Middle-East Journal of Scientific Research 25 (6): 1315-1325, 2017
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2017.1315.1325

Extensive Review on Intelligent Cloud Security Mechanisms

A.R. Arunarani and D. Manjula

Department of Computer Science and Engineering,
College of Engineering Guindy Campus, Anna University, Chennai-600025, Tamil Nadu, India

Abstract: Cloud computing is offering best services in many applications through mobile clouds, cloud networks, cloud databases and web applications. In such a scenario, the greatest challenges faced by many cloud systems are the security vulnerabilities. In order to solve this problem, different solutions were proposed by different researchers who work in the areas of cloud computing and security systems. In this research, a survey on methods used for cloud security including newly proposed methods based on access control, intrusion detection systems and trust management systems is presented. The main advantages of this paper provide a complete survey of all the important security mechanisms that are based on computational intelligence techniques and are available in the literature. In addition to these existing systems survey, we propose an intelligent secured location based log management algorithm for secured data storage in this paper. The experimental results of the proposed algorithm stored the data securely in the cloud environment when compared with the existing algorithms.

Key words: Cloud Computing · Trust Management · Intelligent Intrusion Detection System · Classification · Access Control · Vulnerability · Intelligent Agents

INTRODUCTION

Cloud computing provides effective services in the recent years due to the availability of internet and web technologies. Therefore, the large scale infrastructure in terms of nodes and servers, networks, databases, memory and processing power provided by cloud computing helps to store and retrieve the data very effectively. Moreover, cloud service providers made the model of pay by demand services to the user community. In such a scenario, the usage of internet and web for different applications grows enormously. Due to this growth, security attacks also grow at all levels of cloud computing leading to risk in cloud data storage and management.

In order to secure the data stored in cloud, many security mechanisms are already proposed by many researchers, which are available in the literature. However, the existing security mechanisms are not sufficient to handle the malicious activities and virtual machine intrusion attacks. Hence, newer and more efficient security methods are required to improve the security of cloud system using different mechanisms such as intrusion detection and prevention system, implementation of access control policies and trust management. Even though, many cloud service providers have implemented data encryption techniques, access control policies and firewalls for addressing the security challenges. However, the new type of attacks introduced by malicious users must be detected and prevented before destroy the useful information. Therefore, some researchers have proposed intrusion detection and prevention systems, which suit the cloud environment.

In this paper, a survey on security mechanisms for cloud database systems is provided. This paper focuses on two important aspects namely the works, which proposed security solutions based on the extension of the existing security mechanisms available for networks and databases. The second aspect is the proposal of new techniques by various researchers, which are specifically suitable for cloud environment. From the literature, it is found that the techniques from Artificial Intelligence, Soft Computing and other computational intelligence approaches are providing more security than the existing conventional mechanisms for security. Therefore, this paper provides a survey of important works found in the literature on cloud security with a focus on cloud

Corresponding Author: A.R. Arunarani, Department of Computer Science and Engineering, College of Engineering Guindy Campus, Anna University, Chennai-600025.Tamil Nadu, India.

database security. It also provides a comparative analysis on works related to access control, intrusion detection and prevention and trust management. In this survey, the works related to the application of fuzzy rules, production rules, genetic algorithms and intelligent agents for providing security to cloud using computational intelligence techniques are considered.

The remainder of the paper is organized as follows: Section 2 discusses the related works on access control. Section 3 details the works available in the literature for intrusion detection and prevention. Section 4 explains the works that provide security using trust management. Section 5 describe in detail about the proposed work. Section 6 provides results and discussion. Section 7 gives conclusion on this survey and suggests some additional topics to be survey in future.

Related Works on Access Control: Access control technology for web and cloud databases has become an important area of research in the recent years. Therefore, a number of researchers have contributed their ideas and works in the literature in this area. Among them, Damiani *et al.* [1] proposed a new access control technique for web databases. On the other hand, many researchers including Damiani *et al.* [2] and Bhatti *et al.* [3] have proposed new methods for access control to web documents by providing new rules for making access restrictions directly on both the schema and content of the web documents. However, most of these works have focused more on securing the web databases rather than the cloud databases. Huang *et al.* [4] have proposed new access control policies for web databases that used regular path expressions for specifying the database object for applying the access control policies. Their work is more suitable for providing access control to web databases that use XML based queries. Sriram Mohan *et al.* [5] have proposed a model for access control to secure the web documents by specifying access constraints for enforcing the access privileges using query rewrite operations.

He and Wong [6] have proposed a new type of Role Based Access Control (RBAC) model for providing secured web information management. In this access control scheme, it is necessary to provide a path to access information. This scheme is more suitable for web databases and hence can be extended to suit the cloud database environment. Liu *et al.* [7] proposed a new access control model based on the analysis of the applications to know the access control requirements for web applications. They discussed about the limitations of current access control models for web services and proposed a new attribute based RBAC model for web applications. He and Lee [8] proposed a new web security model by implementing RBAC in the web services environment. Their work focused more on applying the RBAC policies to protect e-learning applications. In spite of all these works, the researchers in this area have proposed no complete access control model for cloud databases yet. Moreover, the inclusion of rules, Spatio-temporal constraints that are intelligently handled by intelligent agents can be more effective for securing the cloud databases.

