

# Detection of Sybil Attacks in Structured P2P Overlay Network

Manjari Kaushik  
M.Tech Student  
Department of CSE  
UTU Dehradun, India

Kamal Kr. Gola  
Department of CSE  
College of engineering  
TMU Moradabad, India

Gulista Khan  
Department of CSE  
College of engineering  
TMU Moradabad, India

Rahul Rathore  
Department of CSE  
College of engineering  
TMU Moradabad, India

## ABSTRACT

The Sybil attack in computer security is an attack where in a reputation system is subverted by forging identities in peer-to-peer networks. The name was suggested in or before 2002 by Brian Zill at Microsoft Research. In a Sybil attack the attacker subverts the reputation system of a peer-to-peer network by creating a large number of pseudonymous identities, using them to gain a disproportionately large influence. A reputation system's vulnerability to a Sybil attack depends on how cheaply identities can be generated, the degree to which the reputation system accepts inputs from entities that do not have a chain of trust linking them to a trusted entity, and whether the reputation system treats all entities identically. Main motto is to secure the Peer to Peer network (P2P) by Sybil attackers. Considering more parameter for labeling a node 'genuine' or 'Sybil'. Our system has two server one is main server and another is trusted server. Trusted server is act as a centralized server so it has the complete list of members with their details. So when the new member is added to the network, trusted server take the identity check test with its database by checking the new member details with the complete database. If it found common parameters then it label that member as Sybil otherwise genuine.

## General Terms

Security.

## Keywords

Sybil Attacks, P2P Overlay Network, Server, Dot Net.

## 1. INTRODUCTION

A Sybil attack in computer security is an attack in which an intentionally mischievous node on a network, felonious claims to be several different nodes concurrently. Many disseminate applications and services, from day to day assumed that each participating entity, controls exactly one identity. In this report, we investigate the Sybil attack, i.e. a dangerous attack in distributed peer-to-peer networks. Almost dispense peer-to-peer systems were based on a very common assumption that each participating entity has controls exactly one identity. In an extensive scale peer-to-peer system, a direct connection is impossible between each pair of nodes is, therefore, the nodes participating create networks usually, and via the relay operations of multiple intercessor nodes message is transmitted from one node to another node. Whenever the assumption cannot get fulfilled, the system lead to Sybil attacks. In this Sybil attack, a dispute, creates a large number of false or duplicate identities. Since all the Duplicate identities are controlled by the opponent, It can be introduce a substantial number of false opinions into the system, and convert it by making decisions which are benefiting system itself. When attacker creates many identities, it can easily change the overall popularity of an option through Sybil ids.

Peer-to-Peer networks are distributed systems. Different types have been defined as and flat Peer to peer network and hierarchical Peer to Peer network. P2P networks are virtual overlay networks built on an underlying network. The main difference between them is based on how many levels, the network topology is utilizing. Hierarchical P2P network is utilizing multiple levels of hierarchy to distribute the overlay node and it can be classified into three categories: structured, unstructured, and hybrid networks. In this, we will just focus on the hierarchical type of network. They are consisting of inter related nodes which are able to be self-organized into network topologies, and with purpose of sharing the resources such as content, CPU cycles, storage and bandwidth, without requiring any support of a global centralized server or authority and accommodating transient populations of nodes while maintaining allowable connectivity and performance .

## 2. LITERATURE REVIEW

Rakesh G.V , Shanta Rangaswamy , Vinay Hegde , Shoba G et.al.[1] .The Sybil attack is an attack where a person as an opponent creates multiple type of Duplicate and False identities to arbitrate, the running of the system. Including the false information by the forgery entities, a system is being misled by the antagonist into making decisions benefitted .Most peer-to-peer systems are vulnerable to Sybil attacks.

Haifeng Yu Michael Kaminsky Phillip B. Gibbons Abraham Flaxman et.al.[2] Peer-to-peer distributed systems are known to be particularly vulnerable to sybil attacks. In a sybil attack, a malicious user obtains multiple fake identities and pretends to be multiple, distinct nodes in the system. By controlling a large fraction of the nodes in the system, the malicious user is able to "out vote" the honest users in collaborative tasks such as Byzantine failure defenses. This paper presents Sybil Guard, a novel protocol for limiting the corruptive influences of Sybil attacks. This protocol is based on the "social network" among user identities, where an edge between two identities indicates a human-established trust relationship.

Roopali Garg , Himika Sharma [3], In this research, the author has implemented the Lightweight Sybil Attack Detection technique which is used to detect the Sybil nodes in the network and also discussed the proposed work with implementation which is used to improve the existing Lightweight technique. Simulation tool used for the implementation is MATLAB.

Himadri Nath Saha, Dr. Debika Bhattacharyya, Dr. P. K.Banerjee[4] :- Sybil attack is a serious threat for today's wireless adhoc networks. In this work, the author attempt to provide a hybrid solution using a combination of two already proposed methods. In this attack a single node impersonates several other nodes using various malicious means. According to this newly proposed method, the total network will be dynamically divided into several subgroups, as more and

more nodes will enter the network. Each subgroup will also contain RSSI detector nodes. Each subgroup will be under the super vision of a single node, a central authority.

Anuja Motarwar, Prof. Amresh Kumar [5]:- In this paper, the author analyze fake identity in network which is created by Sybil attack by detecting its source. Analysis have found some solution that include the communication among the nodes of cluster and analyze the results in different scenarios like fake sender detection, fake receiver blocking, node to node secure connection and packet acceptance and rejection process.

