successful in preventing misbehavior. The advantage of this study is that it offers vital information about O2 trust approach. Trust management in cloud computing was also examined by Noor, Sheng, and Bouguettaya [19] in 2014; however, it does not include how on/off attacks would be prevented by the trust management models. It was suggested by Tong, Liang, LU, and JIN [20] in 2015 that the trust model simply takes into account score value similarity and the collusion size score; however, it does not take into account the impact of scoring time.

Ghafoorian, Abbasinezhad-Mood, and Shakeri [21] carried out a study in 2018 to examine how the RBAC model, trust and reputation-based model is used to provide security to data storage in the cloud. It was determined in the study that the RBAC model successfully deals with the security risks with respect to the reputation and trust of cloud-based systems.

Other approaches have been examined to manage trust and reputation in cloud systems. A study was carried out by Nwebonyi, Martins, and Correia [22] in 2019 to evaluate how effective various models were in preventing trust and reputation risks in cloud-based systems. However, the focus of these studies was essentially on the privacy and security of the system on the whole; hence, they were unable to deal with particular attacks like on/off attacks.

3. Design & Methodology

The design methodology for this study will be a literature review, which is a systematic research method through which findings from earlier studies are collected and integrated [23][24][25]. When literature review is carried out rigorously while adhering to all the rules and conditions of assessing quality of research evidence, a sound basis is created for developing knowledge as well as theory. There is a lot of evidence on the attacks carried out on cloud-based services and the way these attacks can be avoided [26][27]. However, this evidence is extremely fragmented as the research mainly concentrates on a single kind of attack. The focus of this study will be on a single type of attack, which is similar in various ways to different attacks [29][28], despite their differences with respect to their features and how they are carried out in the cloud computing environment [30].

In this kind of attack, malicious behavior is exhibited by the user of cloud system in a small time frame. However, the user subsequently starts exhibiting a good code of conduct so that he/she can deceive the trust system and gain a good reputation. This kind of attack mostly occurs when proper behavior is initially shown by a malicious cloud service user for some time so as to attain a good reputation and gain the trust of other users. The user then starts taking advantages of this trust. Malicious users win the trust of the TMS in majority of the cases by behaving properly when interacting for small things. However, when he/she gets an opportunity in major interactions, his/her malicious intents become evident.

Opportunistic, but malicious behavior of various nodes is characteristic of the attacks that are made in direct trust, including the trust of the system. There is a shift in the good and bad behavior of switches, which creates a disguise due to which the node is considered trustworthy despite its inappropriate behavior (Labraoui, Gueroui, and Sekhri [4]). For instance, malicious behavior can be exhibited by a node that is considered as being trustworthy on an e-commerce website. However, this behavior is not identified because the node was initially considered trustworthy by the system. The interaction trust IT will initially be computed by the trust model system, which offers an accurate result for the trust value of every cloud service consumer CR by calculating the SP's interaction importance II . The feedback F with respect to an interaction is presented as a percentage. Equation (1) given below is used to compute interaction trust IT.

$$IT(CR) = \sum_{i=1}^{n-1} \frac{\alpha_i^t(CR) + P_{CR}}{(\alpha_i^t(CR) + P_{CR}) + (\beta_i^t(CR) + N_{CR})} \quad (1)$$

$$\sum_{i=1}^{n} \alpha_i^t(CR) = \begin{array}{c c} & \begin{array}{ccccc} \alpha_1^t & \alpha_2^t & \cdots & \alpha_{n-1}^t & \alpha_n^t \end{array} \\ \begin{array}{c} CR_1 \\ CR_2 \\ \vdots \\ CR_n \end{array} & \begin{pmatrix} V_{1,1} & V_{1,2} & \cdots & V_{1,n-1} & V_{1,n} \\ V_{2,1} & V_{2,2} & \cdots & V_{2,n-1} & V_{2,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ V_{n,1} & V_{n,2} & \cdots & V_{n,n-1} & V_{n,n} \end{pmatrix} \end{array}$$