Sandhu *et al.* [9] presented another type of RBAC model based on users, roles and operations. The interest in RBAC has led to the use of roles at the application level to control access through the applications that use web data. Li *et al.* [10] proposed new security methods to maintain desirable security by assigning privileges. Barker[19] introduced a generalized RBAC model called Action Status Access Control model for web database security based on automatic changing of access control policies based on the events for trigger. Moreover, the author provided the implementation details for their model and evaluated using performance metrics. Bertino *et al.* [11] proposed a Temporal-RBAC (TRBAC) model by providing temporal extensions to RBAC. The main advantage of this model is that it supports dynamic enabling /disabling of roles and actions using events and triggers. The use of triggers in this model enhanced the decision-making power using intelligent production rules.

James B.D *et al.* [12] proposed a new TRBAC model with the use of temporal constraints for role assignment. Moreover, it allows adding a new set of temporal constraints at any time. Xiutao Cui *et al.* [13] presented an Extended RBAC by adding identity and integrity constraints for a mobile environment. The authors also added some new assignment rules for handling the privileges and roles. Li *et al.* [14] made a comparative analysis of the action based access control model with the other existing access control models and proved that action based access control is more suitable for distributed systems.

Zhou *et al.* [15] proposed a new trust model to secure the stored data in cloud database systems. Their trust model provides a facility for the owners and roles to decide on the trustworthiness of individual roles for users. The authors presented a security model that shows how the trust models are integrated with cryptographic access control schemes. The main advantage of this model is that it helps to provide security to cloud databases.

Table 1: Comparative Analysis

	Model				
Metrics	Role Checking	Temporal Analysis	Role Support	Inference	Virtualization
RBAC (Barker *et al.* [16])	High	High	Medium	Low	No
Ex-RBAC (Cui *et al.* [13])	High	High	High	Medium	No
TRBAC (James *et al.* [12])	High	High	High	High	No
Integrated Trust & Access Control (Zhou *et al.* [15])	High	High	High	High	Yes

Table 1 shows the comparative analysis for all kinds of access control mechanisms based on various metrics such as role checking, temporal analysis, role support, inference and virtualization. In this model, the membership values from 0 to 0.4 are considered as "low", 0.3 to 0.7 are considered as "medium" and 0.6 to 1.0 are treated as "High" to perform the fuzzy classification. The threshold values are set based on the existing works on access control and trust management techniques available from the literature. It has been validated again using the experiments conducted in this work. In addition to fuzzy classification, the system used genetic algorithms to optimize the number of rules to be used in the inference process. The use of computational intelligence techniques namely fuzzy rules and genetic algorithms helped to improve the performance in terms of security, time taken to perform analysis and fast response.

From Table 1, trust based models provide enhanced security cloud databases with virtualization. Hence, it is recommended that a hybrid model that integrates access control, temporal constraints, rules and virtualization is more suitable for providing security to cloud databases.

Taeho Jung *et al.* [17] presented a semi-anonymous privilege control scheme to address not only the data privacy, but also the user identity privacy in existing access control schemes. Muthurajkumar *et al.* [18] developed a cloud security model using transaction logs. According to these authors, Log Management is an important activity in the Cloud. In any cloud based database applications, the challenge lies in the maintenance of log records securely over an interval of time. Moreover, such a log is not only helpful for recovery operations but also useful for maintaining integrity, security and effective auditing. They divided their work into different phases and each phase is identified by a time interval. They proposed a new algorithm for log based recovery of transactions in cloud databases that maintains not only the log records but also the history of data records. They use cryptographic encryption and decryption technique for storing the data with security in which the keys are generated using primary key attributes and temporal information. Their temporal model for log management is a new contribution in the area of cloud database recovery with security. Moreover, their model is powerful than the role based access control model since the use keys with time interval as a component for encryption and decryption.

Xuanxia *et al.* [19] proposed a lightweight ciphertext-sharing scheme that uses an anonymous authorization credential to simplify access control, ensure users' anonymity and support decryption key reconstruction. Zubair A. Baig *et al.* [20] proposed a novel and reactive approach based on a rate limit technique, with low overhead, to detect and mitigate EDoS attacks against cloud-based services. Through this reactive scheme, a limited access permission for cloud services is granted to each user. Tsz Hon Yuen, *et al.* [21] proposed a new scheme called k-times attribute-based anonymous access control, which is particularly designed for supporting cloud environment. Moreover, they also provide a k-times limit for anonymous access control. That is, the server may limit a particular set of users to access the system for maximum k-times within a period or an event. Lan Zhou, *et al.* [22] proposed new trust models to reason about and to improve the security for stored data in cloud storage systems that use cryptographic RBAC schemes. The trust models provide an approach for the owners and roles to determine the trustworthiness of individual roles and users, respectively, in the RBAC system. Their trust models consider role inheritance and hierarchy in the evaluation of trustworthiness of roles. They present a design of a trust-based cloud storage system, which shows how the trust models can be integrated into a system that uses cryptographic RBAC schemes. They also considered practical application scenarios and illustrated how the trust evaluations can be used to reduce the risks and to enhance the quality of decision making by data owners and roles of cloud storage service.

