Deep Learning Approach for Enhancing the Security of Data using Edge Computing for Secure Cloud Data Storage

P.Jenifer[1], Muthu Absara[2], Sathya[3], Sri Rajalakshmi[4]

[1]P.Jenifer, AP/CSE, Francis Xavier Engineering College (Autonomous),
[2,3,4]Muthu Absara, Sathya, Sri Rajalakshmi, UG Scholars, CSE Department,
Francis Xavier Engineering College(Autonomous)

---***---

Abstract**—** *The trust evaluation systems, all feedback ratings on a service are usually exploited to evaluate their reputation. Although these methods are simple and effective, they cannot cope well with the impact of malicious users to improve the accuracy of the reputation assessment model of cloud services and mitigate the impact of reputation attacks initiated by malicious users. Internet of Things (IoT) plays a vital role almost in every field of engineering. Now days, almost every system has adopted this technology due to its ease in access, design and development. However the technology still suffers from the issues of available resources for computing of huge amount of IoT data. In order to solve these issues, it is necessary to adopt trustworthy cloud based architecture. The trust level calculation of these cloud services is a challenging task. In this paper, we have developed a triple integrated assessment for the trust evaluation of a cloud network. This assessment has been carried out using the three major parameters i.e. security, privacy and reputation. Security assessment of the cloud service has been carried out using the security metrics like security controls deliverable. The privacy assessment is evaluated using the Privacy Impact Assessment(PIA) tool. Finally the reputation assessment of the cloud network is carried out using the reputation of it's cloud services. Experiments are carried out on different real - world web service datasets which shows that the proposed assessment model works efficiently than all other assessment models.*

Index Terms — Cloud services, IoT, Privacy Impact Assessment, Privacy and Reputation assessments.

INTRODUCTION

Google introduced the concept of cloud computing in 2006. The cloud computing center uses virtualization technology to organize a large number of idle resources, forming a huge "virtual resource pool", and users can request personalized cloud services through the network. As the scale of cloud services continues to expand, more and more service providers provide services with similar functions and different quality of services. Users select the most suitable cloud services from among many cloud services. In a cloud environment, trust is subjective and dynamic and is influenced by many factors. In today's increasingly competitive environment, the highly scalable technology of cloud services brings vitality to enterprises, and it also challenges users' trust in cloud services. At present, the trust problem of cloud computing is the most concerned issue of most enterprises, and it is difficult to select cloud services. Therefore, it is important to study and establish an effective and objective trust model to improve user satisfaction and interaction success rate

Assurance of secure applications and services in wireless networks relies on the properties of confidentiality. And integrity, correspondingly defined as the ability to keep data secret from unauthorized entities and the ability to verify that data has not been maliciously or accidentally altered. Nowadays, they unruly minutes are accomplishment since regular tragedies to hateful attacks that can radically teamwork the network's ability to meeting this one quality-of-service. Infrastructures in many networks such as telecommunication, transportation networks and power grid systems are highly interdependent and sensitive to both random failures and deliberate attacks. In fact, the fiascos of a small number of nodes may lead to a complete breakup of a network system and severely disrupt the network connectivity. Real-world examples include the unplanned annihilation of fibercables by dragging anchors, malicious cyber-attack to Internet Autonomous Systems and terrorist attacks targeting infrastructures in electrical power grids and highway systems [1]. Therefore, it is essential to judge the network defence lessens to those fatal failure schemes before they happen. There have been abundant efforts on propositioning evaluation measures of the network vulnerability, as summarized. However, these events can neither be rigorously mapped to the overall network connectivity, nor reveal the set of most critical vertices and edges, thus are not suitable to assess the network weakness in terms of connectivity [2]. To facilitate the search for critical infrastructures in networks regarding network connectivity, a new assessment method has-been proposed in form of an optimization problem, so-called -vertex disruptor. The network vulnerability was measured through the least number of nodes that removal incurs a certain level of disorder in the objective network. Extensive experiments on both synthetic and real networks showed that the new assessment method outperforms the traditional ones and successfully identifies small subsets of critical nodes that failures lead to the network wide fragmentation. In addition, the flexibility in selecting the level of disruption assessing vulnerability at multiple disruption levels, providing a complete network vulnerability spectrum [3]. To solve the -vertex disruptor problem, which was shown to be an NP-hard problem, the authors proposed a pseudo-approximation algorithm that can guarantee the performance of the optimal solutions. Despite that the algorithm is of theoretical interests, it has high time complexity and is difficult to be implemented efficiently. Besides designing algorithms with performance guarantees, the -vertex disruptor problem can be formulated using integer programming (IP) and solved for the exact solutions by branch-and-cut methods, which consist of a combination of a cutting plane method with a branch-and-bound algorithm. The same approach has been applied for the critical nodes (Edges) detection problems that seek for a set of k nodes (edges) that removal maximizes the disruption in the residual network [4]. Unfortunately, even for small network instances all proposed formulations become very large integer programming problems that consume excessive amount of memory and time to converge. For example, the largest reported instance with 150 nodes consists more than one million constraints. Moreover, solving those integer programming problems relied solely on the general edition of the branch-and-cut algorithm implemented in the optimization packages that are not tailored to those specific problems [5].

