# A Proposed Approach For Cost Optimization In Authentication With O-Auth Services

**S. Dubey[1], K.Mathur[2]**
[1, 2] International Institute of Professional Studies
[1, 2] Devi Ahilya University, Indore, India

***Abstract-*** *It is the age of science when we need to get facilitated by a huge number of portals and/ or websites. The number of these websites is directly proportional to the number of accounts made by every user. This is creating data redundancy and/or unnecessary duplication of data in the web.There is always a need of a service which will work on centralized aces granting facility. A service in which login or sign in will be given through some other account made in other portal is called open authentication. Here during authentication third party plays a vital role. This paper is throwing light towards open authentication and cost optimized by it, with respect to simple authentication or authorization based services.*

***Keywords***- Open authentication, Optimization, Authorization, Centralized.

## I. INTRODUCTION

Now a day's security and privacy are the highly concerned characteristics of the systems, software, products and services. When dealing with multiusers and heterogeneous groups of user it is highly demanded that system must show higher level security protocol. The need of system security becomes more important when we have a set of users those may differ with respect to their accessing and right on date and its properties. When there are heterogeneous groups of users at that situation a set of users are given right of write, read and modification rights as per demand of the system. Thus there must be a mechanism by which this isolation can be performed. Here it is become more crucial how to isolate the system and how to identify a user. The rights of users may vary as per their category. It is highly expected that a system must perform identification of such user group and restrict their action by limiting their circumstances. These limiting actions are done by allocating the different token to different groups of users. Thus token become the right identifier and a gateway by which this action has been completed.

Authentication is the process under which the verification of the token has been done. This verification uses ID and Password (credentials) by which system derives right of access and right of modification, updating etc. This work (Product) is based on system authentication and authorization where desired demand is to provide open authentication.

## II. LITERATURE REVIEW

G. Liang et al. has emphasized that how to get authenticated by RAS based file encryption [1]. Necessary items needed for authentication are saved in RAR file which will be in encrypted form. In this study authors has focused over the authentication based on third part but no analysis over authorization has been done. Research focuses over scheme for RAR based authentication.

In [2] G. Kaur and D. Aggrwal have discussed about Open authentication 2.0 where authentication of client with third party has been done. H ere third party plays a vital role towards the authentication. In the study research underlines the resource owner, resource server, protocols and access needed for authentication. Research concluded that 2.0 o-auth is more secure and reliable than other authentication approaches.

In "Survey of Authentication and Authorization based on OAuth", K. Jam et.al have discussed about how the open authentication based services work. How these services get affected by the elementary variables. They concluded their research by claiming in order to reduce the task human and eliminating human interaction with systems. Research claims that insertion of IOT will become easier to adopt through O-auth services [3].

## III. ANALYSIS

As far as literature review for this paper is to be concern it has been performed over online literatures. Instead of focusing over literature, here the analysis over some leading social sites/ portals has been done..

A. *Facebook*- It is the leading social network among all. It has highest number of users.
B. *Instagram*- It is highly used media sharing platform.
C. *LinkedIn*-The largest social site of professionals.

D. *Twitter*-The biggest platform of content and thought sharing.
E. *MP Online*-Government portal of Madhya Pradesh Government.
F. *EdX*-Biggest online learning platform. Highly used by professionals and students.
G. *Amazon*-It is most rich site in order to providing Product as a service and Platform as a service.
H. *Flipkart*-Leading service providers in India, Shopping site.
I. *Gmail*- The biggest search engine in the globe. It is facilitating services, space and products.
J. *Yahoo*- The most popular search engine in 90's

Here is the summary of table 1 is shown in table 2 where number of occurrence of particular features are summarized among all 10 based sample space. Table 1 shows details of the site and features found on them. Some of the features are not common those are mentioned in the last column. Right mark (✓) indicates feature found on them. Some of the features are not common those are mentioned in the last column.

| *Site name link* | *Logo* | *Password /login* | *Remember me* | *Forgot password* | *Password Reset* | *Registration* | *login with other site* |
|---|---|---|---|---|---|---|---|
| Facebook | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | |
| Instagram | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ |
| LinkedIn | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ |
| Twitter | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | |
| MP Online | ✓ | ✓ | | ✓ | ✓ | ✓ | |
| EdX | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Amazon | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | |
| Flipkart | ✓ | ✓ | | ✓ | ✓ | ✓ | |
| Gmail | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Yahoo | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | |

Table 1. Table of survey done on social sites home page

| *Features* | *Number of Occurrence out of 10* | *Probability* |
|---|---|---|
| Logo | 10 | 1 |
| User Name | 10 | 1 |
| Remember Me | 6 | 0.6 |
| Forgot Password | 10 | 1 |
| O-Auth | 4 | 0.4 |
| Password Reset | 10 | 1 |
| Registration | 10 | 1 |

Table 1. Table of occurrence of features out of 10

Graphical summary of feature found is mentioned in the figure 1 below, where it is clear that forgot password, password reset, registration and logo are the most common features noticed in study. Open authentication has 0.4 as its probability, which decides its occurrence.