$$\sum_{i=1}^{n} \beta_i^t(CR) = \begin{array}{c c} & \begin{array}{ccccc} \beta_1^t & \beta_2^t & \cdots & \beta_{n-1}^t & \beta_n^t \end{array} \\ \begin{array}{c} CR_1 \\ CR_2 \\ \vdots \\ CR_n \end{array} & \begin{pmatrix} V_{1,1} & V_{1,2} & \cdots & V_{1,n-1} & V_{1,n} \\ V_{2,1} & V_{2,2} & \cdots & V_{2,n-1} & V_{2,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ V_{n,1} & V_{n,2} & \cdots & V_{n,n-1} & V_{n,n} \end{pmatrix} \end{array}$$

$$P_{CR} = \frac{\alpha_n^t(CR) \times II}{NF}$$

$$N_{CR} = \frac{\beta_n^t(CR) \times II}{NF}$$

Here, positive feedback in a given time is shown by α^t; negative feedback in a given time is shown by β^t ; P denotes the value of the new positive recommender feedback and N presents the value of the new negative recommender feedback; the Interaction Importance value is given by II and the feedback numbers are denoted by NF.

The risk of on-off attacks (O^2) can be prevented by incorporating the penalty for the on-off Attack (P^{O^2}). This penalty is fixed from 1 to n, where 1 refers to no risk from this user and n is representative of high Interaction Importance times the dangers rate DR . P^{O^2} for any customer will be calculated by the trust model by using a novel process, in which PC^{O^2} is the smallest value of the greatest interactions.

$$\begin{cases} if\ II \geq PC^{O^2} and\ \beta_n^t < II\ \ then & P^{O^2} = II \times DR \\ else & P^{O^2} = 1 \end{cases}$$

$$IT(CR) = \sum_{i=1}^{n-1} \frac{\alpha_i^t(CR) + P_{CR}}{(\alpha_i^t(CR) + P_{CR}) + (\beta_i^t(CR) + N_{CR} \times P^{O^2})} \qquad (2)$$

The penalty of trust decline (P^{TD}) should be added to prevent the risk of trust decline (TD), where the P^{TD} ranges from 1 to n, in a way that 1 signifies no risk from this customer role and n signifies high risk, PC^{TD} refers to the curve of a penalty of trust decline and its integer greater than 1, L^{II} denotes the limit of low interaction.

$$IT(CR) = \sum_{i=1}^{n-1} \frac{\alpha_i^t(CR) + P_{CR}}{(\alpha_i^t(CR) + P_{CR}) + (\beta_i^t(CR) + N_{CR} \times P^{O^2} \times P^{TD})} \qquad (3)$$

$$\begin{cases} if\ \beta_n^t < II & then \quad P^{TD} = PC^{TD} \\ else & P^{TD} = 1 \end{cases}$$

$$PC^{TD} = \sum\nolimits_{P^{TD} > L^{II}} P^{TD}$$

PC^{TD} is used to find out the value of penalty of trust decline (P^{TD}) and to prevent the attacks, the dangers rate R and the penalty for on-off attack (P^{O^2}) are used. Algorithm 1 is given below:

Algorithm 1: On\off Attack Algorithm

```
Input: $F, II$;
Output: Consumer Trust Value;
procedure Interaction Trust
    $\alpha_n^t(CR) = F$
    $\beta_n^t(CR) = F - 1$
    $P_{CR} \leftarrow (\alpha_n^t(CR) \times II)/NF$
    $N_{CR} \leftarrow (\beta_n^t(CR) \times II)/NF$
    if $II \geq PC^{O^2}$ and $\beta_n^t < II$ then $P^{O^2} = II \times DR$
        else $P^{O^2} = 1$
    end if
    if $\beta_n^t < II$ then $P^{TD} = PC^{TD}$
        else $P^{TD} = 1$
    end if
    for $i = 1, \quad i \leq n - 1$;
        $IT(CR) \leftarrow (\alpha_i^t(CR) + P_{CR}) / \left((\alpha_i^t(CR) + P_{CR}) + (\beta_i^t(CR) + N_{CR} \times P^{O^2} \times P^{TD})\right)$
    end for
end procedure
```

4. Proposed Framework Architecture

The various elements of the trust model are analyzed in this section. The part played by each of the components in making sure that the system functions effectively is also presented. The proposed system architecture is shown in Figure 1.

