Trustworthy Cloud Services for IoT Security: Triple Integration of Security, Privacy and Reputation

Amarnath J L, Pritam Gajakumar Shah, Chandramouli H, Arun Kumar S

Abstract—In this era of digital world, Internet of Things (IoT) plays a vital role almost in every field of engineering. Now a days, almost every system has adopted this technology due to it's 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, Trustworthy cloud, Security, Privacy and Reputation assessments.

I. INTRODUCTION

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 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 problems. As a result, the traditional computational models are replaced by the cloud computing models.

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.

II. 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.

Revised Manuscript Received on August 30, 2019.
* Correspondence Author

Amarnath J L*, Assistant professor, Computer Engineering, Research scholar at Vishveswaraya Technological University Belagavi.

Pritam Gajakumar Shah, Chief editor Australian journal of wireless technology mobility and security Canberra Australia, University of Canberra.

Chandramouli H, Professor, Department of Computer Science and Engineering, East Point College of Engineering and Technology, Bangaluru

Arun Kumar S, Assistant Professor, Department of Computer Science and Engineering, South East Asian College of Engineering and Technology, Bangaluru,

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.

III. SYSTEM 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).

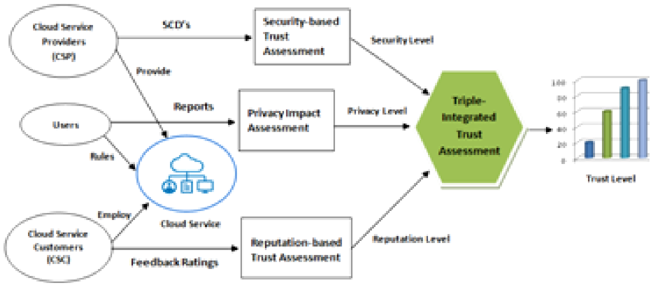
Cloud Service Providers (CSP)
SCD's
Security-based Trust Assessment
Security Level
Provide
Users
Reports
Privacy Impact Assessment
Privacy Level
Rules
Triple-Integrated Trust Assessment
Cloud Service
Employ
Cloud Service Customers (CSC)
Feedback Ratings
Reputation-based Trust Assessment
Reputation Level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

ii. *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.

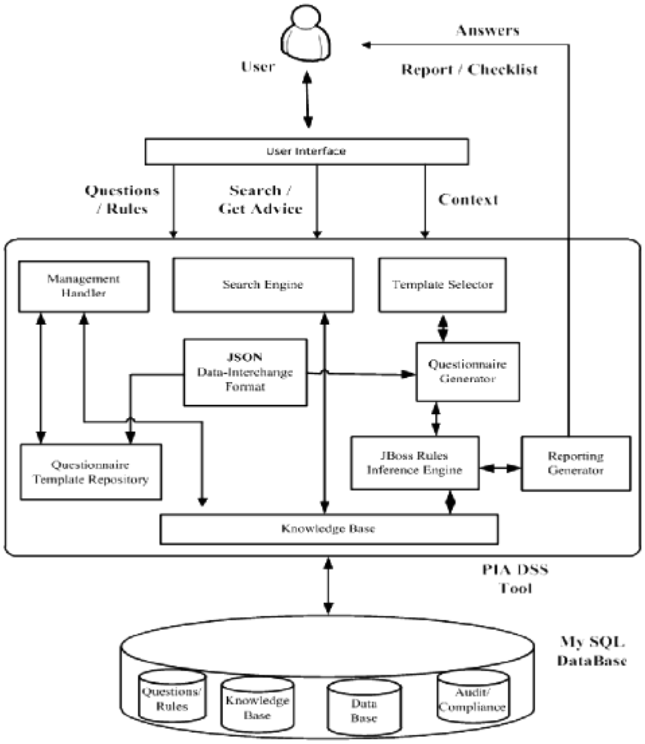

Fig. 3.2: Privacy Impact Assessment tool

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.

iii. 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 $(C_{id},S_{id},S_{id}(A_{id}),F,\Delta t)$.

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.

IV. RESULTS

The experimentation and the results are carried out using the MATLAB tool on the data sets WSdream from github server. 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. As a result, the dataset contains 6x100x10 entries. 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.

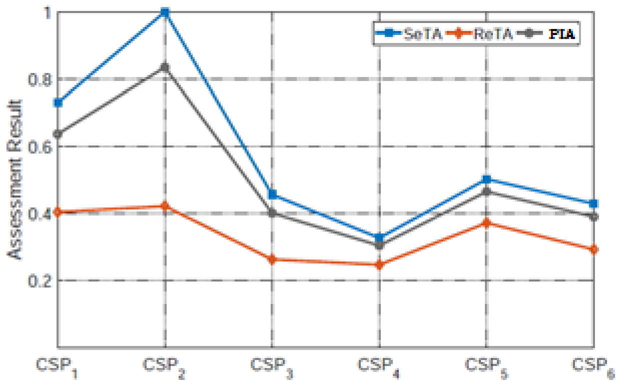

Figure 4.1: The assessment results Integrated Trust Assessment model

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

V. 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 it's 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, " 1^{st} *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.
11. Y. Wang, J. Wen, Zhiou and Leo, " A Novel Dynamic Cloud Service Trust Evaluation Model in Cloud Computing, " S*eventeenth IEEE International Conference On Trust, Security & Privacy In Computing & Communications*, p. p. 010 – 015, 2011.
12. J. Luna, et al., " Quantitative Reasoning about Cloud Security Using Service Level Agreements, " in *IEEE Transactions on Cloud Computing*, volume 05, no. 03, p. p. 0457 - 0471, 1st Jul. – Sept., 2017.
13. V. C. Emeakaroha, et al., " A Trust Label System for Communicating Trust in Cloud Services, " in *IEEE Transactions on Services Computing*, vol. 10, 2015.
14. R. Nagarajan, Selvamutukumaran and Tirunavukarasu, " A fuzzy logic based trust evaluation model for the selection of cloud services, " *International Conference on Computer Communication and Informatics*, p. p. 01 – 05, 2017.