International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-4, November 2019

Real Time Service Level Access Restriction using Dynamic OTUP Generation for Improved Security in Cloud

J.Mohammed Ubada, M. Mohamed Surputheen

Abstract: ***The cloud environment has been identified as the keen platform being used by different cloud users and organizations. The data security has been approached with several techniques like password, attribute based approaches and so on. However, they suffer to achieve higher security performance. To improve the performance, an efficient real time service level access restriction scheme which uses dynamic OTUP (One Time User Password) generation scheme. The method maintains different user information which includes the password details of users. Further, the method collects the one time user password initially. With this, the method restricts the user's service access by generating OTUP in a dynamic way according to different services. The user has been restricted according to the service and OTUP generation methods. According to this, the method estimates service level trust weight (SLTW) to restrict the user. The methods introduce higher security performance and reduces false ratio.***

Keywords: Cloud, Secure Access, Access Restriction, service level access, restriction OTUP, SLTW.

I. INTRODUCTION

The organizations maintain various information around the customers and business. The size of database getting increased every day and they face the problem of maintaining huge data and database servers which are highly costlier. On the other side, the small scale organizations cannot spend huge money in maintaining the database server. The cloud environment has become the solution for that which provides options to maintain their data and allow their user to access the data through set of services. The cloud users can perform access of data and can perform modification access on the cloud data through the services available.

The cloud services are meant to provide access to the registered users, but the presence of malicious entity would try to invoke some malformed access and would involve in different threats. The threat may be of DDos (Distributed denial of service) attack which would generate number of blind access to degrade the service performance. Similarly there are number of threats can be performed by the adversaries or malicious users.

There exist number of access restriction algorithm presented and available. The user has been restricted from malformed access either through the password and keys. However, the leakage of password and keys would introduce threats to the services. To handle this issue, an efficient OTUP based dynamic scheme is presented in this paper. The existing login services claims the username and password with one time password (OTP) to allow them to access the service. But the missing of phones, or other Email details leads the malformed user to perform different misbehaving. This must be stopped and even the person misses the mobile phone or even if the mail details are leaked, then also, the malicious users should be stopped from accessing the service.

Towards the security development, a service level access restriction algorithm is presented in this paper. The system has to use different scheme of OTUP generation which is performed in a dynamic way and the method estimates the service level trust weight (SLTW) measure to perform secure cloud computing. The detailed approach is presented in the next section.

II. RELATED WORKS

There are number approaches available for the problem of secure computing in cloud environment. This section present the detailed review on the problem of secure access and access restriction.

In [1], the author present token based attribute based hierarchical access control system. The method verifies the correctness of data and user according to the token. The method uses metadata in verifying the correctness of data and user. In [2], the author presents a access control algorithm by maintaining hierarchical structure and a clock.

In [3], the author presents a detailed review on the problem of access control and data security in cloud environment. In [4], the author presents a multi-layer encryption standard for the security of cloud data. In [5], the author presents a detailed introduction on the access control methods available and compares their performance in various parameters. In [6], the author present a framework which works based on different policies. According to the policies, the method enforces access control in BYOD environment.

Manuscript published on November 30, 2019.
* Correspondence Author
J.Mohammed Ubada*, Corresponding Author, Research Scholar, Department of Computer Science, Jamal Mohamed College (Autonomous) (Affiliated to Bharathidasan University), Tiruchirappalli, Tamilnadu, India. (Email: ubada786@gmail.com)
Dr. M. Mohamed Surputheen, Associate Professor, Department of Computer Science, Jamal Mohamed College (Autonomous) (Affiliated to Bharathidasan University), Tiruchirappalli, Tamilnadu, India.

In [7], the author performs evaluation on various algorithms on their security performance.

In [8], the author present a taxonomy based approach for the access restriction in cloud environment. The method uses the taxonomy in controlling the access of health care data. In [9], the author analyzes the security issues in cloud environment.

In [10], the author present a location based data security algorithm which performs location based encryption to improve data security. In [11], the author present a detailed review on the data security and control algorithms available. It analyses various security threats towards data services. In [12], the author present ECC based identity and access management algorithm (IBC) and trust orient access control.