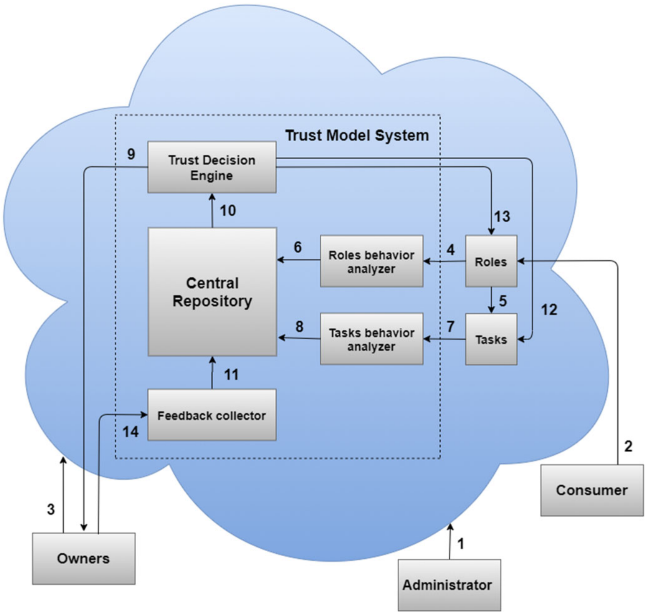

Figure 1: Trust Model System Architecture.

In the proposed design, TMS will be the element that examines the degree to which customers of cloud services wish to rely on the cloud services providers. It will be responsible for offering cloud services with the expectation that the quality that the cloud service providers have promised is actually offered. There are different sub-sections of the trust management system, each of which is assigned distinct tasks that make sure that the data available in the cloud storage system is secure. The rules identified within the level of trust are examined on the basis of the feedback given by service providers (Noor, Sheng, Maamar & Zeadally, 2016). It is important to determine the identity of the user and monitor the activities carried out to make it easier to track unauthorized customers or attackers and to present evidence for any leaking of data. The registered and unregistered customers are updated using the TMS. In addition, all activities carried out by the customers are also identified. This will monitor the authorization of all those adding feedbacks into the system. The TMS can recognize invalid feedback and remove it from the system.

Trust Management System (TMS):

Different layers are added to the trust model to increase the effectiveness of the overall system. There are different sub-sections in the trust management system and these are described subsequently.

Central Repository: this functions as the interaction store. It stores all kinds of trust records and interaction histories created by interacting tasks and roles for being used subsequently by the decision engine trust for assessing the task and role values. The central repository cannot access those elements that are not present in the trust management system.

Role Behavior Analyzer: It is the component that analyses the functions and roles related to smallest levels of trust regulations with respect to shared resources. It evaluates those rules that have been identified in the level of trust, based on the feedback given by the service providers in the central repository (Noor, Sheng, Maamar & Zeadally, 2016). The roles are linked by the role behavior analyzer to obtain information about them and identify any leakage that occurs. It is imperative to determine the user's identity and monitor all actions carried out by them so that unauthorized customers or attackers can easily be tracked and evidence for any kind of data leakage can be presented. The accounts of registered and unregistered customers are also updated by the role behavior analyzer and all events carried out by a customer are identified.

Task Behavior Analyzer: It is the responsibility of the task behavior analyzer to evaluate tasks and functions with respect to minimum trust level laws when accessing shared resources. The tasks identified within the trust level are analyzed in terms of the feedback of owners by calculating trust value and this value is then stored in the central repository. It obtains information from the channels; there are two channels here, which include the reports from tasks regarding data leakage and the reports from role behavior analyzer to determine the histories of customers with respect to the stored data. Customers should be identified by the task behavior analyzer and the tasks performed should be tracked. This would make it easier to track attackers or unauthorized customers and present proof of data leakage if it has occurred. Registered customer accounts will also be updated and it will be determined if the incident has been carried out by a customer account.

