Middle-East Journal of Scientific Research 23 (11): 2783-2790, 2015
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2015.23.11.22816

Dynamic Session Based Enforcement of Encryption Standards in Service Orient Cloud Environment for Intrusion Detection Using One Step Elliptic Curve Cryptography

[1]A. Murugan, [2]M. Nithya and [3]A. Nagappan

[1]Research Scholar, Department of Computer Science,
Vinayaka Missions University, India
[2]Research Supervisor, Head of the Department,
Department of Computer Science, VMKV Engineering College, Salem, India
[3]Principal, VMKV Engineering College, Salem, India

Abstract: The problem of time complexity involved in key generation and verification has deeply suppress the performance of the service orient cloud environment. Also the identity management and key verification has become time consuming in attributed encryption systems, to overcome these issues, an novel one step verification process has been proposed in this paper. There are some malicious user who intend to spoil the performance of the cloud environment and service orient architecture performance by generating malicious requests. The proposed method generates user specific private key at the time of registration and distributes elliptic curve values at the time. The user will be verified for his identity at the service request time, and will be queried for a particular point in the curve. By receiving the curve point the users identity is authenticated and verified in simple manner, the difficulty of predicting the curve point values of elliptic curve helps in verifying the user identity in easy manner. The values of curve is modified at each time interval and given to the registered user. If the user submits wrong values then the method performs service access analysis to identify the nature of user and restrict them from accessing the service. The proposed method improves the performance of the cloud environment and increases the efficiency of providing service security and increase the throughput of the cloud environment.

Key words: Cloud Security · Intrusion Detection · EC Cryptography · Session Based Approach · SOA

INTRODUCTION

The cloud is the environment where the service provider can deploy number of services into the network which can be accessed from the external world. The external users who registered in the cloud environment can access the services available in the cloud. There may be services which belongs to any organization and should be accessed only by the users of the organization and the access to be restricted in different level of the organization. Because some of the services should be only accessible for some of the destination users. To perform such restriction the user has to be authenticated and his access permission has to be verified in proper manner.

Public and private key based authentication approaches are discussed earlier in this environment and has more possibility of compromising and some of the malicious user could break and guess the user password or key easily and perform different attacks, or the malicious user could try to access the service in unauthorized manner. Such activity can be named as intrusion and has to be detected. The process of intrusion detection can be done in variety of ways by simply verifying the key of user at the time of service access and there are attribute based encryption mechanisms are enforced to detect the intrusion. Such systems introduces more overhead in key verification and authentication which reduces the service throughput and affects the quality of service of the cloud environment [1].

Corresponding Author: A. Murugan, Research Scholar, Department of Computer Science,
Vinayaka Missions University, India.

In any service orient architecture (SOA), the services can be accessed from the external world through internet communication independent of user location. But the user identity has to be verified and his rights to access the service has to be verified. The password based approaches, public and private key based approaches are not suitable for such dynamic environment where there is a huge number of request being received at a time. Similarly they require Third party auditor to verify the identity of the user which also introduces the overhead of network communication and increases the time complexity of service access. In some of the systems, they introduced attribute based encryption methods which uses different key for different attributes which also increases the overhead of key verification. So the requirement of simple and efficient verification approaches are necessary, also if the password or key has been stolen then the malicious user can access the service without any restriction and generate intrusion into the network [2].

The Elliptic curve cryptography is the most efficient and difficult cryptography standard which is well proven in the world of cryptography. In this curve is initialized with set of coordinate points and at each coordinate point there will be an integer value which can be considered as the key. In this approach, the service can choose any point at a time and can query the value present in the point to verify the identity of the user. This will become a simple one step and reduces the time of verification. Also in a session based approach, the parameters of the elliptic curve can be exchanged and modified which increases the tampering quality of the encryption standard [3].

Related Works: There are many approaches has been discussed for the development of intrusion detection in cloud environment. Here we discuss some of them here around the problem statement.

mOSAIC-Based Intrusion Detection Framework for Cloud Computing [1], proposes an architectural framework that collects information at different Cloud architectural levels, using multiple security components, which are dynamically deployed as a distributed architecture. The proposed solution allows to monitor different attack symptoms on different Cloud architectural levels, which can be used to perform complex event correlation and diagnosis analysis of intrusion in the Cloud system.

An Adaptive Distributed Intrusion Detection System for Cloud Computing Framework [2], proposes a unique Distributed Intrusion Detection System (DIDS) based on a novel combination of two variant trends in intrusion detection-the behavior based and knowledge based intrusion detection mechanisms. The behavior based approach facilitates improved detection in the dynamic cloud environment and the knowledge based approach supports the detection scheme with its definitive rule base. The functionality of both these approaches has been improved by the addition of an adaptive approach which helps to significantly assist in lowering the false positives.