With the advancements in the computer technology, the internet has become an integral part of the human's life. The user requirements of internet are also increased tremendously with the increasing internet applications and data services. In order to meet these challenges the Internet Service Provider (ISP) has to deploy more number of storage devices and processing modules. The synthesized dataset comprises security metrics that were derived from the cloud SLAs. The response time (RT) and the throughput (TP). For objectivity and convenience, we randomly select 6 services within 10 different time slices and identify the feedback ratings

The drawbacks of Internet Service Providers are that the requirement of very costly memory storage, personnel management and equipment maintenance. These problems have been addressed and resolved by the cloud computing technology [1 - 3]. Cloud computing is the distributed computing system which divides its tasks among the different computers using the wide spread internet platform. This technology finds the benefits like efficient resource allocation and utilization and providing fast, efficient, and inexpensive computing methods to the different real world

The cloud computing offers dynamic scalable resources provided as a service over the internet. It has several advantages than the convention method of computation, i.e. in terms of high reliability, very large scale service, on –demand and low cost. The classification [4 - 6] of the cloud depends on the physical location of the user. Private clouds [7 - 9] are installed within the user's location whereas the public clouds are provided by the third party service providers. These public clouds require high level of trustworthiness in terms of security and privacy. It becomes a challenging task for the organizations since security and privacy should be provided in parallel with any services. A good assessment model is necessary to evaluate the trust level in these public clouds.

PROBLEM STATEMENT

A key-aggregate encryption scheme consists of five polynomial-time algorithms as follows. The data owner establishes the public system parameter via Setup and generates a public/master-secret3 key pair via KeyGen. Messages can be encrypted via Encrypt by anyone who also decides what cipher text class is coupled with the plaintext message to be encrypted. The data owner can use the master-secret to generate a collection decryption key for a set of cipher text classes via Extract. The generate keys can be passed to delegates securely (via secure e-mails or secure devices) finally any user with an aggregate key can decrypt any cipher text provided [6.7].

LITERATURE REVIEW

In the paper [10], by V. Varadharajan and U. Tupakula proposed architecture of secure services for multi-tenant cloud networks. This architecture follows the security policies of tenant domains and trusted virtual domains. The authors have described the different methods for the detection of attacks among the virtual machines, malicious, DNS, database and web server attacks. Also the authors have addressed the security policies related to the trusted virtual domain management, forensic analysis, detection of malicious entities and restoration.

In the paper [11] by Y. Wang, et al., have proposed a dynamic cloud services trust level evaluation architecture using service level agreement (SLA) and privacy considerations. In this method, trust level is evaluated based on the direct, indirect and reputation trust. An SLA will be selected depending on the QoS parameter which is decided by the SLA. User data is protected using the data protection model. Experimentation has been carried out on the public datasets which shows the architecture provides better services with less malicious interference also with good accuracy and feasibility.

In the paper [12], by J. Luna, et al., have developed QPT and QHP models for security level assessment of a CSP. This helps in improving the security requirement specification which allows the users to identify and represent the security needs. Validation of this model was achieved using the case scenarios and prototypes, leveraging the real world CSP secSLA data, Trust and Assurance Registry. There are many challenges and risks are involved in the implementation of cloud services.

The novelty in the cloud computing for the business services can lead to the consumer perceptions of uncertainty. There exist the different reasons for the uncertainty like lack of trustworthiness and the poor QoS of service providers. To resolve these problems, the authors Vincent C. E., Kaniz F., et al., have proposed a trust label system [13]. This novel system communicates the trustworthiness of the CSPs. Experimentation was carried out on use case scenario to compute the trust level of CSPs.