In [13], the author presents a role and trust degree based access control algorithm for multi domain. The trust of the user is measured on direct, feedback based. The trust weight has been adjusted according to the trust values.

In [14], the author presents a review on different security techniques and details the challenges. The privacy protection schemes are well analyzed towards the scope. Similarly in [15,25], the author present a detailed review on the methods of access control towards performance development of cloud environment.

In [16], an shared authentication protocol is presented which adapts shared access authority and enforces attribute based access control with pre-encryption methods. In [17], a time orient one-time password based access control algorithm is presented. The method uses time-based one-time password (TOTP) and automatic blocker protocol (ABP) to provide complete security. In [18], the author present a finger print based technique to encrypt the data and to perform access control.

In [19], the author present a hierarchical sensitive support (HSS) based access control algorithm. The method uses taxonomy of access control in hierarchical form. According to the taxonomy the value of HSS is measured for each level and finally a cumulative data retrieval support (CDRS) is estimated. Estimated CDRS value has been used to perform access restriction and data retrieval.

In [20], a Context Aware Based Access Control Model is presented. The method uses situation recognition technology based access control model which can control lots of cloud's users and access of device flexibly. In [21], an Attribute Role Based access control (ARBAC) algorithm is presented. The method uses role-based access control authorization mechanism and combines it with attribute based access control to determine which tenant that user can access.

In [22], presents a generic ACaaS framework that should be adequate for providing high level of extensibility and security by integrating multiple access control models.

In [23], the author suggests the data access control model and the method for multimedia content sharing and security based on XMDR-DAI in the mobile cloud storage. The method establishes XMDR-DAI-based metadata relationship for the problems that occurred in searching to increase the reliability. And this research suggests the prototype using TPM emulator that is operated in secure world of ARM TrustZone and TrustZone environment.

In [24], the author proposed analytical models provide a closed form solution for access probability and resource utilization at a given time.

All the methods suffer to achieve higher performance in data access control and produces higher false classification ratio.

III. REAL TIME SERVICE LEVEL ACCESS RESTRICTION USING DYNAMIC OTUP GENERATION

The proposed service level access restriction with dynamic OTUP Generation scheme performs access restriction in service level. For each service, the method uses different OTUP generation scheme according to the service being requested. The generation of OTUP is performed according to the OTUP provided at the signing stage and manipulated for the restriction of service access. The detailed approach is presented below:

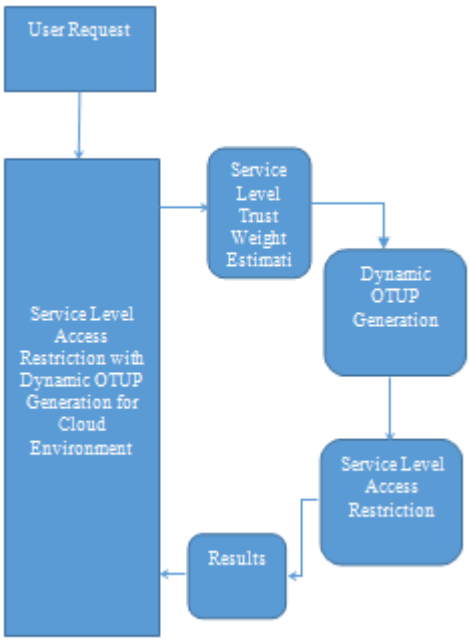

Fig. 1. Architecture of proposed service level access restriction and dynamic OTUP Scheme

The Figure 1, shows the architecture of proposed dynamic OTUP scheme for the restriction of access and shows various components which are explained in detail.

A. Service Level Trust Weight Estimation

The service level trust measure is the factor which represents the trustworthy of the user in accessing the service. It has been measured according to the previous history of access. The user would have accessed the service for number of times but the completion of the service access in proper way represents the trust of the user. It has been measured according to the number of access and number of successful completion. Using these two, the method estimates the SLTW value which has been used to perform access restriction.