Cooperative intrusion detection system framework for cloud computing networks [3], proposed system could reduce the impact of these kinds of attacks. To provide such ability, IDSs in the cloud computing regions exchange their alerts with each other. In the system, each of IDSs has a cooperative agent used to compute and determine whether to accept the alerts sent from other IDSs or not. By this way, IDSs could avoid the same type of attack happening.

SLA Perspective in Security Management for Cloud Computing [5-14], explores Service Level Agreements for Security or just Sec-SLAs. Is tried to provide an overview on the subject, the difficulties faced during the security metrics definition process and the Sec-SLA monitoring, as well as an analysis on the Sec-SLA role in new paradigms like cloud computing.

Intrusion Tolerance of Stealth DoS Attacks to Web Services. [7], focuses on one of the most harmful categories of Denial of Service attacks, commonly known in the literature as “stealth” attacks. They are performed avoiding sending significant volumes of data, by injecting into the network a low-rate flow of packets in order to evade rate-controlling detection mechanisms. This work presents an intrusion tolerance solution, which aims at providing minimal level of services, even when the system has been partially compromised by such attacks. It describes all protection phases, from monitoring to diagnosis and recovery.

An evaluation of alternative architectures for transaction processing in the cloud [8], lists alternative architectures to effect cloud computing for database applications and reports on the results of a comprehensive evaluation of existing commercial cloud services that have adopted these architectures. The focus of this work is on transaction processing (i.e., read and update workloads), rather than analytics or OLAP workloads, which have recently gained a great deal of attention.

Layered Approach for SLA-Violation Propagation in Self-manageable Cloud Infrastructures [9], present a novel approach for mapping low-level resource metrics to SLA parameters necessary for the identification of failure

sources. Second, we devise a layered Cloud architecture for the bottom-up propagation of failures to the layer, which can react to sensed SLA violation threats. Moreover, we present a communication model for the propagation of SLA violation threats to the appropriate layer of the Cloud infrastructure, which includes negotiators, brokers, and automatic service deployer.

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.

Self-similarity Based Lightweight Intrusion Detection Method for Cloud Computing [15], propose a lightweight IDS with self-similarity measures to resolve these problems. Normally, a regular and periodic self-similarity can be observed in a cloud system's internal activities such as system calls and process status. On the other hand, outliers occur when an anomalous attack happens, and then the system's self-similarity cannot be maintained. So monitoring a system's self-similarity can be used to detect the system's anomalies. We developed a new measure based on cosine similarity and found the optimal time interval for estimating the self-similarity of a given system. As a result, we can detect abnormal activities using only a few resources.

All the above discussed approaches has the problem of identifying malicious request and not consider about the behavior of the users. We propose a simple one step verification approach and user behavior details in performing intrusion detection.

Proposed Method: The proposed dynamic session based service orient one step elliptic curve cryptography 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 Session Based Key Generation, One Step Verification, and Intrusion Detection. We discuss each of them here in detail in this chapter.

The Figure 1, shows the architecture of proposed session based approach and it shows the functional component of the proposed method.

Session Based Key Generation: The key generator generates a public and private key for each use registered to the cloud. The public key is a random one generated for the user and the private key has four parameters namely Group id, Service id, user id and session id. The computed public and private key will be sent to the user. Along with this the method generates the elliptic curve parameters and the user will be given with all these parameters. At each session, the method generates the private key and elliptic curve parameters and sent to the user.

Algorithm:

Input: User Id UID, GroupID GID, Cloud ID CID, Service Id SID, Session ID SEID.
Output: Public Key pk, Private Key Prk.

Initialize public key set Pkset = $\sum_{i=1}^{100} Generate(key)$
while(true)
Receive user request.
Generate public key pk = Rand(Pkset)
Generate private key Prk = {CID,GID,SID,UID,SEID}.
Initialize Elliptic curve parameters ECpr = {Points, values}
Send to the user.
wait for next session.
End.