In the paper [14], the authors R. Nagarajan, et. al., have proposed a novel system for the evaluation of trustworthiness and QoS of cloud services using the fuzzy logic model. This model was implemented using the customer's feedback. Using this model, weights are assigned for the different feedback element. The trust level is predicted using the fuzzy goal, constraints and user feedbacks in this model.

The block diagram of assessment of trustworthy cloud services for IoT security is shown in figure 3.1. The proposed system model consists of triple integration of security, privacy and reputation based assessments.

i. Security based Assessment

The security assessment model consists of Cloud Service Providers(CSP) and security metrics like facility security, risk management, information security. Here, the security metrics are defined in the form of deliverable template by the Cloud Service Customers(CSCs). And these templates are called as the security controls deliverable(SCD)

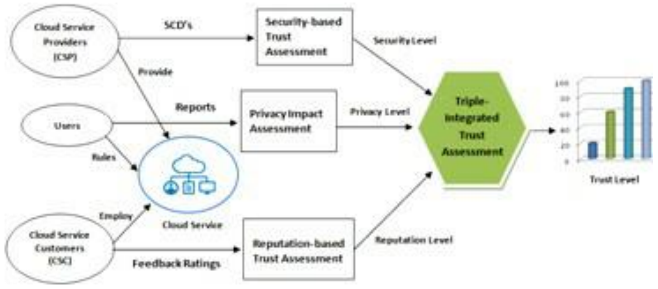
Cloud Service Providers (CSP)
SCD's
Security-based Trust Assessment
Security Level
Provide
Users
Reports
Privacy Impact Assessment
Privacy Level
Triple-Integrated Trust Assessment
Rules
Employ
Cloud Service
Cloud Service Customers (CSC)
Feedback Ratings
Reputation-based Trust Assessment
Reputation Level
100
80
60
40
20
0
Trust Level

Fig. 3.1: Assessment of Trustworthy Cloud Services: Triple Integration of Security, Privacy and Reputation model

a). Standardization: SCD is used as the standardization which defines the security controls to implement in the cloud services of the respective CSP. The security metrics of this standardization fulfil the requirements of CSCs. Many of these metrics are already defined by the security standards like CSA, FedRAM, NIST, ISO/IEC. Different security metrics are selected from the existing standards to develop the SCD. These security metrics ensure that CSC's are comfortable using the secure cloud service.

b). Conformity: The CSP is responsible to measure and verify the security controls of the SCD. Also it fills the SCD upon the conformity between the metrics and the control parameters. It is assumed that the conformity between security metrics and security capability of CSP, are true and credible. This parameter helps in evaluating the security level of the cloud service.

i. Privacy Impact Assessment (PIA)

Along with the security and reputation of the cloud services the privacy also an important parameter to be considered in the evaluation process of trustworthiness. Here the PIA tool gives the complete assessment of a particular cloud service. It studies and analyses the privacy risks and compliances to aware the unskilled users/organizations. So that users can identify those risks at an early stage and avoid them if they are the potential risks. These PIA tools are inserted in the cloud which can be accessed from the web browser. For this purpose, it uses Software as a Service (SaaS) model. This model can be used as on payment basis. Also it helps in generating the PIA reports. It also includes security models to protect the confidential information.

Trust Evaluation Process

The comprehensive trust consisted of the direct trust, recommendation trust, and reputation. The direct trust relationship means that both sides have historical interaction experience. Recommended trust has no historical interaction of both interactive experiences; relevant factors include the degree of similarity recommendation respondents and the level of the respondents. The reputation represents the evaluation of all the cloud service users.

The specific steps of the trust evaluation are as follows.

Step 1 (register). Cloud service provider resources are registered by CSAPI.

Step 2. Request.

Step 3 (calculate the comprehensive trust CST). History interaction records are inquired by the cloud trust management center. A gray relational analysis method is used to calculate the similarity recommended trust and get the recommended trust RT, and the reputation of is calculated by all users of the cloud service. Meanwhile, three different types of trust are assigned different weights for evaluation.

Step 4. If CST≥θ, indicating that the service meets the requirements of the user, go to Step 5; otherwise, if the cloud service does not meet the user requirements, please go to Step 2.

Step 5. Users select the cloud service with the highest CST.