Feedback Collector: It is the responsibility of the feedback collector to manage feedback from the owners of service to the repository headquarters before its automatic allocation. However, the user's trustworthiness is shown by the feedback given on roles and tasks. To ensure security, the collector of task and roles feedback secures its integrity. The authorization of the one uploading feedbacks into the system is ensured by this component. It has the ability to recognize invalid feedback and also eliminate all those feedbacks from the system that are not valid. In addition, information is acquired by the collector of role feedback regarding data assignments of tasks and roles before it is uploaded to the central repository

Trust Decision Engine: This section analyses and identifies the value of trust of the data owners, the roles and the values of the entity. It obtains all kinds of information regarding the interaction histories that are found in the repository centre and the trust values of a specific customer before determining the kind of response that the system should give.

5. Simulation Results

Experiments will be used in this section to determine the trust model's capability to resist reputation attacks.

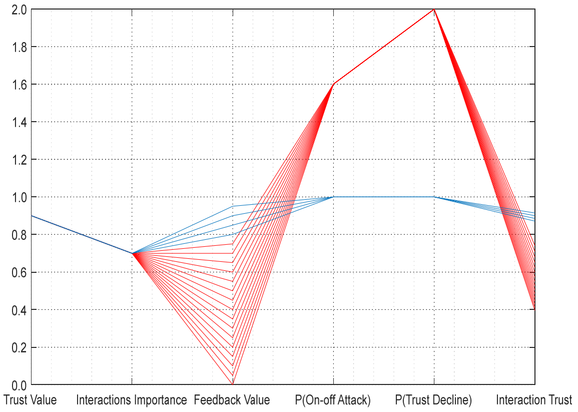

Figure 2: Penalties of On/off Attack and Trust Decline

The penalties for the on-off attack will be determined by the TMS based on two conditions; whether the Interaction Importance is more than or equal to the dangers rate DR, and whether the feedback F of the recommender is less than the interaction importance II. When the recommender's feedback F is lower than the Interaction Importance II, the trust decline penalty P^{TD} will be determined by the trust model. The effect of the penalty of on/off attack and Trust Decline in the interaction trust values are illustrated in Figure 2.

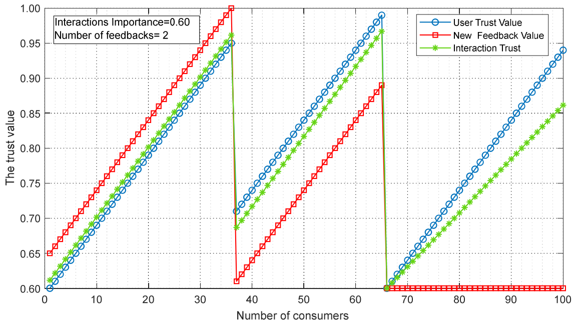

Figure 3: Interaction trust values for 100 trusted consumers

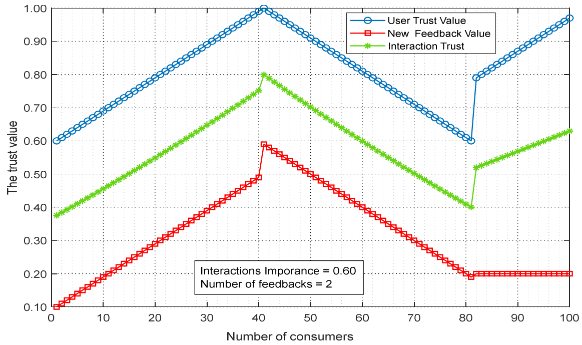

Figure 4: Interaction trust values for 100 malicious consumers

The value of Interaction Trust for malicious users will be determined by the trust model by using the penalties of malicious behavior. The effect of new feedbacks on the Interaction Trust for malicious users and trusted users are demonstrated in Figures 3 and Figures 4.

6. CONCLUSION

Authorization concerns regarding access to cloud computing storage are a significant challenge for several users and big data of cloud computing because the data involved is very sensitive. A trust model was presented in this paper that provides dependable solutions for preventing on/off attacks, which is a major security issue being faced by cloud computing users. To adequately handle these concerns, control models should be integrated with trust models for decentralized systems.