Algorithm:
Input: Trace T, Request R
Output: ALTW.
Start
Read trace T, request R.
Identify the service S = $\int Service \in R$
Compute number of times accessed
Tac.
Tac = $\int_{i=1}^{size(T)} \sum T(i).Service == S \&\& T(i).user == R.User$Compute number of access complete Nca.
Nac = $\int_{i=1}^{size(T)} \sum T(i).Service == S \&\& T(i).user == R.User \&\& Ti.staus==1$Compute Service level trust weight

SLTW = $\frac{Nac}{Tac}$.
Stop

The estimation of service level trust weight is described in the above algorithm. Estimated trust weight has been used to perform access restriction.

B. Dynamic OTUP Generation

The generation of OTUP has been performed according to different service types. For any service requested, its type has been identified. Based on the type, the method generates the OTUP for the user which has been used to verify the user. The method uses four types of method for OTUP generation which is namely pre-concatenation, post-concatenation, pre-replacement, and post-replacement. Any of the type will be selected according to the type of service and the user will be given with the OTUP and used to perform access restriction.

Algorithm:
Input: Request R, Scheme set S, OTUP set Os
Output: UOTUP
Start
Read R, s, Os.
Identify service Rs = $\int R.Service$
if Rs.Type==Forget then
Hint H = $\int_{i=1}^{size(Os)} Os(i).User == R.User \&\& Os(i).Hint$
Send H to User.
Hint Result Hr = Receive Hint Answer from user
If $\int_{i=1}^{size(Os)} Os(i).User == R.User \&\& Os(i).HAnswer == H1$ then
Send OTUP to User.
end
else

Identify the OTUP predefined Potup = $\int_{i=1}^{size(Os)} Os(i).User == R.User$

Generate OTP as uotp = $\int_{i=1}^{size(OTp)} concat(uotp) + Random(0,10)$

Type t = $\int_{i=1}^{2} Random(1,2)$

If t==1 then
Uotp = Uotp+potup
Else
Uotp = Uotp-potup
end
If Rs.Type ==1 then //pre-concatenation
Uotp = potup+uotp
If Rs.Type==2 then //post-concatenation
Uotp = uotp+potup
If Rs.Type ==3 then //replace first two digits
Uotp = potup+substring(2,uotp)
If Rs.Type == 4 then //replace last two digits
Uotp = substring(0,length(uotp)-2)
End
UOTUP = Uotp.
End
Stop

The working principle of dynamic OTUP generation algorithm is presented and it generates the one time user password for the users according to the service and scheme selected. The generated OTUP has been used to perform access restriction.

C. Service Level Access Restriction

The service level access restriction algorithm works based on the service level trust weight being measured for any user request. Any user would claim for the service but it is necessary to measure the trust of the user. The trust of the user is measured according to the SLTW estimation algorithm. Estimated value of SLTW has been used to restrict the user. If the users have enough value of SLTW, then he has been generated with the dynamic OTUP. Based on the correctness of OTUP submitted, the user request has been fulfilled.

Algorithm:
Input: Service Request R, Trace T.
Output: Boolean
Start
Read R, T.
SLTW = Estimate service level trust weight SLTW.
If SLTW>Th then
OTUP = Generate dynamic OTUP
Send to user U.
OTUPr = Receive OTUP
If OTUP==OTUPr then
Access grant
Else
Deny access
End
Else
Deny access
End
Stop

The above discussed algorithm shows how the access restriction is performed according to the OTUP generated for the user. The method generates the OTUP for the user and verifies the same at the reception from the user.

IV. RESULTS AND DISCUSSION

The proposed role based class level access trust block chain algorithm have been implemented and evaluated for its performance.

The proposed CLAT algorithm is hardcoded in advanced java. The result obtained through evaluation is presented in this section.

Table- I: Details of Simulation

Parameter	Value
Tool Used	Advanced Java
Number of Users	200
No of services	25
No of Features	60

The details of simulation being used for the evaluation of proposed SLTW algorithm has been presented in Table 1.