Massimo Ficco and Massimiliano Rak [23] proposed a strategy to orchestrate stealthy attack patterns, which exhibit a slowly increasing intensity trend designed to inflict the maximum financial cost to the cloud customer, while respecting the job size and the service arrival rate imposed by the detection mechanisms. They described both how to apply the proposed strategy and its effects on the target system deployed in the cloud. Yasir Mehmood [24] proposed a unique security scheme called

Distributed Intrusion Detection System using Mobile Agents in Cloud Computing (DIDMACC) to detect the distributed intrusions in cloud. They have used mobile agents to carry intrusion alerts from consumer virtual machines to the management server where correlation takes place. Their system can detect the intrusions on virtual machines, identify the vulnerable ports and can correlate malicious events to detect distributed intrusions in a cloud-based network. Mobile agents used to update the signature database at virtual machines being monitored. Mobile agents, being lightweight and flexible software programs, reduce the network load by carrying intrusion-related data and code. Their scheme provides a scalable and robust intrusion detection system, which is a key requirement for cloud networks.

Xinfeng Ye [25] proposed scheme allows cloud users to delegate their access permissions to other users easily for facilitating the resource sharing. Their scheme uses cryptographic techniques to obscure the access control policies and users' credentials to ensure the privacy of the cloud users. They used data encryption to guarantee the confidentiality of data. Hu Ma *et al.* [26] identified some mistakes from the existing anonymous attribute based encryption scheme, which is calculates the system wide master key. The attribute based encryption scheme focused on the data contents privacy and the access control with less attention to the privilege control and privacy identification problem. Joseph K. Liu *et al.* [27] introduced a new fine-grained two-factor authentication access control systems for web-based cloud computing services. Specifically, their system based on attribute-based access control mechanism which is implemented with the both user secret key and a lightweight security device. Moreover, their system enables the cloud server to restrict the access to those users with the same set of attributes while preserving user privacy.

Works on Intrusion Detection and Prevention: Many works on Intrusion Detection are found in the literature for cloud security. Among them, Mansour *et al.* [28] proposed a machine learning based method called Growing Hierarchical Self organized Map for effective intrusion detection in cloud. Their system reduces the false positive rate and false negatives significantly for enhancing the security. Amjad *et al.* (2013) proposed anew anomaly based Intrusion Detection System using soft computing techniques for virtual machines on cloud computing. Their model is best-suited cloud environments.

Zubair *et al.* [30] proposed a new intrusion detection system, which classifies the network data into normal and abnormal groups using two types of techniques namely Monolithic and Ensemble-based techniques for intrusion detection. Louvieris *et al.* [31] proposed an intrusion detection technique, which detects the attacks networks by identifying the contributing features. Reda *et al.* [32] proposed a network intrusion detection system using the random forests algorithm for classification. This algorithm defects both insider and outsider attacks. Koc *et al.* [33] used Naive Bayes classifier in their work for the detection of Denial-of-Services (DoS) attacks.

Hasani *et al.* [34] introduced a new wrapper based model based on Genetic Programming and Bees Algorithm for feature selection algorithm to build an IDS. Gisung Kim *et al.* [35] proposed a new hybrid intrusion detection model, which is capable of finding, both misuse and anomaly intrusions. Qiao Yan *et al.* [36] explained the causes for Distributed Denial of Service (DDoS) attacks and their growth in cloud computing environments. In addition, they explained the good features of Software Defined Networking (SDN) based cloud for preventing DDoS attacks. Zhifeng Xiao and Yang Xiao [37] systematically presented the security and privacy issues in cloud computing and identified the most representative security/privacy attributes for cloud security. They also explained about attack and prevention models for cloud data security.

Table 2 shows the comparative analysis for the different environments with various techniques used for intrusion detection and prevention. In this model, triangular membership values are used to form the fuzzy rules. Moreover, the fuzzy rules formed in this work have been validated by consulting with domain experts in the field of security. Moreover, we considered three fuzzy linguistic variables namely "Low", "Medium" and "High" to express the performance of network monitoring in the 0 to 1 scale. For this purpose, the membership values from 0.7 to 1.0 are considered as "High", 0.5 to 0.8 are considered as "Medium" and 0 to 0.51 are treated as "Low" to perform the fuzzy classification. The threshold values are fixed for fuzzy membership based on the related work on intrusion detection based on classification techniques. The models considered in this work include classification based, signature based, anomaly based and Virtualization and Elasticity property based and based on intelligent techniques. Moreover, intelligent agents are deployed at each node of the cloud network as well as the servers. The uses of intelligent agents for network and database monitoring help to enhance the security in comparison with other existing works.

Table 2: Comparative analysis for IDSs

Model	Network Monitoring	Host Monitoring	Database Monitoring	Cloud Resource Monitoring
Classification based [33, 32]	High	Medium	Medium	Low
Signature Based [37]	High	High	Low	Low
Anomaly based [35]	High	High	Medium	Low
Virtualization and Elasticity Property [28]	Low	Low	Low	High
Intelligent Techniques [36, 38]	High	High	High	High

From Table 2, it is observed that the use of intrusion detection models for securing the cloud databases provide better performance in comparison with other security methods used for securing the cloud databases.