Step 6. Update the direct trust according to formula (30).

Related Work

In the prior work, they have focus only on the centrality measurements. It income measuring the degree, between's and closeness centralities. In the prior work, they concentrate only to identify either the critical nodes or critical links. In other prior work, they judge the multiple attacks which happen at both links and nodes at the same time. The other prior work does not work well when the network connectivity is of soaring priority. In the other prior work, they proved that the critical node detection problem is also the NP-complete problem on trees for the total biased pair wise connectivity metric.

System Architecture

In the proposed system they considered the framework in presence of both node and link attack. They initially proposed an algorithm called JLNA which is used to reduce the β-disruptor problem. But they have used the sparse cut method which has more unwanted cuts. Hence they propose an algorithm called hybrid meta-heuristic (HMM) algorithm. It is used control the difference between the connectivity in the residual graph and the target connectivity. In the proposed system we attain the reconstructed network to attain the maximum transmission without loss of the data and time consumption for the transmission. Here the process takes place with the high link cost and the less distance between the each transmission nodes.

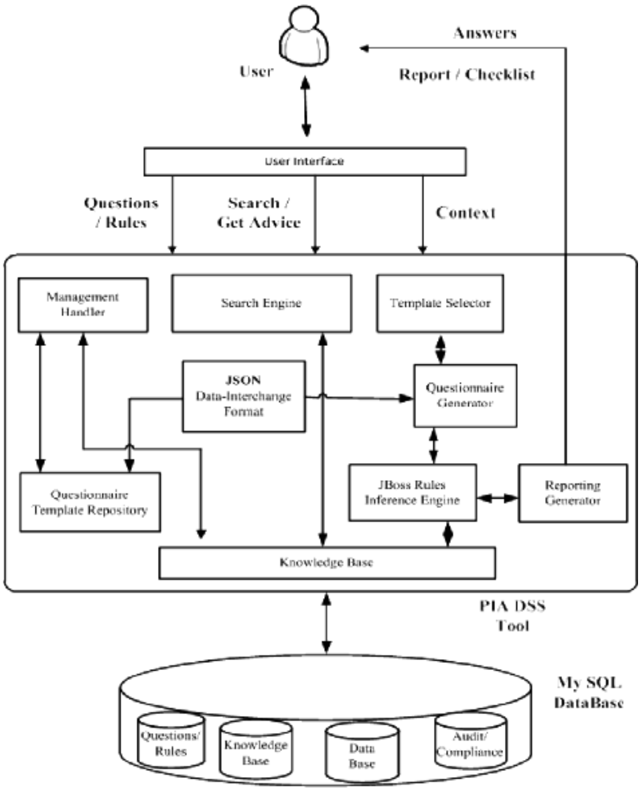

Fig. 3.2: Privacy Impact Assessment tool

The main components of the PIA tool and storage services with the cloud provider are shown in fig. 3.2. It will be deployed in the cloud as a service which is available for the third party users. In this model, end user (customer) fills the answers to the questions to generate the PIA report whereas the domain expert creates and maintains the KB. A web based user interface is provided for the end user to interact with this tool. Different templates and contexts are used to generate the questions and answers. It uses the JBoss rules to make the inference by deciding which rules are satisfied and assigns the priority to it. In this approach forward chaining method is used to search the inference rules.

This PIA tool generates the report as an output which is based on the answers of the end users. This report is helpful in evaluating the assessment and audit analysis of the cloud services. This tool is accessible for the customers as an application through their web browser. This kind of tools can be deployed in the public, private and hybrid clouds to analyse the privacy and security features of the particular cloud.

ii. Reputation based Assessment

In this assessment approach, the feedback ratings of the cloud services are reported by the CSC. This feedback depends on the quality of services.

The feedback rating is calculated with the help of a multi-tuple (C_{id},S_{id},S_{id}(A_{id}),F,Δt).

C_{id}⍰Identity of CSC

S_{id}⍰ Identity of cloud services $S_{id}A_{id}$⍰ Cloud service attribution F⍰ Feedback rating

Δt⍰ time duration of service

These multi-tuples represent the feedback report of the cloud services. Each feedback report plays an important role in evaluating the trustworthiness of cloud service.