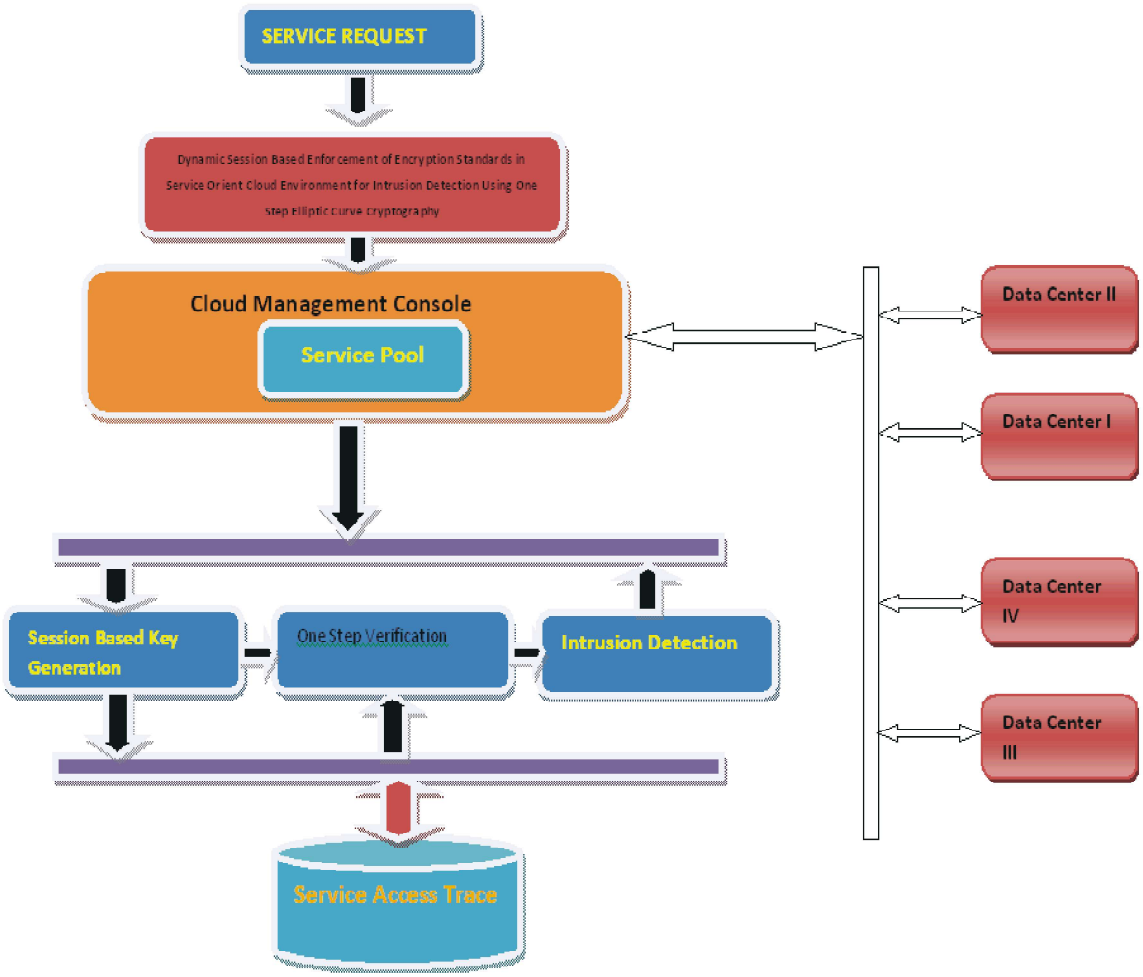


Fig. 1: Proposed System Architecture.

The above discussed algorithm generates key at each session and generates elliptic curve parameters and distribute to the users of the cloud who has registered.

User Behavior Analysis: The user behavior analysis is performed whenever a service request is received. Firs the method collects the set of all service access performed by the user at each session. Then the method computes the malicious request at each session and if the frequency of malicious request is less than the threshold then it is concluded as general behavior and the request is ignored otherwise it is concluded as malicious and generate the trace to the malicious log.

Algorithm:

Input: Service History Sh, Service Request SR

Output: CAR, AAR.

Identify Service requested Sr = SR.Service ID.

for each time window

collect all the records generated for the service.

Service trace St = $\sum_{i=1}^{size(services)} Sh(sr).UserID = UID$

Compute service access rate SAR

SAR = $\int \frac{\sum_{i=1}^{T} No\ of\ times\ access\ at\ time\ window\ Tw}{Total\ number\ of\ access.}$

T- Number of time window

End

Compute average access rate AAR = $\int \frac{\sum access\ of\ all\ time\ window}{Total\ time\ domain\ values} \times 100$

Compute access rate at current time window CAR.

CAR = $\int \frac{size\ (St)}{Total\ number\ of\ access.}$

return CAR, AAR.

Stop

One Step Verification: The one step verification is performed whenever a service request is received. At this stage the controller, receives the user request and then it chooses a point from the elliptic curve and send to the user. The user has to reply with the integer at that point which is in form of encrypted and will be decrypted by the controller. The controller verifies the integer sent by the user and then decides about the trustworthy of the user.