Kulothungan *et al.* [39] proposed a new cluster based secure routing scheme, which is useful for energy optimization through clustering and key-based security. They extended the Adhoc Ondemand Distance Vector (AODV) routing protocol for enhancing the QoS in networks. Sindhu *et al.* [40] proposed about the construction of a lightweight Intrusion Detection System (IDS), which is useful for detecting the anomalies in computer networks. Moreover, they proposed a new feature selection algorithm that is based on genetic algorithm for identifying the most important features from the dataset. They focused on three aspects namely unbiased dataset for training and testing and wrapper based approach for feature selection. They used neuro-tree based IDS, which performs effective classification by applying the selected features on a new type of neuro-tree to improve the detection accuracy. They considered the sensitivity and specificity for evaluating their system. They compared their result with six types of decision tree algorithms namely Decision Stump algorithm, C4.5 Classifier, Naive Baye's Tree for classification, Random Forest algorithm, Random Tree classifier and Representative Tree classification model in order to perform intrusion detection effectively.

Anand *et al.* [41] proposed a new rule based feature selection algorithm for reducing the number of features by eliminating the redundant and non-contributing features from the dataset. Their work focused mainly on extracting the most important and suitable features which can specially identify the Denial of Service (DoS) attacks. Moreover, the authors proposed a new version of Multiclass Support Vector Machines (MSVM) for performing effective classification and they developed the algorithm by enhancing the existing Multiclass SVM. The main advantages of their model are improvements in detection and classification accuracy and additionally reduction in false positive rate.

Ganapathy *et al.* [42] provided a survey on the use of techniques from artificial intelligence and soft computing for effective feature selection and better classification to develop efficient intrusion detection systems to be deployed in computer networks. In their survey, they focused on different areas of artificial intelligence namely intelligent agents, neural classifiers, genetic algorithm based classification, neuro-genetic modeling for classification, use of fuzzy logic and rough sets to handle uncertainty in classification and the application of particle swarm optimization for developing intelligent intrusion detection systems. According to them, the proposed techniques collected from different works are useful for effectively identifying the attacks and for effective prevention of network intrusions. Their survey focuses on the existing models on IDS and they provided a suggestion to improve the performance by proposing a new model.

Sannasi *et al.* [43] proposed intelligent IDS by proposing a modified form of Conditional Random Field (CRF) called Intelligent CRF for feature selection, which applies statistical methods in order to select optimal number of features from available set of features. In addition, the authors proposed a new classification algorithm called modified layered approach in which they extended the existing Layered Approach algorithm by including a middle layer to enhance the classification accuracy. They proved their model using different metrics namely detection time, false alarm rate and classification accuracy. They carried out suitable experiments by using network trace data as well as benchmark dataset to establish the efficiency of their model.

Works on Trust Management: In the past, many researchers have worked on trust management systems to tackle the attacks by inside attackers in distributed database systems. In such an approach, its neighbors monitored each node's traffic and data communication decisions were made based on the traffic patterns and volume. Similarly, a number of trust based security models for computer networks have been proposed in the literature and some of them used trust in their routing protocols.

Hwang and Li [44] proposed a new trust model using an overlay network that is built over multiple data centers. The main aim of their model uses to implement a reputation-based system for establishing trust between

Table 3: Comparative Analysis for trust mechanisms

Model	Network	Cloud	File System	Databases
Kai Hwang and Deyi Li (2010)	High	High	Low	High
Xiaoyong Li and Junping Du (2013)	High	High	Low	Medium
AyadBarsoum and Anwar Hasan (2013)	High	High	Medium	Medium
HaiyingShen and Guoxin Liu (2014)	High	High	Medium	High
Lan Zhou *et al.* (2015)	High	High	High	High

clients and data owners. Li and Du [45] proposed a Cloud based Trust model to analyze the history of services provided by the cloud provider. It helps the user to select a more trustworthy service provider in the web applications. Barsoum and Hasan [46] proposed a cloud-based storage method that supports outsourcing of dynamic data. In this model, the owner is capable of archiving and accessing the data stored by the client service provider. Their scheme enables the authorized users to ensure that they are receiving the most recent version of the outsourced data and helps to handle the data stored in remote systems.

Shen and Liu [47] proposed a new reputation management model for enhancing the security of cloud computing by recognizing the inter dependencies between resource management and reputation management modules. Zhou *et al.* [15] explained the trust issues in cryptographic RBAC systems for securing data storage in a cloud environment. Their trust models assist owners and roles to create flexible access policies and their cryptographic RBAC schemes ensure that the trust policies a reinforced in the cloud.

Table 3 shows the comparative analysis for various trust mechanisms over the different environments such as network, cloud, file system and databases. In this model, fuzzification and defuzzification are carried out using fuzzy membership values based on triangular membership. Here, the amount of trust is measured using three fuzzy qualitative variables namely “High”, “Medium” and “Low”. The range of membership values are 0 to 0.35 for “Low”, 0.3 to 0.65 for “medium” and 0.6 to 1.0 for “High”. The trust values are computed based on network communication metrics namely packet drop ratio, bandwidth consumption and error rate. In addition, rules are used to find out trust values provided by the neighbors.

From Table 3, it can be observed that cloud based trust management system with role based access control model is more suitable to enhance the security of cloud databases.