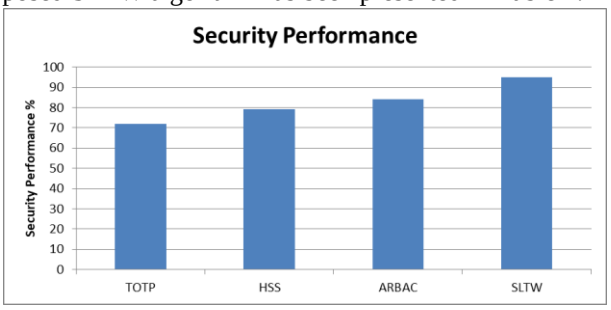

Fig. 2. Performance in Security

The performance in security has been measured for the proposed SLTW algorithm and compared with the values of other methods. The proposed SLTW algorithms have achieved higher performance in security compared to other methods.

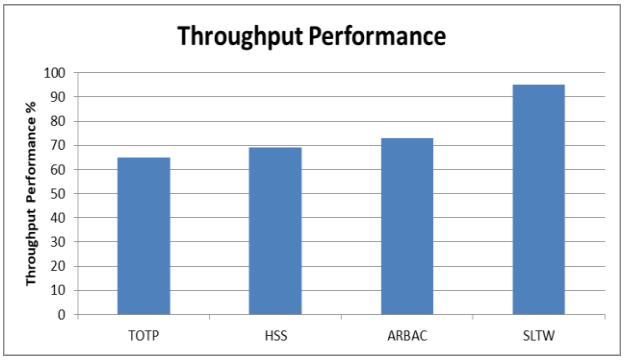

Fig. 3. Performance on throughput achievement

The achievement in throughput performance has been measured and compared with the result of other methods. The proposed SLTW algorithms have achieved higher throughput performance compare to other methods.

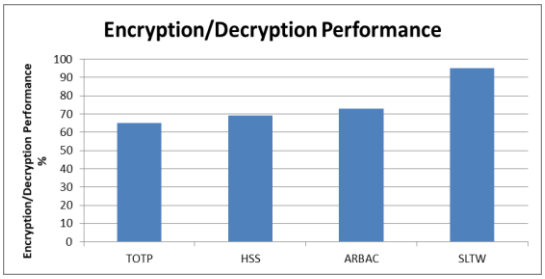

Fig. 4. Performance in Encryption / Decryption

The performance in encryption and decryption has been measured and compared with the values of other methods in Figure 4. The proposed SLTW algorithms have produced higher performance than other methods.

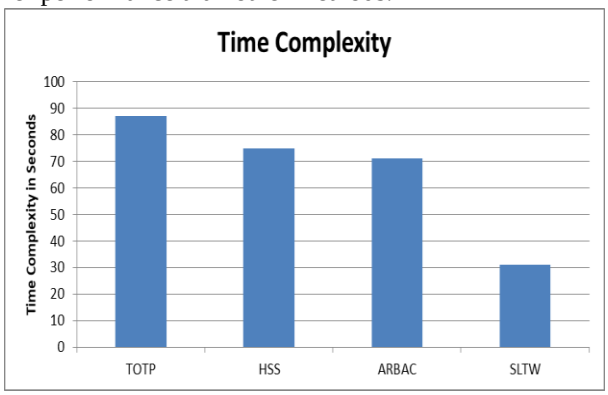

Fig. 5. Performance in time complexity

The performance in time complexity has been measured and presented in Figure 5. The proposed SLTW algorithms have produced less time complexity than other methods.

V.CONCLUSION

In this paper an efficient time orient service level access control algorithm with dynamic OTUP generation algorithm is presented. The method maintains different services and methods of generating one time user password. According to that, the method identifies the user request and measure the service level trust weight. Based on the value of SLTW, the method identifies the class of service and according to that the method generates a one-time user password. Based on the OTUP, the method produces higher performance in the security and access control.

