International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 6 (2015) pp. 15747-15758

http://www.ripublication.com

Service Orient Approximation Technique Based Multi Attribute Encryption Standards For Intrusion Detection In Cloud Environment

A. MURUGAN, M.Sc., M.Phil.

Research scholar, Department of computer science, Vinayaka Missions University, Salem. muruganphd123@gmail.com

Dr. M. NITHYA, M.E., Ph.D.,

Research supervisor, Head of the department, Department of computer science, VMKV Engineering College, Salem.

Prof. Dr. A. NAGAPPAN, B.E., M.S., Ph.D.,

Principal, VMKV Engineering College, Salem.

ABSTRACT:

The cloud environment has various services at different levels of the architecture and the resources available at certain level of the architecture can be accessed through such service. The user data located at cloud data centers has to be provide public auditability where the access of data has to be restricted in many ways not only by encrypting the data at the clouds. There are many malicious threats been involved at any point of time to get access the cloud data in malformed manner or tries to spoil them by malware and so on. To overcome these issues of cloud security, I propose a service orient approximation technique which restricts the user access in many ways and uses multi attribute encryption standards for the cloud data to form an intrusion detection system to secure cloud environment from various threats. The user request being approximated based on the service requested and the approximation of the request is performed in many ways using number of factors like, the frequency of access, the user profile, the role in organization and many more. The proposed approach enforce an encryption standard based on number of attributes and the intrusion detection is performed using service approximation and encryption standards and user keys. Based on all these measures and variants the proposed approach maintains data auditability and

provides efficient security to the cloud resources. The proposed method increases the data security, auditability and reduces the complexity in user authentication and increases the efficiency of intrusion detection.

Key Terms: Cloud Computing, Data Auditability, Intrusion Detection, Service Orient Architecture, Data Encryption.

1. INTRODUCTION:

The cloud is an loosely coupled environment where the costly resources could be shared between users and the users could be allowed to access them on cost. In cloud the costly resource of any type like processing elements, memory units, or any documents of the organizations, databases could be deployed in the sense to share between users of the organizations. The maintenance of the cloud resource is costlier and the identity management also becomes higher burden task which needs more resource management criteria. To escape from such burden the resource providers simply deploy the resource in the cloud and let everything under the hands of service providers and third party audtitors. The third party auditor (TPA) is responsible for identity management which process all the user specific key which is provided by the key generator or the cloud service provider. Initially the service provider generates users keys and distribute them to the user as well as the TPA. On behalf of that the TPA verifies the identity of the user according to the key values submitted.

This general procedure has various flaws according to cloud security; there are many issues where the threats are increasing like spoofing, malware, botnet and so on. To overcome these issues of security there is a need of intrusion detection system to secure the cloud environment. The intrusion detection system is one which performs an analysis of the features of the request being received. Based on the features of the request or packet the trustworthy of the packet has to be identified before allowing the request to be processed. Sometimes the malicious uses are capable of clearing all the security check and access the privacy information. To provide more secure protocol, the intrusion detection system or the data enforcement has to be performed based on various attributes which challenges the malicious user and could not be obtained by them.

Data Auditability is the process of maintaining the originality that the modification performed by any user should reflect on the copy of others and each user has to get the feeling that they view the same and original information. In any service orient architecture, there may be N number of services available and to access each service there will be protocol enforced by the service providers. Similarly in our case the services could be accessed by the users upon clearing the trust protocol and the intrusion detection mechanism employs such enforcement and verifies the trustworthy of the user. Based on the result of intrusion detection system the user will be allowed to access the services available.

2. RELATED WORKS:

There are many approaches has been discussed earlier for the intrusion detection in service orient architecture. I discuss few of them here in this chapter.

The mOSAIC-Based Intrusion Detection Framework for Cloud Computing [1], maintains level based information of cloud services which are deployed at different levels using component based architecture. The method monitors various threats at different levels according to the symptoms available. The monitored information could be used on diagnosis analysis on intrusion detection in cloud environment.

A novel distribute intrusion detection system has been proposed in [2], which combines behavior orient mechanism as well as knowledge based intrusion detection mechanism. The first one uses the behavior of different users at the cloud which helps increase the performance of intrusion detection and the knowledge based approach works based on the rules provided to the intrusion detection system. However both the mechanism helps improving the performance of overall IDS to reduce the false positive and false negative results.