Berger *et al.* [48] provided an extend version of their security model by using access control policy and security labels for implementing a prototype management system. Their model provides constraint satisfaction facility for implementing the integrity and security of the system. Moreover, they designed a hierarchical model for trust management and hence their model can be applied for applications of different complexity. Lin Guoyuan *et al.* [49] developed an access control model for the data stored in the cloud by proposing a trust based access control technique. In their model, they focused on mutual trust, user behaviour and mechanism for handling uncertainty, properties of dynamism and the issues in data distribution. They also developed a weight-based model for trust management and performed optimization using Ant colony optimization techniques. Their model is unique in nature due to the dynamic access control policies proposed and applied in their work.

Talal *et al.* [50] explained that cloud computing is an important and useful technology. Therefore, it can provide many services to the business community. One of the challenges in cloud data management is the maintenance of security. According to them, the security goals can be achieved through trust management. For this purpose, they proposed a framework for analyzing the merits and demerits of trust management systems. Their model is a useful contribution since it provides an innovative solution for maintaining security using privacy, trust and personalization. In another work by Talal *et al.* [51], the authors described about a reputation based security framework that uses trust management was proposed for enhancing the cloud security. They called their model as Cloud Armor and they included trust as special types of service provided by the cloud in addition to the platform, software and infrastructure. They also proposed a new protocol that uses user feedbacks for enhancing the privacy. They compared the services provided by normal users and malicious users.

Proposed Work: In this paper, we propose a new algorithm called Intelligent Secured Location based Log Management Algorithm (ISLMA) which performs key generation, trust computation, encryption and log updation operations. For key generation, it generates a large prime number ‘p’ and sends it to a Trusted Key Distribution Centre (TKDC) along with the user id and IP address of the sender in the following format.

$$K1 = ID1 \parallel IPA1 \parallel p \quad (1)$$

where,
K1 = Initial Key
ID1 = User Identity
IPA1 = Internet Protocol address of the user computer.

Now, the TKDC generates a nonce N1 and selects a prime number 'q' and multiply them with 'p' to generate the key. It also sends the location of the data centre in which the user data can be stored and manipulated. The TKDC informs the database manager present in the specified location about the values of N1 and 'q' in encrypted form using Caesar Cipher [52] so that the database manager can decrypt and use the values of N1, p and q for verification. Now, the final key is generated by using the equation2.

$$K = ID1 \parallel IPA1 \parallel p \parallel N1 \parallel q \quad (2)$$

Now, the key will be verified by the service provider by taking last three components after checking the first two components and generates a final key by finding the multiplication modulo p value of N1 X q, which will be used to encrypt the data before it is stored in the storage space using the Hill Cipher [52]. It performs trust computation of each user using initial trust, historical trust and neighbor trust. If trust values are less than 0.5, the user is not allowed to store and retrieve any data from the cloud database.

The trust computation module initially computes the initial trust by assigning the value 0.1 by default. This initial trust is updated periodically based on the queries and transactions made by the user with the database systems. In addition, it computes the trust by considering the history of the user and the trust values obtained from other sites of the distributed database system called neighbors. The updated trust values are known as recent trust. There are two types of trusts namely initial and recent trust, which are represented by ITij and recent trust denoted by RT_{ij}. Moreover, the historical trust is computed by using initial trust, transaction behavior and recent trust and is denoted by HT_{ij}

$$HT(t)_{ij} = \alpha IT(t)_{ij} + \beta RT(t)_{ij} + STR/TTR \quad t_1 \le t \le t_2 \quad (3)$$

The weights α and β ($\alpha, \beta >= 0$, $\alpha > \beta$ and $\alpha + \beta = 1$) are assigned to BT_{ij} and CT_{ij}. Now the basic trust is computed using the relation represented by $SE_m(i, j)$.

where, STR is the number of successful transactions, TTR is the total number of transactions requested by the current user, α and β are constants to denote the weights. Here, t1 and t2 are the start time and end time of an interval in which the trust values are valid and t is the time at which the trust values are computed. Finally, recent trust is obtained by taking average between recent trust and historical trust as follows:

$$RT = (RT + HT) / 2 \; t_1 \le t \le t_2 \quad (4)$$

The steps of the proposed algorithm are as follows:

Intelligent Secured Location based Log Management Algorithm (ISLMA)

Phase 1: Log creation

Step 1: Begin transaction and start timer.
Step 2: Initialize the key values and trust values with 0.
Step 3: Apply rule and generate the complexity value of key based on application.
Step 4: Generate public and private keys
Step 5: Compute trust based on history and neighbor information.
Step 6: Perform encryption using Elliptic key cryptographic algorithm [52]
Step 7: Store the encrypted data in the database log.
Step 8: Perform transaction update in the database.
Step 9: Write transaction 'Commit' or 'Abort' record.
Step 10: End transaction and close timer.

Phase 2: Log maintenance

Step 1: Read the first record from the log
Step 2: Read timestamp values
Step 3: Identify the user and the application using the log.
Step 4: Update the trust values based on current user activity.
Step 5: Perform recovery-using Redo and Undo operations
Step 6: Perform decryption of data records
Step 7: Apply location and temporal constraints
Step 8: Provide data to the user based on location.