If the transaction is successful, it is , the transaction failure is , and the number of failures is indicated by n. In order to prevent the problem of small amount of transaction fraud, the transaction amount is considered. The trust value will be decreased rapidly in the transaction failures by the acceleration factor, so that once the main trading promises to each other, their trust values will decline rapidly.

RESULTS

The experimentation and the results are carried out using the Visual Studio and SQL tool. Approximately six CSPs with 142 users, 4,500 web services are considered for evaluation. The Quality of Service parameters like response time and throughput are considered for the analysis. Over 6 services in 10 different time slices and the feedback ratings from the 100 users considered as the for experimentation. Each service is assigned to the each CSP for the trust assessment. These datasets with security metrics and real world web services are used to validate the methods of Security based Trust Assessment (SeTA) and Reputation based Trust Assessment (ReTA), respectively. The security level, reputation level and the privacy level are combined to calculate the trust level of a CSP. These are calculated using SeTA, ReTA and PIA tools as shown in figure 4.1. In this, CSP3 has the more security level than CSP6, while CSP6 has the more reputation level than CSP3. So therefore, CSP3 has higher trust level than CSP6. Aggregate of these results gives the overall trustworthiness

CSP	SeTA	ReTA	PIA
CSP1	0.78	0.4	0.62
CSP2	1	0.41	0.82
CSP3	0.42	0.24	0.4
CSP4	0.36	0.23	0.3
CSP5	0.5	0.38	0.48
CSP6	0.41	0.3	0.4

Figure 4.2: The assessment results Integrated Trust Assessment model

CONCLUSION

Due to the rapid increase of cloud service providers, the trustworthiness evaluation of cloud services has become an important issue. In this paper, we have discussed the importance of the trustworthiness of the cloud services. We have developed a triple integrated assessment for the trust evaluation of a cloud network. This assessment has been carried out using the three major parameters i.e. security, privacy and reputation. Security assessment of the cloud service has been carried out using the security metrics like security controls deliverable. The privacy assessment is evaluated using the Privacy Impact Assessment (PIA) tool. Finally the reputation assessment of the cloud network is carried out using the reputation of its cloud services. Experimentation results show that our proposed assessment model is efficient than all other assessment models.

REFERENCES:

1. R. Buyya, "Cloud computing: The next revolution in information technology, " 1st International Conference On Parallel, Distributed & Grid Computing, 2010, p. p. 02 - 03.

2. S. Chaisiri, Lee and Niyato, " Optimization of Resource Provisioning Cost in Cloud Computing, " in IEEE Transactions on Services Computing, volume 05, no. 02, p. p. 0164 - 0177, Apr - Jun - 2012.

3. C. Wang, Q. Wang, et al., " Toward Secure and Dependable Storage Services in Cloud Computing, " in IEEE Transactions on Services Computing, volume 05, no. 02, p. p. 0220 - 0232, Apr – Jun - 2012.

4. M. Thangapandyan and Anand, "A secure and reputation based recommendation framework for cloud services," IEEE International Conference on Computational Intelligence & Computing Research, Chennai, 2016, p. p. 01 - 04.

5. Yu Zhi - Yong, et al., "Research on service trust evaluation approach under cloud computing environment," 3rd International Conference on Cyberspace Technology, 2015, p. p. 01 - 05.

6. L. Wang et al., "A Trustworthiness Evaluation Framework in Cloud Computing for Service Selection," IEEE 6th International Conference on Cloud Computing Technology & Science, p. p. 0101 - 106.

7. S. Jeuk, Szefar and Zhiou, "Towards Cloud, Service and Tenant Classification for Cloud Computing, "Fourteenth IEEE/ACM International Symposium on Cluster, Cloud & Grid Computing, p.p. 0792 – 0801, 2014.

8. S. Jeuk, Salguero and Zhiou, "Universal Cloud Classification and its Evaluation in a Data Center Environment, "IEEE sixth International Conference on Cloud Computing Technology & Science, p. p. 0469 – 0474, 2014.

9. D. W. Chadwick, Liewens, Hartogh, Pashalides and Alhadef, " My Private Cloud Overview: A Trust, Privacy and Security Infrastructure for the Cloud, " IEEE Fourth International Conference on Cloud Computing, p. p. 0752 - 0753, 2011.

10. V. Varadharajan and Tupakula, " Securing Services in Networked Cloud Infrastructures, " in IEEE Transactions on Cloud Computing, volume 06, no. 04, p. p. 01149 - 01163, 1st October – December – 2018