REFERENCES

[1] Talal H. Noor, Quan Z. Sheng, and Abdullah Alfazi, "Reputation Attacks Detection for Effective Trust Assessment Among Cloud Services," in *12th IEEE International Conference on Trust*, Security and Privacy in Computing and Communications, 2013, pp. 469–476.

[2] Eric Chang, "General Attacks and Approaches in Cloud-Scale Networks," in *IEEE International Conference on Computer Communications,* 2019.

[3] Swati Mahajan, Sarika Mahajan, Shubhangi Jadhav, and Sangita Kolate, "Trust Management in E-commerce Websites," in *International Research Journal of Engineering and Technology (IRJET),* 2017, pp. 2934–2936.

[4] T. H. Noor, Q. Z. Sheng, L. Yao, S. Dustdar, and A. H.H. Ngu, "CloudArmor: Supporting Reputation-Based Trust Management for Cloud Services," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 2, pp. 367-380, 2015.

[5] P. Varalakshmi, T. Judgi, and D. Balaji, "Trust Management Model Based on Malicious Filtered Feedback in Cloud. In International Conference on Data Science Analytics and Applications," in *International Conference on Data Science Analytics and Applications,* 2018, pp. 178–187.

[6] X. Li, and J. Du, "Adaptive and Attribute-based Trust Model for Service Level Agreement Guarantee in Cloud Computing," IET Information Security, vol. 7, no. 1, pp. 39-50, 2013.

[7] Huang Lanying, XiongZenggang, Wangguangwei, "A Trust-role Access Control Model Facing Cloud Computing," Proceedings of the 35th Chinese Control Conference , July 27-29, 2016.

[8] G. Lin, D. Wang, Y. Bie, and M. Lei, "MTBAC: A Mutual Trust Based Access Control Model in Cloud Computing," China Communications, vol. 11, no. 4, pp. 154-162, 2014.

[9] C. Zhu, H. Nicanfar, V. C. M. Leung, and L. T. Yang, "An Authenticated Trust and Reputation Calculation and Management System for Cloud and Sensor Networks Integration," IEEE Transactions on Information Forensics and Security, vol. 10, no. 1, pp. 118-131, 2014.

[10] C. Uikey, and D. S. Bhilare, "TrustRBAC: Trust Role Based Access Control Model in Multi-domain Cloud Environments," in International Conference on Information, Communication, Instrumentation and Control (ICICIC), 2017, p. 978-1-5090-6314-7.

[11] P. Zhang, Y. Kong, and M. Zhou, "A Domain Partition-Based Trust Model for Unreliable Clouds," IEEE Transactions on Information Forensics and Security, vol. 13, no. 9, pp. 2167-2178, Sept. 2018.

[12] Zhanjiang Tan, Zhuo Tang, Renfa Li, Ahmed Sallam, and Liu Yang, "Research of Workflow Access Control Strategy based on Trust," in 11th Web Information System and Application Conference, Sept. 2014.

[13] X. Li, H. Ma, F. Zhou, and W. Yao, "T-Broker: A Trust-Aware Service Brokering Scheme for Multiple Cloud Collaborative Services," IEEE Transactions on Information Forensics and Security, vol. 10, no. 7, pp. 1402-1415, 2015.

[14] Mali Varsha, Prof. Pramod Patil, "A Survey on Authentication and Access Control for Cloud Computing using RBDAC Mechanism," International Journal of Innovative Research in Computer and Communication Engineering , 2015, 12125–12129.

[15] X. Li, H. Ma, F. Zhou, and X. Gui, "Service Operator-Aware Trust Scheme for Resource Matchmaking across Multiple Clouds," IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 5, pp. 1419-1429, May. 2014.

[16] T. Bhattasali, R. Chaki, N. Chaki, and K. Saeed, "An Adaptation of Context and Trust Aware Workflow Oriented Access Control for Remote Healthcare," International Journal

of Software Engineering and Knowledge Engineering, vol. 28, no. 6, pp. 781–810, 2018.