This algorithm works in two phases namely log creation phase and log maintenance phase. In the first phase, log is created and it follows the deferred mode of log-based recovery techniques used in relational databases in combination with the two-phase commit

protocol for transaction failure recovery. In the log creation phase, it starts a timer and generates a key. In addition, it performs trust computation in the distributed transaction management environment by taking the opinion of all the participating nodes on building a trust model by adding the historical trust with the neighbor trust values. For each type of trust and application, requirement separate types of keys are generated using Elliptic Curves. In the phase one of the algorithm, the log details are encrypted and stored in the transaction log along with location details and time information. In the phase two of this algorithm, trust values are updated by applying the user behavior values obtained from current transactions. In addition, recovery operations are performed based on log based recovery techniques with decryption of data and by checking the location and temporal constraints. The main advantage of this algorithm is that it provides a facility for secured and dynamic storage of log data and to perform transaction recovery with higher security.

RESULTS AND DISCUSSION

The experiments have been carried out with five business applications namely Book sales, Apparel sales, Mobile sales, Computer sales and Food item sales. All these applications have very large volume of data with wide varieties of items and hence stored in MongoDB. The transactions were executed with two-phase commit protocol and log based recovery techniques for relational databases. The same experiments were carried out with the proposed algorithm and the results are obtained.

Figure 1 shows the security analysis for the existing two-phase commit approach and the proposed secured log management algorithm. We have considered five different applications for evaluating the performance of the proposed algorithm in cloud environment.

From Figure 1, it can be observed that the performance of the proposed algorithm is better when compared to the existing two phase commit protocol with respect to the security of data based on storage and retrieval. In addition, it considers the recovery of data during failures.

Figure 2 depicts the access control analysis for the access control for user level data management when the applications were executed using log based recovery in combination with transaction processing using two-phase commit protocol and the proposed algorithm.

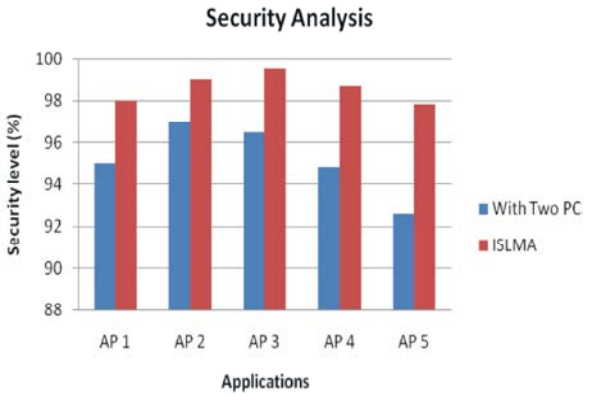

Fig. 1: Security Analysis

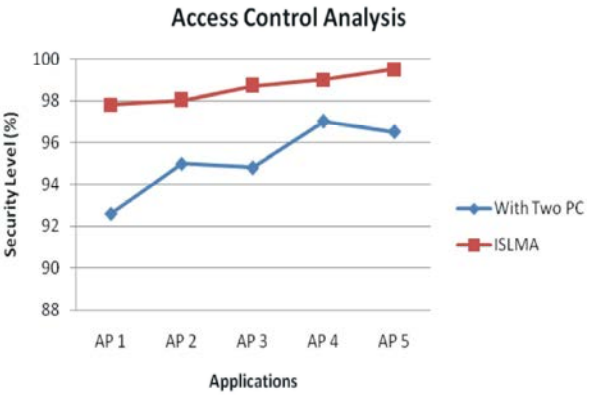

Fig. 2: Access Control Analysis

From Figure 2, it has been noticed that the security level of the database log maintenance is higher when compared to the role based access control model used in the existing database management systems. This is due to the fact that the existing relational databases follow the access control hierarchy based on user roles. On the other hand, the propsoed algorithm not only considers the user roles but also the trust values, key values and application types to enhance the security.

All the security models available in the literature were considered in the design of this algorithm and every work available in the literature were compared with the two-phase commit protocol with log-based recovery. Most of these algorithms provided same level of security or showed only a slight improvement over the existing algorithms. The reason for that lies in many factors including the application type, spatio-temporal constraints and data volume and trust values. On the other hand, the proposed model provides enhanced security when it is compared with the existing works on access control and log based recovery.

Conclusion and Future Work: In this paper, a survey on related work on three areas of cloud security namely access control, intrusion detection systems and trust management systems, which are based on computational intelligence techniques namely intelligent classification using fuzzy rules, use of intelligent agents for cloud network monitoring and the use of genetic algorithms for rule optimization, are used. In addition, an intelligent log management system is proposed for improving the data security in cloud. An analysis on the existing work shows that computational intelligence techniques are more useful for enhancing the cloud security. The salient feature of this survey is the use of qualitative analysis rather than quantitative analysis for making the comparison of related work. Further work in this direction can be the inclusion cryptographic techniques and security proof methods that use mathematics analysis for providing effective proof methods for cloud security.