REFERENCES

1. Balamurugan Balusamy, A Secured Access Control Technique for Cloud Computing Environment Using Attribute Based Hierarchical Structure and Token Granting System, (IJNS), Volume 19, Number 4, 2017, PP.559-572..
2. BIBIN K ONANKUNJU, Access Control in Cloud environment, Research Gate, Volume 3, Issue 9, 2013.
3. Ravi Kumar, Exploring Data Security Issues and Solutions in Cloud Computing, Research Gate, 2018, PP 691-697.
4. Naveen N, Security and Privacy Challenges Using Multi-Layer Encryption Approaches In Cloud Computing Environments, (IJITEE), Volume-8 Issue-8 ,2019.
5. Priya G, AN ACCESS CONTROL MODELS IN CLOUD COMPUTING: A REVIEW, (IJPAM), Volume 116, Number 24, 2017, PP 539-548.
6. Khalid Almarhabi, A Proposed Framework for Access Control in the Cloud and BYOD Environment, (IJCSNS), Volume 18, Number 2, 2018.

7. Django Armstrong, Towards energy aware cloud computing application construction, Springer open (JCC), Volume 6, Number 14, 2017.
8. Fangjian Gao, Rethinking the Meaning of Cloud Computing for Health Care: A Taxonomic Perspective and Future Research Directions, (JMIR), Volume 20, Number 7, 2018.
9. Prachi Deshpande, Security and service assurance issues in Cloud environment, IDEAS, 2018.
10. Goikar Vandana T, Improve Security Of Data Access In Cloud Computing Using Location, (IJCSMC), Volume 4, Issue 2, 2015, PP 331-340.
11. Mahesh B, Data Security And Security Controls In Cloud Computing, (Ijaecs), 2016.
12. Salim Ali Abbas, Enhancing the Security of Identity and Access Management in Cloud Computing using Elliptic Curve Cryptography, (IJERMT), Volume 4, Issue 7, 2015.
13. Lixia Xie, Cloud Multidomain Access Control Model Based on Role and Trust-Degree, HINDAWI (JECE), 2016.
14. Yunchuan Sun, Data Security and Privacy in Cloud Computing, (IJDSN), Volume 6, Number 50, 2014, PP 1-9.
15. I. Indu, Identity and access management in cloud environment: Mechanisms and challenges, Science Direct (ESTIJ), Volume 21, Issue 4, August 2018, PP 574-588.
16. Mohammed Abdul Waheed, CLOUD SECURITY USING SAP-SHARED AUTHENTICATION PROTOCOL, (IJCSMC), Volume 4, Issue 6, 2015, PP 106-113.
17. Sheren A El-BooZ, A secure cloud storage system combining time-based one-time password and automatic blocker protocol, Springer open (JIS), Number 13, 2016.
18. Nithya Chidambaram, Enhancing the Security of Customer Data in Cloud Environments Using a Novel Digital Fingerprinting Technique, HINDAWI (IJDMB), 2016.
19. A. Antonidoss, Real-Time Hierarchical Sensitivity Measure-Based Access Restriction for Efficient Data Retrieval in Cloud, Springer Link (ISDIA), Volume 862, 2018, PP 189-197.
20. Yun Sang Byun, Context Aware Based Access Control Model in Cloud Data Center Environment, (FIFCC), Volume 301, 2014, PP 515-524.
21. Nai Wei Lo, An Attribute-Role Based Access Control Mechanism for Multi-tenancy Cloud Environment, Springer Link (WPC), Volume 84, Issue 3, 2015, pp 2119-2134.
22. Rahat Masood, Cloud authorization: exploring techniques and approach towards effective access control framework, Springer Link (FCS), Volume 9, Issue 2, 2015,PP 297-321.
23. Kye-Dong Jung, Data access control method for multimedia content data sharing and security based on XMDR-DAI in mobile cloud storage, Springer link (MTA), Volume 76, Issue 19, 2017, PP 19983-19999.
24. A. Anas, "Autonomous Workload Balancing in Cloud Federation Environments with Different Access Restrictions," IEEE (MASS), 2017, pp. 636-641.
25. M. A. Safvati, "Investigating the features of research environments on cloud computing," IEEE (KBEI), 2017, pp. 0404-0411.