**OAuth 2.0 framework Authorization Process (May 2020)**

**H M P K Ranjan Kumara Herath**

**Faculty of Computing**

**Sri Lanka Institute of information Technology**

**Malabe, Sri Lanka**

**MS20911058@my.sliit.lk**

**Abstract –** **In this paper emphasized that security of Information Technology of public network in aspect of security impact to a client and the resource server which is use art of the technology implementation of this era called Oauth framework 2.0. This RFC 6749 protocol standard particularly restricted the third party applications through HTTP services without authorization from the respective resource owner. In fact, it is a challenge of the expertise in this new era due to the complexity of the software industry and as well as aspect of the client requirement. A range of new sophisticated applications further create an uncertainty due to the vulnerabilities and exploitation of the threats unexpectedly. In this review is further illustrated the Oauth framework practically implemented with web applications how could compromised with Google Application Program Interface.**

**Key Words: Oauth 2.0 Framework, API, Resource Server, Resource Owner, Client, Authorization Server. Access Token, Authorization Request, Authorization Granted**

**I. INTRODUCTION**

Information security is based on very primitive but potential important three fundamental principles of security aspects such as confidentiality, integrity, and availability. They are the pillars of the information. Then the challenge would be implementation of the secure systems to prevent or mitigate such intentional misuse of the public or private properties.

Open Authorization (OAuth) is a protocol which is used to protected the data shared in a public platform such a as Google Drive API. Internet Engineering Task Force has been implemented a framework such as RFC 6749 by defining the standards protocol flow with proper steps of procedures.

The OAuth framework is illustrated mainly in four different services as following steps:

* Authorization requested from resource owner and directly granted to the client
* Sent the granted authorization to authentication server by requesting the token
* Issued the token by initializing the granted authorization
* Client requested the protected resources for the given token
* Resource server validate the access token, if valid grants the service

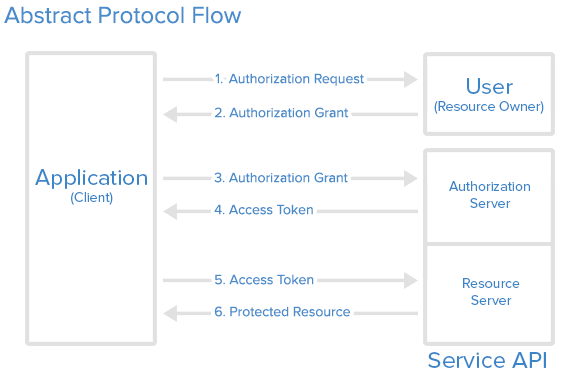


Figure 1 OAuth 2.0 Protocol Flow

1. **OAUTH ROLES:**

* Resource Owner
* Client
* Resource Server
* Authorization Server

1. **ACCESS TOKEN:**

Access token is credentials which are access protected resources. It is denoted as unidentified some encrypted date or signature in variable manner. Server can be identified both name and the password in it. Access token basically two formats such as structures and method of utilization whereas cryptographic properties.

**II. OBJECTIVES**

OAuth framework is critical for network security and quite new for many users however to be concern to protect unexpected threats exploitation of the client data. Mainly focus on here to emphasized the practically shows the application of the OAuth process in technically with created application. It is obvious that many difficulties to be faced to overcome issues and uncertainty circumstances happening such configurations and installation process. In the latter part of the review allocate the space to discussed further problems in the real issues.

**III. OAUTH PROCESS**

There are many important terminologies to be simplified on this process for learning perspective before further evaluation.

1. **HTTP REDIRECTIONS**

Critical part of the Oath flow is the redirection the URL to another destination. After successful authorization an application the authorization server redirect the user - agent according to the access code or access token in the URL. Due to the criticality of the data in the redirected URL doesn’t redirect the user arbitrary details.

1. **APPLICATION REGISTRATION**

Application should be registered with the service before using the OAuth. This process to be done via a registration form in the “developer” or “API” of the service’s website by providing the information as application Name, Application Website and the Redirect URI or Callback URL

1. **CLIENT ID AND CLIENT SECRET**

After registration of the application, in the form of client identifier and a client secret will issue the client credentials. The client ID is publicly exposed which is used by service API identify the application and also used to build authorization URL to users.

**IV. AUTHENTICATION GRANT**

In the figure 1 shows the first steps such as cover obtaining an authorization grant and access token.