The Cooperative intrusion detection system framework for cloud computing networks [3], works in cooperative manner to perform intrusion detection. The nodes exchange different information about the attacks scenario and available alerts between them. The method uses agent technology to compute and distribute the alert messages. Also the agents are used to verify the alert messages from other nodes of the cloud. The method has produced efficient result than the snort IDS which runs with the support of predefined rule base.

In [6], service level agreement based security enforcement is defined for cloud. The method looks for the agreements at all the times while receiving any request from different users of the cloud. Based on the service level agreements the intrusion or misbehavior of any user is identified.

The Intrusion Tolerance of Stealth DoS Attacks to Web Services [7], has been proposed towards denial of service (DDOS) attacks. The method handles the low flow rate attacks which intend to override the rate control mechanisms while sending large amount of data. The method is capable of providing minimum level service even at the system has compromised partially. The method produces efficient results and maintains service availability at all the stage of the cloud.

An evaluation of alternative architectures for transaction processing in the cloud [8], focused towards providing choices for the data base services at different security stages. Also the method gives variety of architecture could be used for data base orient applications. The method mainly attended the problem of transaction processing at the more work loads. The results shows that such moderate alternative architecture has been adapted by many vendors to handle different workloads.

An layer based approach for cloud infrastructure to handle service level agreement violation has been discussed in [9]. The method performs mapping of low level resource details and the SLA parameters to validate the resource availability. Then a bottom up strategy has been proposed for the failure propagation which supports the SLA based threats. Also a set of communication model has been

discussed for the SLA violation based threats which increases the performance of the overall cloud security environment.

A Hybrid Intrusion Detection Architecture for Defense against DDoS Attacks in Cloud Environment [10], propose hybrid architecture for deployment of intrusion detection system which takes into account security at both the front end and the clusters. This Paper also includes a critical review of previously proposed architectures on deployment of Intrusion Detection Systems in Cloud Environment and a detailed description of the research Gaps identified. Our approach leverages VMware virtualization techniques using open nebula as a test bed for deploying our proposed system.

An Entity-centric Approach for Privacy and Identity Management in Cloud Computing [12], propose an entity-centric approach for IDM in the cloud. The approach is based on: (1) active bundles—each including a payload of PII, privacy policies and a virtual machine that enforces the policies and uses a set of protection mechanisms to protect themselves; (2) anonymous identification to mediate interactions between the entity and cloud services using entity's privacy policies.

A light weight intrusion detection mechanism for cloud computing has been proposed in [15]. The method uses self similarity of different users to perform intrusion detection. The method maintains similarity of different users at periodic interval which is observed by the cloud environment. The method monitors the activities of the users like the number of system calls they used and their status and so on. Based on this activity, the method computes the self similarity measure to perform intrusion detection in the cloud environment. The method has produced good results in small set of users

All the above discussed approaches has the problem of identifying malicious request and not consider about the

3. PROPOSED METHOD:

The proposed service orient approach has focused on providing efficient security measures for the organizational resources and the users of organizations. The proposed service orient model has the following functional components namely Key Generation, Service orient request approximation, and Intrusion Detection, Multi Attribute Encryption. We discuss each of them here in detail in this chapter.

I discuss each of the functional components in detail in this section. The key generation process generates key for the user and distribute them and the service orient approximation performs approximation according to the number of request has been received and the intrusion detection process uses all these functional components then the method uses the multi attribute encryption.