[17] 3Talal H. Noor, Quan Z. Sheng, and Abdullah Alfazi, "Detecting occasional reputation attacks on cloud services," in *International Conference on Web Engineering,* 2013, pp. 416–423.

[18] 4Nabila Labraoui, Mourad Gueroui, and Larbi Sekhri, "On-off attacks mitigation against trust systems in wireless sensor networks," in *IFIP International Conference on Computer Science and its Applications,* 2015, pp. 406–415.

[19] 5Talal H. Noor, Quan Z. Sheng, and Athman Bouguettaya, *Trust management in cloud services*, Springer, Cham, 2014.

[20] 6Tong Wei-ming, Liang Jian-quan, LU Lei, and JIN Xian-ji, "Intrusion detection scheme based node trust value in WSNs," in *Systems Engineering and Electronics,* 2015, pp. 1644–1649.

[20] 7Mahdi Ghafoorian, DariushAbbasinezhad-Mood, and Hassan Shakeri, "A Thorough Trust and Reputation Based RBAC Model for Secure Data Storage in the Cloud," *IEEE Transactions on Parallel and Distributed Systems*, Vol: 30, Issue: 4, Apr. 2019.

[21] 8Francis N. Nwebonyi, Rolando Martins, and Manuel E. Correia, "Reputation based approach for improved fairness and robustness in P2P protocols," in *Peer-to-Peer Networking and Applications,* 2019, pp. 951–968.

[22] Wenyang Deng, and Zhouyi Zhou, "A Flexible RBAC Model Based on Trust in Open System," in Third Global Congress on Intelligent Systems, 2012.

[23] Huang Lanying, XiongZenggang, and Wangguangwei, "A Trust-role Access Control Model Facing Cloud Computing," in Proceedings of the 35th Chinese Control Conference, 2016.

[24] Lan Zhou, Vijay Varadharajan, and Michael Hitchens, "Integrating Trust with Cryptographic Role-based Access Control for Secure Cloud Data Storage," in 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2013.

[25] Wei Chang, Feng Xu, and Jianping Dou, "A Trust and Unauthorized Operation Based RBAC (TUORBAC) Model," in International Conference on Control Engineering and Communication Technology, 2012.

[26] D. Marudhadevi, V.Neelaya Dhatchayani, and V.S. Shankar Sriram, "A Trust Evaluation Model for Cloud Computing Using Service Level Agreement," The Computer Journal, Vol.58, pp.2225–2232, Nov. 2014.

[27] W.T.Tsai, Peide Zhong, Xiaoying Bai, and Jay Elston, "Role-Based Trust Model for Community of Interest," in IEEE International Conference on Service-Oriented Computing and Applications (SOCA), 2009.

[28] Fan Yue-qin, and Zhang Yong-sheng, "Trusted Access Control Model Based on Role and Task in Cloud Computing," in 7th International Conference on Information Technology in Medicine and Education, 2012.

[29] Bhatt, Smriti, Ravi Sandhu, and Farhan Patwa, "An Access Control Framework for Cloud-Enabled Wearable Internet of Things," in *IEEE 3rd* International Conference on Collaboration and Internet Computing (CIC), pp. 213-233, Oct. 2017.

SALAH T. ALSHAMMARI Ph.D. student at King Abdulaziz University, department of computer science, college of computing and information technology, Jeddah, Saudi Arabia. His main research interests are Information Security, Cybersecurity, Security in Cloud Computing, Trust in Cloud Computing, and Software Testing.

DR. AIIAD ALBESHRI Associate professor at King Abdulaziz University, department of computer science, college of computing and information technology, Jeddah, Saudi Arabia. His main research interests are Cloud Computing, Security in Cloud Computing, Storage in Cloud Computing, Geographic Assurance in Cloud Computing, Trust in Cloud Computing, and Big Data.

DR. KHALID ALSUBHI Associate professor at King Abdulaziz University, department of computer science, college of computing and information technology, Jeddah, Saudi Arabia. His main research interests are Information and Network Security, Security of Big Data and IoT, Software Defined Networking and Network Function Virtualization.