Algorithm:
Input: Service Request Sr
Output: Boolean
Start

Receive request Sr.
Read the elliptic curve parameters EP.
Choose a random point from the curve Rp = $\int RandomSelection(Ep)$
Send Rp to the user.
Receive value from the user.
if Ep(Rp) == UserInteger then
return true
else
return false
end

Stop.

Intrusion Detection: Whenever the controller receives the user request, it performs the intrusion detection by verifying the feature of service request and details. First it identifies the identity of the user and if the identity does not match or the service request parameters does not match with the service signature, then it performs one step verification. If one step verification fails then it is concluded as malicious otherwise the method performs the user behavior analysis. With the result of user behavior result the method computes the legitimate weight and based on the weight computed the method classifies the request as malicious or genuine.

Algorithm:
Input: Service Request Sr, Public key Set Pks, Private key Set Prks.
Output: Boolean
Start

Receive Service Request Sr.
Verify public and private keys of user.
identify the user UID = Sr.UID.
verify the key details.
if Pk.UID==Pks(UID).Pk && Prks.UID==Pk.UID && Prks.GID==Pk.GID && Prks.CID==Pk.CID then
Boolean bool = Perform One Step Verification.
if true then
genuine packet.
return true.
else

```
                generate trace and classify malicious.
        end
    Else
        Boolean bl = Perform One step verification.
        if true then
                BA = perform user behavior analysis.
                Compute legitimate weight Lw = BA.CAR×BA.AAR
                if lw>Th then
                        classify genuine packet.
                        Add to trace.
                else
                        classify malicious packet.
                        Add to trace.
                end
        else
                classify malicious packet.
                Add to trace.
Stop.
```

The above discussed algorithm performs intrusion detection in cloud environment using the other functional components of the proposed approach.

RESULTS AND DISCUSSION

The proposed dynamic session based one step verification approach based intrusion detection system for cloud environment 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.

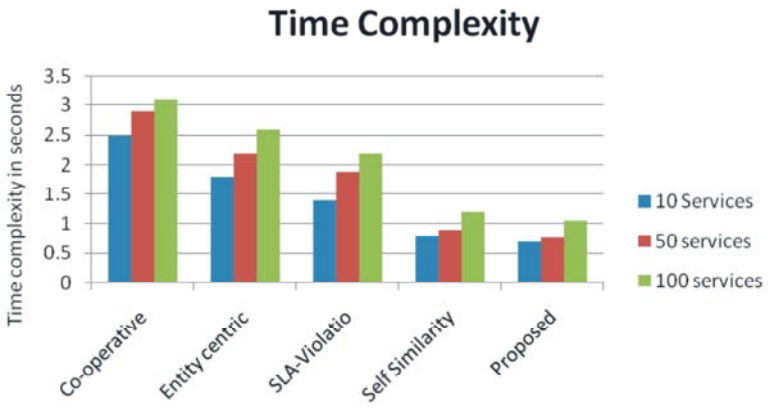
The proposed solution has been implemented Hadoop, which is the cloud computing platform integrated with the proposed solution to evaluate the proposed methodology. We have created three different clouds, each running on different locations and three service providers which are running at N-Number of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

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

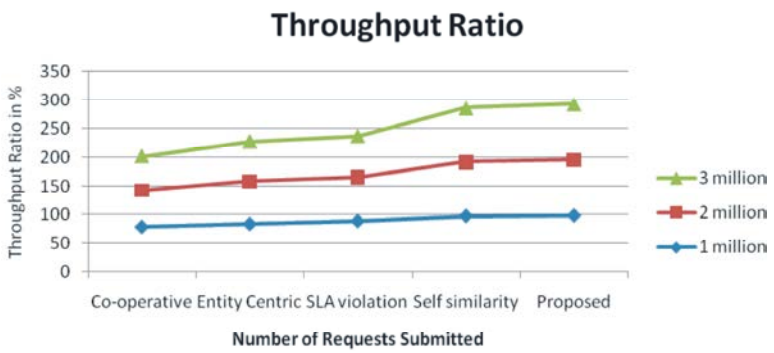
The time complexity is □ (N×M), where N- is the number of services, and M- is the size of trace available. The overall time complexity is computed as follows:

Time complexity Tc = N × Log (M).