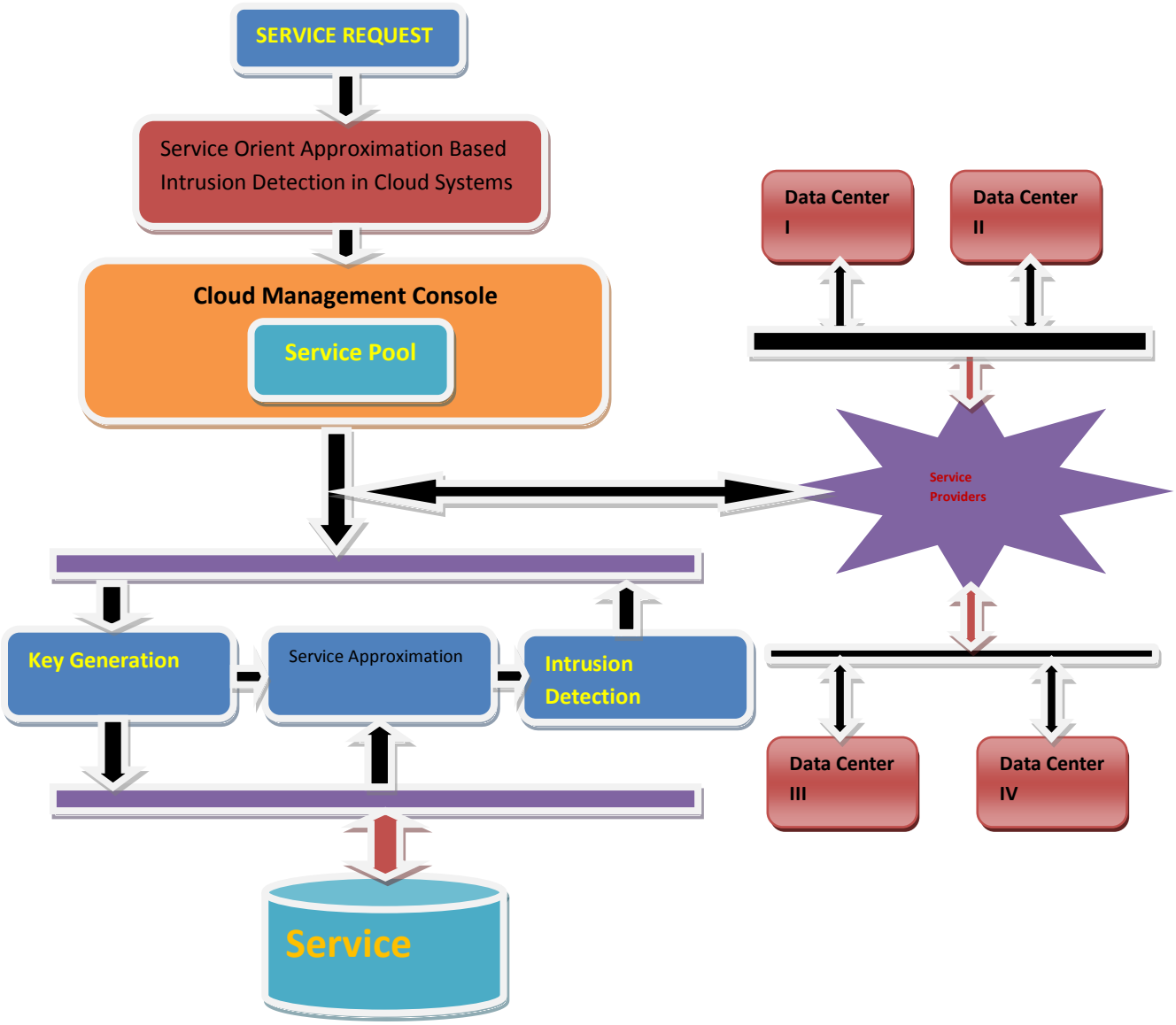


Figure 1: Proposed System Architecture

The Figure 1, shows the architecture of the proposed service orient model and its functional components.

3.1 Key Generation:

The key generator generates two different keys for each person or user registered with the cloud environment. The first key generated is the private key which composes of group key with distinct user information. The private key is a 32 bit key where each 8 bit has different information about the user and the group the user belongs and the service registered, the cloud he belongs to and so on. The first two bit represent the group id, the second two bit represent the cloud registered , the third eight bit

sequence belongs to the service registered and the final eight bit sequence represents distinct user. The second key is generated to perform encryption and decryption process. The second key is generated based on the user profile and how deep the user could be allowed to access or decrypt the information. The proposed method maintains various types of attributes and the user will be allowed to encrypt or decrypt the information according to the level of key he has.