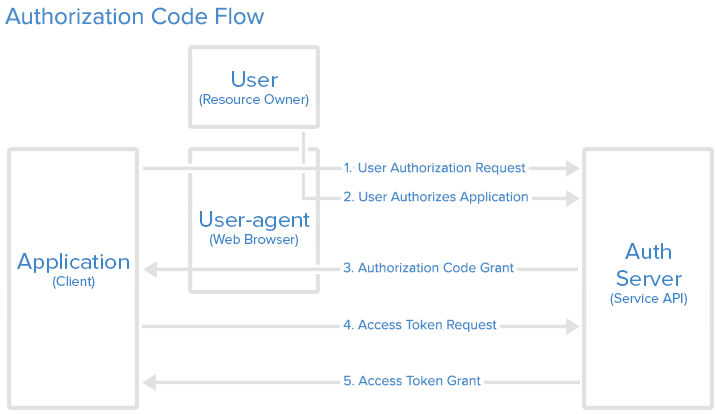
Here are the OAuth 2 authorization grant types:

* **Authorization Code**: used for server-side Applications
* **Implicit**: used for Mobile Apps or Web Applications
* **Resource Owner Password Credentials**: used for trusted Applications
* **Client Credentials**: used with Applications API access

Now we will describe grant types in more detail, their use cases and flows, in the following sections.

1. **AUTHORIZATION CODE**

For optimization of the server-side applications the **authorization code** grant type is being used apart of that it can be maintained the client Secret confidentiality. Authorization code is a process of redirection such as implication of interacting with the web browser (user-agent) and receiving API authorization codes.

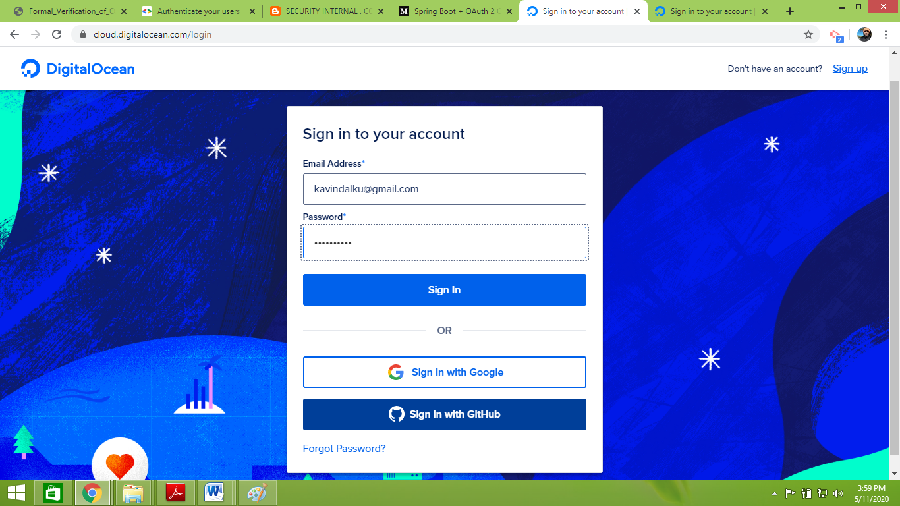


**Figure 2 Authorization code flow**

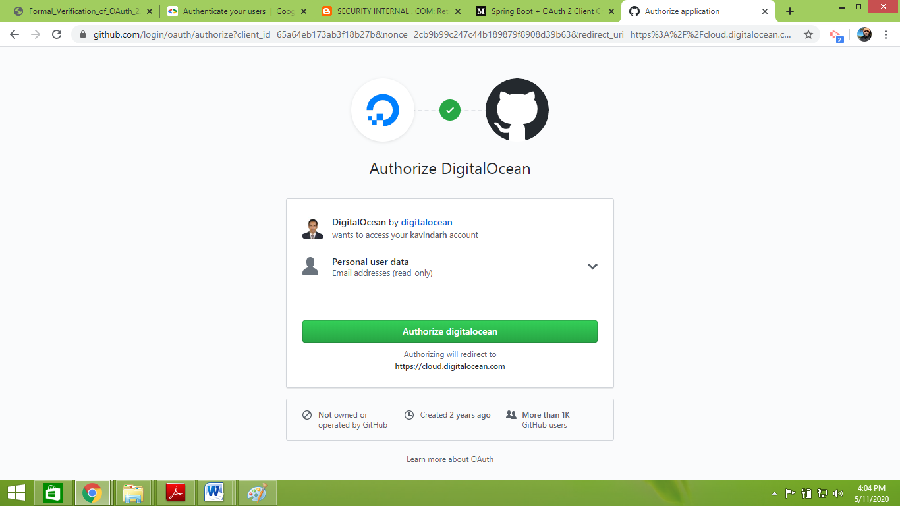
1. **AUTHORIZATION CODE LINK**

User must give the authorization as shown in the figure 3

https://cloud.digitalocean.com/v1/oauth/authorize?response\_type=code&client\_id=CLIENT\_ID&redirect\_uri=CALLBACK\_URL&scope=read