REFERENCES

1. Damiani, E., S.C. di Vimercati, S. Paraboschi and P. Samarati, 2000. Securing XML Documents. In Proceedings of the International Conference on Extending Database Technology, (pp: 121-135), Konstanz, Germany.
2. Damiani, E., S.C. diVimercati, S. Paraboschi and P. Samarati, 2002. A Fine-Grained Access Control System for XML Documents. ACM Transactions on Information and System Security, 5(2): 169-202.
3. Bhatti, R., J.B.D. Joshi, E. Bertino and A. Ghafoor, 2003. Access Control in Dynamic XML-Based Web-Services with XRBAC. In Proceedings of the First International Conference on Web Services, Las Vegas, pp: 23-26.
4. Huang, X., H. Wang, Z. Chen and J. Lin, 2006. A Context Rule and Role Based Access Control Model in Enterprise Pervasive Computing Environment. In Proceedings of the International Symposium on PC and Applications, (pp: 497-502).
5. Mohan, S., A. Sengupta and Y. Wu, 2006. A Framework for Access Control for XML. ACM Transactions on System and Information Security, 5: 1-38.
6. He, H. and K.R. Wong, 2000. A Role Based Access Control Model for XML Repositories. In Proceedings of the First International Conference on Web Information Systems Engineering, 1: 138-145.
7. Liu, M., H. Guo and J. Su, 2005. An Attribute Based Access Control Model for Web Services. In Proceedings of the International Conference on Machine Learning and Cybernetics, 18(21): 1302-1306.
8. He, J. and J. Le, Apply the Technology of RBAC and WS-Security for Secure Web Services Environment in Campus. In Proceedings of IEEE International Conference on Machine Learning and Cybernetics, pp: 4406-4411.
9. Sandhu, S.R., J. Edward Coynek, L. Hal Feinsteink and E. Charles Youmank, 1996. Role-Based Access Control Models. IEEE Computer, 29(2): 38-47.
10. Li, N., V. Mahesh and Tripunitara, 2006. Security Analysis in Role-Based Access Control. ACM Transactions on Information and System Security, 9(4): 139-420.
11. Bertino, E., P.A. Bonatti and E. Ferrari, 2001. TRBAC: A Temporal Role-Based Access Control Model. ACM Transactions on Information and System Security, 4(3): 191-233.
12. James, B.D., E. Joshi Bertino, U. Latif and A. Ghafoor, 2005. A Generalized Temporal Role-Based Access Control Model. IEEE Transactions on Knowledge and Data Engineering, 17(1): 4-23.
13. Cui, X., Y. Chen and J. Gu, 2007. Ex-RBAC: An Extended Role Based Access Control Model for Location-Aware Mobile Collaboration System. In Proceedings of Second International Conference on Internet Monitoring and Protection, pp: 36-41.
14. Li, F., W. Wang, Jianfengna and H. Su, 2010. Action-Based Access Control for Web Services. Journal of Information Assurance and Security, 5: 162-170.
15. Zhou, L., V. Varadharajan and M. Hitchens, 2015. Trust Enhanced Cryptographic Role-Based Access Control for Secure Cloud Data Storage. IEEE Transactions on Information Forensics and Security, 10(11): 2381-2395.
16. Barker, S., 2008. Access Control by Action Control. In Proceedings of the 13th ACM Symposium on Access Control Models and Technologies (SAGMAT), pp: 143-152.
17. Taeho Jung, Xiang-Yang Li, Zhiguo Wan and Meng Wan, 2015. Control Cloud Data Access Privilege and Anonymity with Fully Anonymous Attribute-Based Encryption. IEEE Transactions on Information Forensics and Security, 10(1): 190-199.