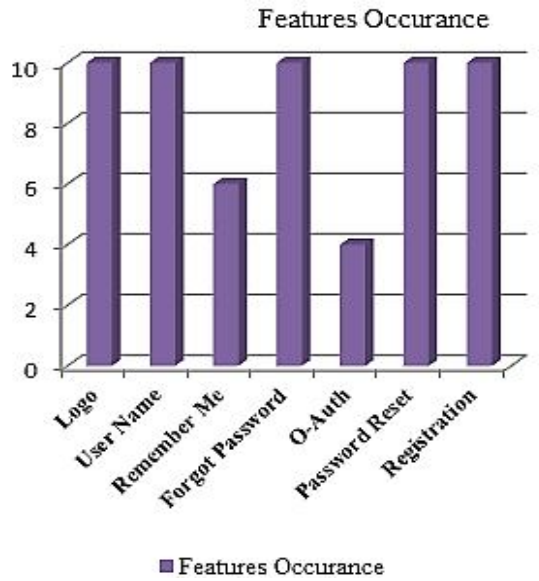


**Figure 1. Graphical representation of features found in study**

Among all ten features few features are actually compulsory to exist. Some features are generating redundancy of data, which may cause web garbage. Certain features are in such a way those are implicitly binding some more features which are generating overhead. Features like login with other site may reduce the overhead of registration. It will reduce multiple passwords which will reduce the overhead of maintaining multiple reset passwords, forgot password based services.

*A. Registration cost*

At the moment when, a user get register in any of the portal a record i.e. a tuple in relation has been made for him/ her. This tuple may be associated with some more relations. Here system needs to take-care that tuple until user will deactivate his/ her account. Here ultimately a cost of time, space, data management scheme etc. has been paid for that particular user.

*B. Cost of password reset and forgot password maintaining service*

A registered user must be provided the service like reset password, forgot the password etc. thus it is highly demanded to maintain a scheme that will handle these

services. If password reset services are implemented they may cause creation of more tables and procedures to go through the database.

*C. Taking care of redundant data*

Same user performs registration in so many portals / websites. It may cause the multiplicity of the same data in the web. Thus system need to take care of these data sets those may cause redundancy.

*D. Cost of processing same data*

Since the data is available at various warehouse thus it need to be processed independently. It actually increases the cost of system maintenance and processing cost as well.

*E. Decentralized data maintenance scheme*

Multiplicity of the data increases the overhead of facilitating all facilities to the same data. If centralized login scheme i.e. open authentication is used these overheads can be reduced up to some extent.

## IV. RESULTS AND DISCUSSION

As per analysis it is clear that the in general authentication, there are so many costs those are cumulating together and are making the system more costly. In such situations there is need of a system which can reduce the cost of all above mentioned factors. Here Table 3 represents the cost optimized through open authentication. Proposed model based cost optimization is given below.

| Feature / Cost taken | Level of Optimization | | | | |
|---|---|---|---|---|---|
| | *Less than satisfactory* | *Satisfactory* | *Good* | *Very good* | *Highest* |
| Power | | | | ✓ | |
| Maintenance | | | | ✓ | |
| Reset Password | | ✓ | | | |
| Developing | | | ✓ | | |
| Forgot password | | ✓ | | | |
| Security | ✓ | | | | |
| Authentication | | | | ✓ | |
| Web garbage | | | | | ✓ |
| Redundant data | | | | ✓ | |
| Multiplicity | | | | | ✓ |

Table 3. Table of optimized cost levels

From the table 3 it is clear that web garbage and data multiplicity have been optimized up to highest level. Cost of power, Maintenance cost, Authentication and redundancy of the data have been improved up to very good level. There is no improvement in security has been done while reset and forgot of the password have improved up to a marginal level.

## V. CONCLUSION

As analysis was done there were some certain objectives those are achieved in the research. Cost optimizations are done for the features were noticed highly affecting the system performance. This cost optimization not only improves the system's performance but also the system which supports both homo and heterogeneity.

It is clear that highest improvement is achieved in the cost of taking care of data multiplicity and unnecessary data kept on web. Reset password and forgot password were improved up to a level of satisfactory i.e. partial improvement has been noticed. In development cost there is a positive optimization has been found, it's because of no need to develop same code for same task. Power, maintenance and redundant data management have been improved a lot. Since no need to create multiple accounts this will already decreases all associated costs of redundant data. A thing which is not too improved is security. Improvement on security level hasn't been done so far, since it was not our premier concern.

## REFERENCES

[1] Liang Ge, Lianhai, Wang, "Research of Password Recovery Method for RAR Based on Parallel Random Search", Springer ATIS, CCIS 490, pp 211-248, 2014.

[2] G. Kaur, D. Aggarwal, "A Survey Paper on Social Sign-On Protocol O-Auth 2.0",ournal of Engineering, Computers & Applied Sciences (JEC&AS),Volume 2, No.6,pp. 93-97,2013.

[3] K. Jam, A. Mistry, A. Shah, A. Ganatra, "Survey of Authentication and Authorization based on OAuth", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 5, Issue 3, March 2017.

[4] B. Gowrigolla, S. Sivaji," Design and auditing of Cloud computing security", Information and Automation for Sustainability (ICIAFs), 2010 5th International Conference, Dec. 2010, pp.292 - 297

[5] S. Dubey, K. Mathur, "Comparative Performance Analysis of Binary Search in Sequential and Parallel Processing "International Journal for Research in Applied Science & Engineering Technology (IJRASET),ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887,Volume 5, November 2017.

[6] B. Leiba, "O-Auth Web Authorization Protocol ", www.computer.org/internet computing, Vol. 16, No. 1.February, 2012.
[7] F. Yang, S. Manoharan, “A security analysis of the OAuth protocol”, 2013 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM), Victoria, BC, pp. 271-276, 2013.
[8] L.Seitz, S.Gerdes,“Authentication and Authorization in Constrained Environments”, SICS Swedish ICT,Internet Engineering Task Force(IETF),ISSN:2070-1721 Philips Research January 2016.