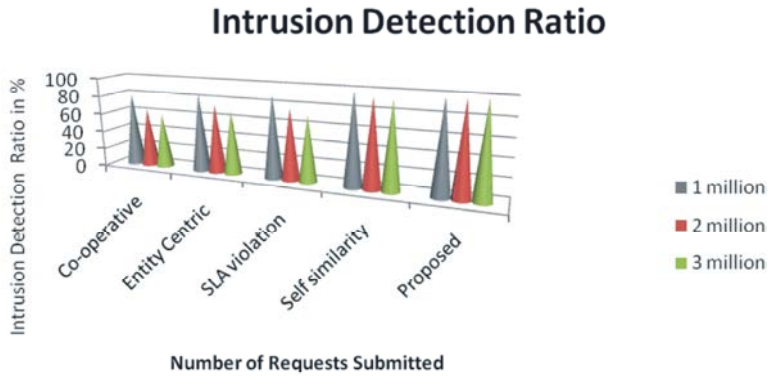
The Graph1 shows that the proposed method has produced higher efficient results compare to other algorithms.



Graph1: shows the time complexity of different approaches.



Graph 2: shows the comparison of throughput ratio.



Graph 3: Comparison of intrusion detection 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.

The Graph 3 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.

CONCLUSION

We proposed service orient session based one step verification approach based intrusion detection using elliptic curve cryptography has been proposed for the development of cloud environment. The controller generates two different keys like public and private key. The public key is common for all the users of the cloud and the private key has different information about the user id, session id, cloud id, group id and service id. The generated keys with the elliptic curve parameter will be distributed to the cloud users. Whenever a service request is received by the controller, it verifies the public and private keys and if they are true then it performs one step verification to verify the identity of the user. If both sequence is successful then the user is allowed to access the request and generate trace in the data base. If not the controller performs one step verification and user behavior analysis to compute the legitimate weight of the packet. Based on computed legitimate weight the packet is classified as malicious or genuine. The proposed method increases the efficiency of intrusion detection and increases the throughput of the cloud services with less time complexity of user verification.

REFERENCES

1. Ficco Massimo, Salvatore Venticinque and Beniamino Di Martino, 2012. Mosaic-Based Intrusion Detection Framework for Cloud Computing, springer, On the Move to Meaningful Internet Systems, 7566: 628-644.
2. Deepa Krishnan and Madhumita Chatterjee, 2012. 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, 335: 466-473.
3. Lo, C.C., C.C. Huang and J. Ku, 2010. A cooperative intrusion detection system framework for cloud Computing Networks, (10): 1530-2016.

4. Vieira, K., A. Schulter, C.B. Westphall and C.M. Westphall, 2010. Intrusion Detection for Grid and Cloud Computing, IEEE, (10): 1520-9202.
5. Gul, I. and M. Hussain, 2011. Distributed Cloud Intrusion Detection Model. International Journal of Advanced Science and Technology, 34: 71-82.
6. Westphall, C.B. and F.R. Lamin, 2010. SLA Perspective in Security Management for Cloud Computing. In: Proc. of the Int. Conf. on Networking and Services (ICNS), pp: 212-217.
7. Ficco, M. and M. Rak, 2012. Intrusion Tolerance of Stealth DoS Attacks to Web Services. In: Gritzalis, D., Furnell, S., Theoharidou, M. (eds.) SEC 2012. IFIP AICT, Springer, Heidelberg, 376: 579-584.
8. Kossmann, D. and S. Loesing, 2010. An evaluation of alternative architectures for transaction processing in the cloud. In: Proc. of the Int. Conf. on Manag. of Data.
9. Emeakaroha, V.C., M. Maurer, S. Dustdar, S. Acs, A. Kertesz and G. Kecskemeti, 2010. 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.
10. Gupta Sanchika, Susmita Horrow and Anjali Sardana, 2012. A Hybrid Intrusion Detection Architecture for Defense against DDoS Attacks in Cloud Environment, Springer, Contemporary Computing Communications in Computer and Information Science, 306: 498-499.
11. Dhage, S.N., B.B. Meshram, R. Rawat, S. Padawe, M. Paingokar and A. Mishra, 2011. Intrusion Detection system in Cloud Computing Environment. In: ICWET 2011 Proceedings of the International Conference & Workshop on Emerging Trends in Technology, pp: 235-238.
12. Ranchal, R., B. Bhargava, L.B. Othmane, L. Lilien and P. Angin, 2010. An Entity-centric Approach for Privacy and Identity Management in Cloud Computing. In: 29th IEEE symposium on Reliable Distributed Systems, IEEE press, pp: 177-183.
13. Bugiel, S., Nürnberger, S. Sadeghi, A. Schneidera and T. Twin, 2011Clouds: 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.
14. Kwon Hyukmin, Taesu Kim, Song Jin Yu and Huy Kang Kim, 2011. Self-similarity Based Lightweight Intrusion Detection Method for Cloud Computing, Springer, Intelligent Information and Database Systems, 6592: 353-362.