****

**Figure 3 Authorization Code Link**

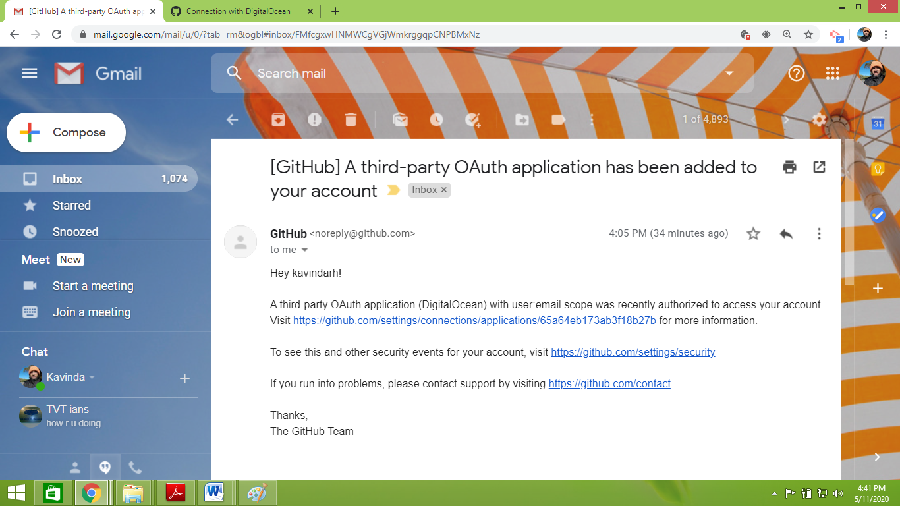
****

**Figure 4 Authorized Digital Osean**

1. **USER AUTHORIZED APPLICATION**

Click the link to get into the service then authenticate the identity then they will prompted the service authorized or deny the access. Figure 4 shows the authorized.

### APPLICATION RECEIVES AUTHORIZATION CODE



**Figure 5 Authorized Application**

User must click the authorized application to redirect the user –agent applications of URL