Algorithm:
Input: User Id UID, GroupID GID, Cloud ID CID, Service Id SID.
Output: Private Key pk, Data Key Dk.
Initialize 32 bit private key.
Enable Group key Gk
Pk(0,7) = $\int Gk(GID) \in \sum Groups(Cloud)$
Encode Cloud ID CID.
Pk(8,15) = Convert Stream(CID).
Encode Service ID SID
Pk(16,23) = convert Stream(SID).
Encode User ID UID
Choose maximum users registered UID.
Pk(24,32) = convert stream(UID).
Identify user profile Up.
Generate Data key Dk = $\int_{i=1}^{N} Attr(SID) \times Up(i)$

The key generation algorithm generates 32 bit key for each user being registered. The first four bit represents the group key and the second four bit represent the cloud id and the third four bit represent the service id being registered. Finally the fourth bit represents the user id of the user.

3.2 Service Approximation:
The service approximation is performed when there is a user request and it collects the similar service the user requested. For each distinct service the method groups the access records towards each service. From the grouped service history, I identify the user profile that how deep the user has access permissions against the attributes of the service. Once the similar user profiled service access has been collected, the frequency of service access is computed for each time window. Based on computed service access frequency, the service request is verified for its legitimateness against the service requested. I compute the average access frequency of particular service and based on computed value the user request is verified for its legitimateness using the access threshold.

Algorithm:
Input: Service History Sh, Service Request SR
Output: Boolean.
Identify type of service St = $\int_{i=1}^{N} Service.Type \in (SR.serviceType)$

Identify set of all similar service SSS.
SSS = $\int_{i=1}^{N} \sum Service.Type \in Sh$
for each service Si from SSS
Compute service access frequency for each time domain SDM.
SAF = $\int \frac{\sum_{i=1}^{T} No\ of\ times\ acccess\ at\ time\ window\ Tw}{Total\ number\ of\ access.}$
T- Number of time window

Compute average access rate AAR = $\int \frac{\sum access\ of\ all\ time\ window}{Total\ time\ domain\ values} \times 100$
End.
if AAR < Access Threshold
Return true
Else
Return false
End

The service approximation algorithm computes the service access frequency for each of the service available. Also the method computes the average access rate for each of the service being available and if the access rate is less than the access threshold then the service will be returned with the value true, otherwise the service request will be returned with false.

3.3 Intrusion Detection:
The intrusion detection is performed based on the result of service approximation and the verification process. The verification process is performed using the private key submitted. The proposed key generation approach maintains number of users has been enrolled under a group and the user id assigned to them is also depend on that. At any point of time the number of users present at particular time could be verified and also the log available about the service being registered and the group key being used at that particular time window will help verify the user request. The proposed method generates different group key at different time window and the user private key with the particular eight bit will be similar at one time slot only. All these will be helpful in verifying the user identity and if any malformed request found then an alarm will be produced at the data set. The same will be used in identifying the intrusion detection also.

Algorithm:
Input: Service Malicious History SMH, Private Key pk, Service Log SL.
Output: Boolean
Read Service log Sl.
Read first 8 bit
Gk = $\int_{i=1}^{8} \sum Pk(i)$
Read User ID
UID = $\int_{i=25}^{32} \sum Pk(i)$

Read Cloud id CID
CID = $\int_{i=9}^{16} \sum Pk(i)$
Read Service ID
SID = $\int_{i=17}^{24} \sum Pk(i)$
for each time domain Tm
dentify group key used GKS = $\int_{i=1}^{T} Sl(i)(Gk)$
Identify the user key at time domain Ti
x = $\int_{i=1}^{N} (UID \in Sl(Ti), 1,0)$
if GKS equals Gk and x==1 then
Compute service approximation SA.
If SA==True Then
Generate access trace.
Allow service request.
Else
Generate malicious access trace.
End
End
End