18. Muthurajkumar, S., S. Ganapathy, M. Vijayalakshmi and A. Kannan, 2015. Secured Temporal Log Management Techniques for Cloud. Procedia Computer Science, 1(46): 589-595.
19. Xuanxia Yao, Huansheng Ning, Laurence T. Yang and Yang Xiang, 2015. Anonymous Credential-Based Access Control Scheme for Clouds. IEEE Cloud Computing, pp: 34-43.
20. Zubair A. Baig, Sadiq M. Sait and Farid Binbeshr, 2016. Controlled access to cloud resources for mitigating Economic Denial of Sustainability (EDoS) attacks. Computer Networks, 97: 31-47.
21. Tsz Hon Yuen, Joseph K. Liu, Man Ho Au, Xinyi Huang, Willy Susilo and Jianying Zhou, 2015. K-Times Attribute-Based Anonymous Access Control for Cloud Computing. IEEE Transactions on Computers, 64(9): 2595-2608.
22. Lan Zhou, Vijay Varadharajan and Michael Hitchens, 2015. Trust Enhanced Cryptographic Role-Based Access Control for Secure Cloud Data Storage. IEEE Transactions on Information Forensics and Security, 10(11): 2381-2395.
23. Massimo Ficco and Massimiliano Rak, 2015. Stealthy Denial of Service Strategy in Cloud Computing. IEEE Transactions on Cloud Computing, 3(1): 80-94.
24. Yasir Mehmood, Ayesha Kanwal, Muhammad Awais Shibli and Rahat Masood, 2015. Distributed Intrusion Detection System using Mobile Agents in Cloud Computing Environment. Conference on Information Assurance and Cyber Security, pp: 1-8.
25. Xinfeng Ye. (2016). Privacy Preserving and Delegated Access Control for Cloud Applications. *Tsinghua Science and Technology*, *21*(01), 40-54.
26. Hui Ma, Rui Zhang and Wei Yuan, 2016. Comments on Control Cloud Data Access Privilege and Anonymity with fully Anonymous Attribute-Based Encryption. IEEE Transactions on Information Forensics and Security, 11(4): 866-867.
27. Joseph K. Liu, Man Ho Au, Xinyi Huang, Rongxing Lu and Jin Li, 2016. Fine-Grained Two-Factor Access Control for Web-Based Cloud Computing Services. IEEE Transactions on Information Forensics and Security, 11(3): 484-497.
28. Mansour, N., M. Chehab and A. Faour, 2010. Filtering intrusion detection alarms. Cluster Computing, 13(1): 19-29.
29. Amjad Hussain, Bhat Sabyasachi and Patra Debasish Jena, 2013. Machine learning approach for intrusion detection on cloud virtual machines. International Journal of Application or Innovation in Engineering & Management (IJAIEM), 2(6): 57-66.
30. Zubair, Baig, A., Sadiq, M. Sait Abdul, Rahman and Shaheen, 2013. GMDH-Based networks for intelligent intrusion detection. Engineering Applications of Artificial Intelligence, 26: 1731-1740.
31. Louvieris, P., Natalie, Clewley, Xiaohui and Liu, 2013. Effects based feature identification for network intrusion detection. Neurocomputing, 121: 265-273.
32. Reda, M., Elbasiony, Elsayed, A. Sallam, E. Tarek, Eltobely, M. Mahmoud and Fahmy, 2013. A hybrid network intrusion detection framework based on random forests and weighted k-means. Aim Shams Engineering Journal, 4(4): 753-762.
33. Koc, L., T.A. Mazzuchi and S.A. Sarkani, 2012. Network intrusion detection system based on a hidden naive bayes multiclass classifier. Expert Systems with Applications, 39: 13492-13500.
34. Hasani, S.R., Zulaiha, Ali, Othman, Seyed, Mostafa Mousavi and Kahaki, 2014. Hybrid feature selection algorithm for intrusion detection system. Journal of Computer Science, 10(6): 1015-1025.
35. Gisung Kim, Seungmin Lee and Sehun Kim, 2014. A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. Expert Systems with Applications, 41(4): 1690-1700.
36. Yan, Q.F., R. Yu, Q. Gong and J. Li, 2016. Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues and Challenges. IEEE Communications Surveys and Tutorials, Article in Online.
37. Xiao, Z. and Y. Xiao, 2013. Security and Privacy in Cloud Computing. IEEE Communications Surveys & Tutorials, 15(2): 843-859.
38. Tanzim Khorshed, A.B.M., A. Shawkat and S.A. Wasimi, 2011. Trust Issues That Create Threats for Cyber Attacks in Cloud Computing. In Proceedings of IEEE 17th International Conference on Parallel and Distributed Systems, pp: 900-905.
39. Kulothungan, K., S. Ganapathy, S. Indira Gandhi, P. Yogesh and A. Kannan, 2011. Intelligent secured fault tolerant routing in wireless sensor networks using clustering approach. International Journal of Soft Computing, 6(5): 210-215.

41. Anand, K., S. Ganapathy, K. Kulothungan, P. Yogesh and A. Kannan, 2012. A rule based approach for attribute selection and intrusion detection in wireless sensor networks. Procedia Engineering, 38: 1658-1664.
42. Ganapathy, S., P. Yogesh and A. Kannan, 2012. Intelligent Agent based Intrusion Detection System using Enhanced Multiclass SVM. Computational Intelligence and Neuroscience, pp: 1-9.
43. Sannasi Ganapathy, Pandi Vijayakumar, Palanichamy Yogesh and Arputharaj Kannan, 2016. An Intelligent CRF Based Feature Selection for Effective Intrusion Detection. International Arab Journal of Information Technology (IAJIT), 13(1): 44-50.
44. Hwang, K. and D. Li, 2010. Trusted Cloud Computing with Secure Resources and Data Coloring. In Proceedings of IEEE Internet Computing, pp: 14-22.
45. Li, X. and J. Du, 2013. Adaptive and Attribute-Based Trust Model for Service Level Agreement Guarantee in Cloud Computing. IET Information Security, 7(1): 39-50.
46. Barsoum, A. and A. Hasan, Enabling Dynamic Data and Indirect Mutual Trust for Cloud Computing Storage Systems. IEEE Transactions on Parallel and Distributed Systems, 24(12): 2375-2385.
47. Shen, H. and G. Liu, 2014. An Efficient and Trustworthy Resource Sharing Platform for Collaborative Cloud Computing. IEEE Transactions on Parallel and Distributed Systems, 25(4): 862-875.
48. Berger, S., J. Thomas, R. Hawthorne Caceres, K. Goldman, D. Pendarakis, *et al.*, 2009. Security for the cloud infrastructure: Trusted virtual data center implementation. IBM Journal of Research and Development, 53(4): 1-12.
49. Lin Guoyuan, Wang Danrul, Bie Yuyul and Lei Min, 2014. MTBAC: A Mutual Trust Based Access Control Model in Cloud Computing. China Communications, pp: 154-162.
50. Talal H. Noor, Quan Z. Sheng, Lina Yao, Schahram Dustdar and Anne H.H. Ngu, 2016. CloudArmor: Supporting Reputation-Based Trust Management for Cloud Services. IEEE Transactions on Parallel and Distributed Systems, 27(2): 367-380.
51. Talal H. Noor, Quan Z. Sheng, Zakaria Maamar and Sherali Zeadally, 2016. Managing Trust in the Cloud: State of the Art and Research Challenges. Computer, pp: 34-45.
52. William Stallings, 2013. Cryptography and Network Security. Fifth Edition, Pearson Education.