### APPLICATION REQUESTS ACCESS TOKEN

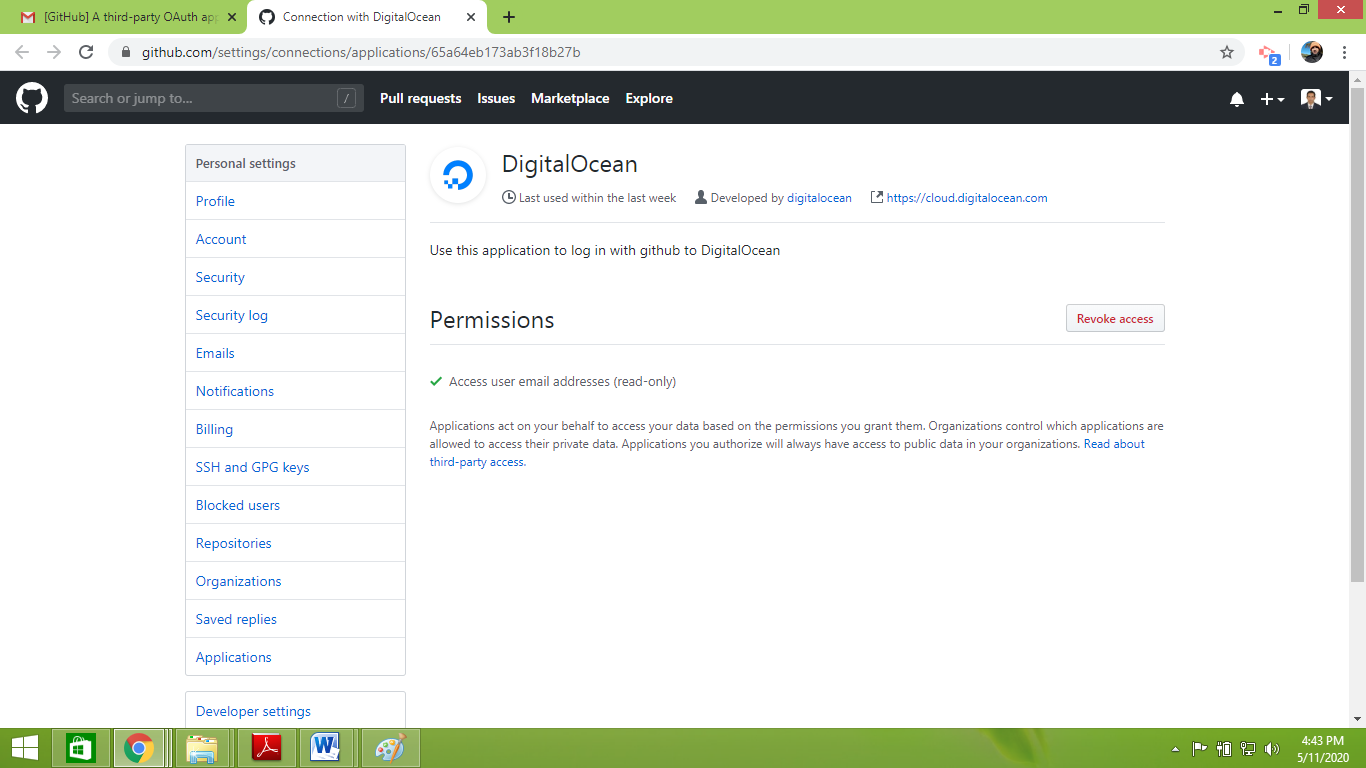
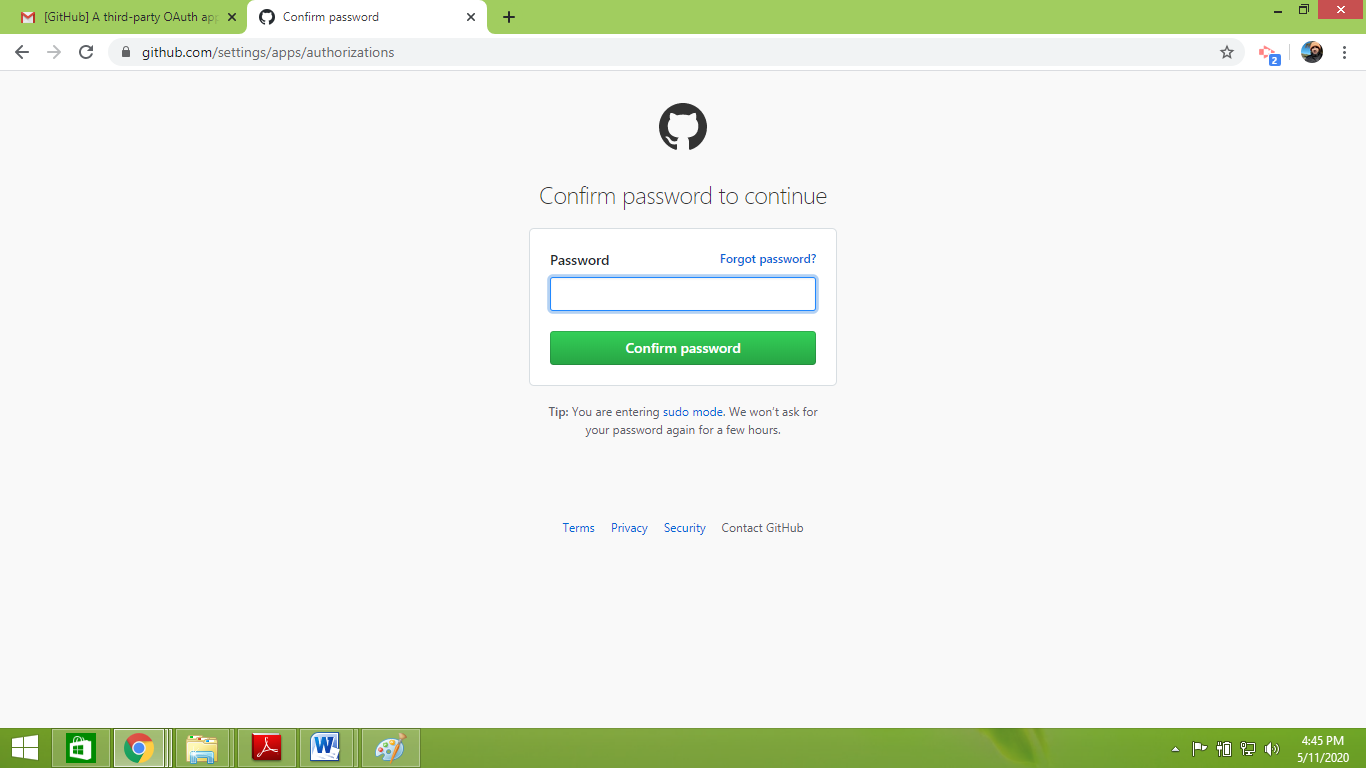