4. RESULTS AND DISCUSSION:

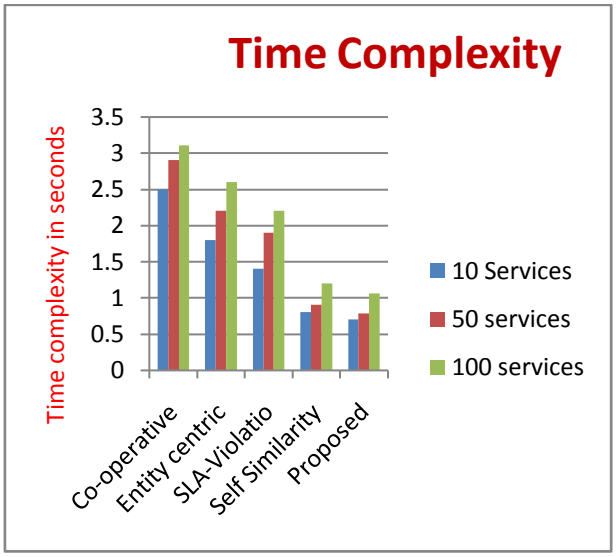
The proposed service approximation based intrusion detection has been implemented and tested for its efficiency. The proposed approach has produced efficient results in all the factors of quality of service of cloud computing in multi clouds.

Table 1: Details of implementation

Parameters	Value
Platform	Hadoop
Number of Services	100
Number of Users	500
Service Log Size	1 million
Time window	3 Months

The Table 1, shows the implementation details of the proposed method.

The proposed solution has been implemented Hadoop, which is the cloud computing platform integrated with the proposed solution to evaluate the proposed methodology. I have created three different clouds, each running on different locations and three service providers which are running at N-Number of locations. The proposed method has maintains various data centers and access traces to evaluate the performance of the proposed approach.

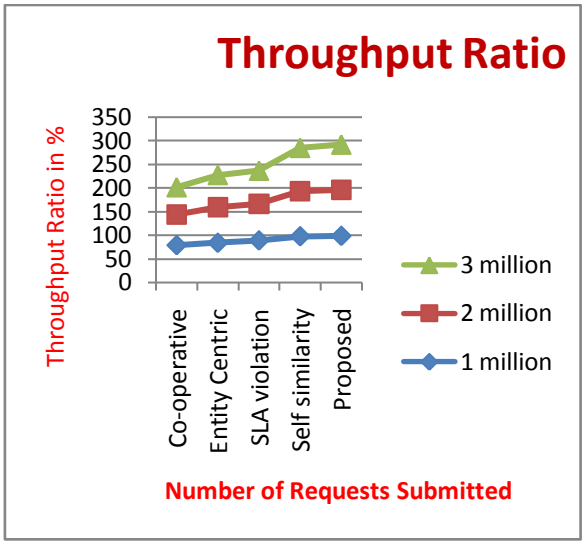


Graph1: shows the time complexity of different approaches.

The graph1 shows the time complexity of different methods to identify and verify the service request against its trustworthy.

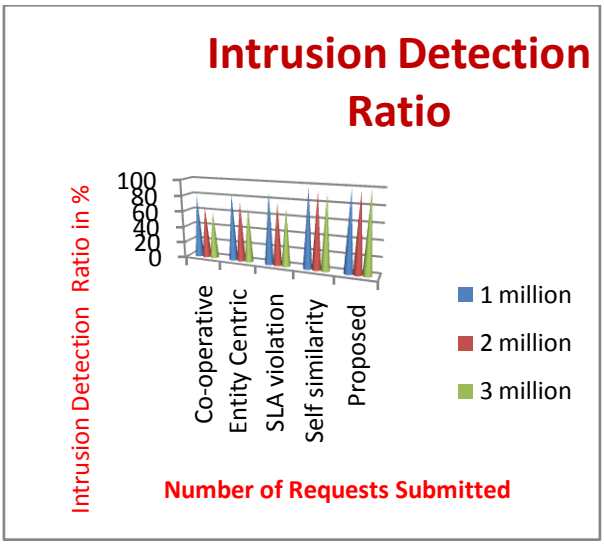
The time complexity is ϕ (N×M), where N- is the number of services, and M- is the size of trace available. The overall time complexity is computed as follows:

Time complexity Tc = N × Log (M).



Graph2: shows the comparison of throughput ratio.

The Graph2 shows the comparison of overall throughput generated by different algorithms, it shows that the proposed method has produced higher throughput than other methods.



Graph 3: Comparison of intrusion detection ratio

The graph3 shows the comparison of intrusion detection ratio achieved by different methods. It shows clearly that the proposed method has produced efficient detection rate than others.

5. CONCLUSION:

I proposed a multi attribute service approximation technique based intrusion detection system for cloud environment. The proposed method generates two different keys for each use and based on that key provided the users trustworthy are identified. The user private key has various features encoded and the other key used is to perform encryption and decryption of data present in the cloud. The proposed intrusion detection system has performed well and has produced efficient result by verifying the user submitted key by all the attributes like group id, cloud id, service id and user id. Based on these features the users identity is verified and the service approximation is performed to identify the behavior and verify them in accessing the service. The proposed method has produced efficient results and reduces the time complexity also. The method has produced higher accuracy in identifying intrusion in cloud environment.

REFERENCES:

1. Massimo Ficco, Salvatore Venticinque, Beniamino Di Martino, mOSAIC-Based Intrusion Detection Framework for Cloud Computing, springer, On the Move to Meaningful Internet Systems: , Volume 7566, 2012, pp 628-644.
2. Deepa Krishnan, Madhumita Chatterjee, An Adaptive Distributed Intrusion Detection System for Cloud Computing Framework, Recent Trends in Computer Networks and Distributed Systems Security Communications in Computer and Information Science Volume 335, 2012, pp 466-473.
3. Lo, C.-C., Huang, C.-C., Ku, J.: A cooperative intrusion detection system framework for cloud computing networks, 1530-2016/10,2010 IEEE
4. Vieira, K., Schulter, A., Westphall, C.B., Westphall, C.M.: Intrusion Detection for Grid and Cloud Computing, 1520-9202/10,2010 IEEE
5. Gul, I., Hussain, M.: Distributed Cloud Intrusion Detection Model. International Journal of Advanced Science and Technology 34, 71–82 (2011)
6. Westphall, C.B., Lamin, F.R.: SLA Perspective in Security Management for Cloud Computing. In: Proc. of the Int. Conf. on Networking and Services (ICNS), pp. 212–217 (2010)
7. Ficco, M., Rak, M.: Intrusion Tolerance of Stealth DoS Attacks to Web Services. In: Gritzalis, D., Furnell, S., Theoharidou, M. (eds.) SEC 2012. IFIP AICT, vol. 376, pp. 579–584. Springer, Heidelberg (2012)
8. Kossmann, D., Loesing, S.: An evaluation of alternative architectures for transaction processing in the cloud. In: Proc. of the Int. Conf. on Manag. of Data (2010)
9. Emeakaroha, V.C., Maurer, M., Dustdar, S., Acs, S., Kertesz, A., Kecskemeti, G.: LAYSI: A Layered Approach for SLA-Violation Propagation in Self-manageble Cloud Infrastructures. In: Proc. of the IEEE 34th Conf. on Computer Software and Applications, pp. 365–370 (November 2010)
10. Sanchika Gupta, Susmita Horrow, Anjali Sardana, A Hybrid Intrusion Detection Architecture for Defense against DDoS Attacks in Cloud Environment, Springer, Contemporary Computing Communications in Computer and Information Science Volume 306, 2012, pp 498-499.
11. Dhage, S.N., Meshram, B.B., Rawat, R., Padawe, S., Paingokar, M., Mishra, A.: Intrusion Detection system in Cloud Computing Environment. In: ICWET 2011 Proceedings of the International Conference & Workshop on Emerging Trends in Technology, pp. 235–238. ACM, NY (2011)
12. Ranchal, R., Bhargava, B., Othmane, L.B., Lilien, L., Angin, P.: An Entity-centric Approach for Privacy and Identity Management in Cloud Computing. In: 29th IEEE symposium on Reliable Distributed Systems, pp. 177–183. IEEE press (2010)
13. Bugiel, S., Nürnberger, S., Sadeghi, A., Schneider, T.: Twin Clouds: An Architecture for Secure Cloud Computing. In: Workshop on Cryptography and Security in Clouds, ECRYPT II, the European Network of Excellence in Cryptology, and TClouds (2011)

14. Hyukmin Kwon, Taesu Kim, Song Jin Yu, Huy Kang Kim, Self-similarity Based Lightweight Intrusion Detection Method for Cloud Computing, Springer, Intelligent Information and Database Systems Volume 6592, 2011, pp 353-362