Figure 6 Access permission

### APPLICATION RECEIVES ACCESS TOKEN



**Figure 7 Authentication**

**IX. CONCLUSION**

Except of traditional or legacy encryption methodologies, OAuth would be a standard protection mechanism for critical data and information in this era.

Along with IPSec VPN, there are several other successful techniques which are useful to mitigate the threats on public networks. Firewall and IPSec gateways are the devices which have become sophisticated network elements required for enterprise an as well as small networks. Firewalls dedicated to protect the front of the network by controlling and filtering the traffic which is identified as the unwanted source coming from and as well as going out to the other network. Zero vulnerability of the applications is practically not possible however risk level can be minimal since followed by the international standards and good practices. Cyber security is the dedicated subject area where attempt to more and more research to rectifying further solution on information security. Realistic of this master course is to become a master of the ethical hacker.

**X. REFERENCES**

# [1] D. Hard, Internet Engineering Task Force (IETF) “ The OAuth 2.0 Authorization Framework” RFC 6749, Microsoft, Category Standards Track ISSN: 2070-1721, October 2012.

[2] OKTA <https://www.oauth.com/oauth2-servers/redirect-uris/>

# [G. Pernul](https://www.sciencedirect.com/science/article/abs/pii/0268401295000105#!), “Information systems security: Scope, state-of-the-art, and evaluation of techniques”, [International Journal of Information Management](https://www.sciencedirect.com/science/journal/02684012), [Volume 15, Issue 3](https://www.sciencedirect.com/science/journal/02684012/15/3), Pages 165-180, 22 December 1999

## [2] C. Onwubiko† and A. P. Lenaghan, “Managing Security Threats and Vulnerabilities for Small to Medium Enterprises”, Networking and Communications Research Group, Faculty of Computing, Information Systems and Mathematics, Kingston University, Penrhyn Road, Kingston Upon Thames, London, KT1 2EE, UK

[3] Bhrouz A. Forouzan, “Cryptography and network security”, The McGraw Hill Company, Tata McGraw-Hill publishing company limited, in India.

[4] Vijay Bollapragada, Mohamed Khalid, Scott Wainner “IPSec VPN design”, In Security, 800 East 96th Street Indianapolis, IN 46240 USA, Cisco Press, April 2005, (22-52)

[5] R. L. Rivest, A. Shamir, and L. Adleman , “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems” MIT Laboratory for Computer Science and Department of Mathematics, pages (120-126)

[6] Stefan Jakoubi , Simon Tjoa , Gernot Goluch , Gerald Quirchmay, “A Survey of Scientific Approaches Considering the Integration of Security and Risk Aspects into Business Process Management”, Secure Business Austria, University of Vienna, 3 University of South Australia

[7] Miltiadis Kandias, Nikos Virvilis, Dimitris Gritzalis, “The Insider Threat in Cloud Computing”, Information Security & Critical Infrastructure Protection Research Laboratory, Dept. of Informatics, Athens University of Economics and Business, Greece

## [8] Joe Levy, “Victories against cybercrime demand radical change to defense” Sophos Sophos labs 2019, Threat report,

[9] J.P. McDermott, “Attack Net Penetration Testing”, Department of Computer Science, James Madison University, Harrisonburg, Virginia 22807.

## [10] [Rossouw Von Solms](https://www.mendeley.com/authors/55970955300), “Information Security Governance: A model based on the Direct–Control Cycle”, [Computers & Security](https://www.sciencedirect.com/science/journal/01674048), [Volume 25, Issue 6](https://www.sciencedirect.com/science/journal/01674048/25/6), September 2006, Pages 408-412

**INDEX**