A. Muruganandam1, R. Anitha[6] -Ad hoc routing protocols are used to find a path end-to-end through the cooperative network. This research focuses on the Sybil Attack Detection of Wireless Sensor Networks. Sybil Attack may act indifferent ways such as threading, voting system, fair resource allocation, etc. In a Sybil attack, single node presents different multiple fake identities to different other nodes present in the network. And In proposed method, the author had used Passive Ad Hoc Identity Method and Key Distribution by using Neighbor Discover Distance Algorithm. This work used throughput, delivery ratio, delay time and energy efficient parameters to differentiate the results and to improve the overall performance of secure data transmission on Wireless Sensor Network.

Hussain et al. [7]:- presented a scheme in which they detect not only Sybil attack but also privacy is preserved of a node. Authors then also introduced a very new term called as Event Reporting Message (ERM). These ERMs are supported by the RSU, to get suspected Sybil nodes in its range and afterwards the RSU reports, those nodes for revocation authority. In this scheme, pseudonym-less beaconing is then used to preserve privacy of node and a temper resistant module is used to carry out pre-assembly analysis of data for Sybil attack detection, this data is used to assemble beacons. In this defined scheme RSUs then distributes authorized tokens to benign the vehicles and then report ERMs by using those tokens node. RSUs collect those ERMs for particular event and checks if, more

than one ERMs contain the identical token or not. If RSU found such type of ERMs, it reports those ERMs to revocation authority. In turn revocation authority takes particular action against those nodes.

### 3. PROPOSED ALGORITHM

1. First we created the main server who has its own database.
2. Then the main server created the trusted server and the main server has it unique ID and details.
3. Now, suppose the new member came with the request to join the group and send request to the trusted server. (For all the new members join the group or send request to the group, for all of them the trusted server is act as the main server)
4. The trusted server sends the group joining form with the unique ID.
5. New member fill the form and send back to the trusted server.
6. Now the trusted server checks the details filled by the member with their database.
7. This check is performing on the different parameters like house no., mobile no., landline no., email ID and so on...
8. While the check perform we leave some parameter like name, city, and state because these parameter are commonly same with the other members.
9. Now once this checking is done, then the trusted server decide that this member is Sybil or genuine and label them.
10. If the member is genuine, then only he/she will join the group.
11. Otherwise the request is rejected and label it as 'SYBIL'

### 4. IMPLEMENTATION

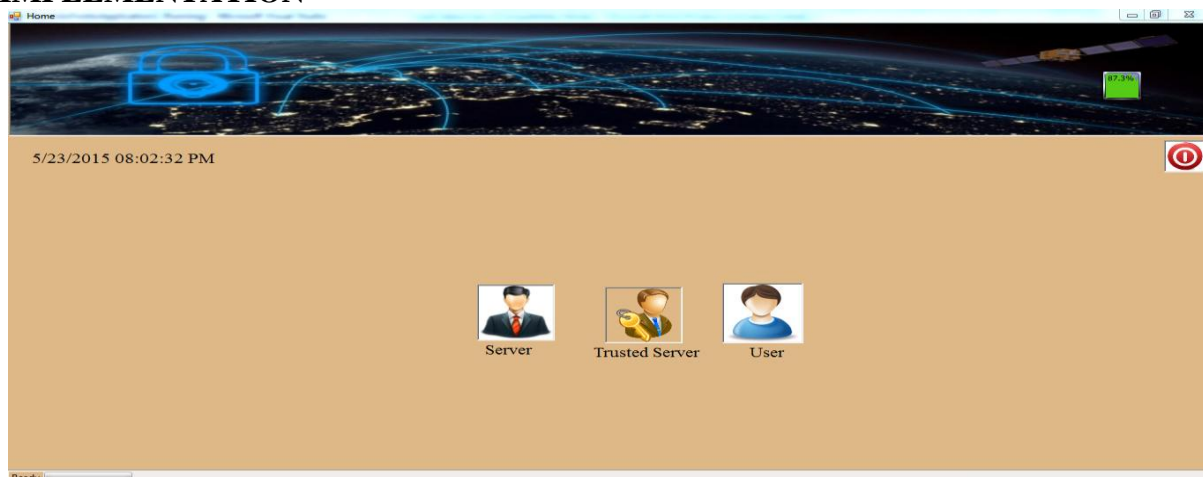
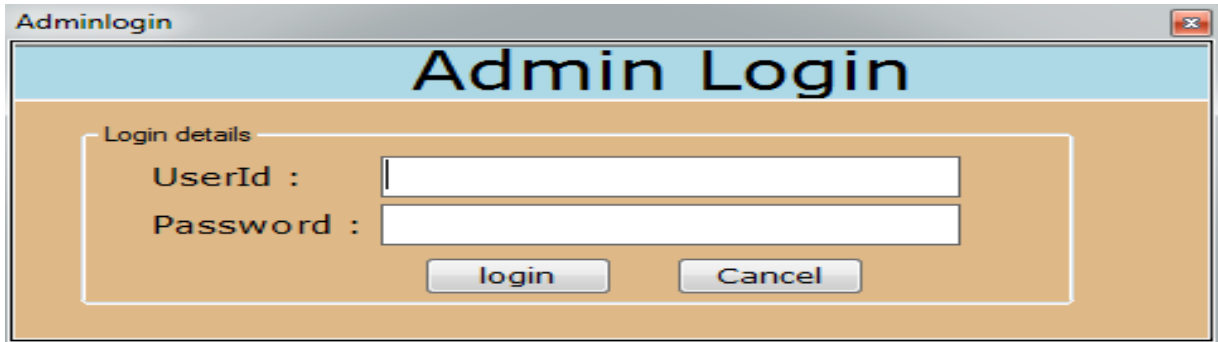
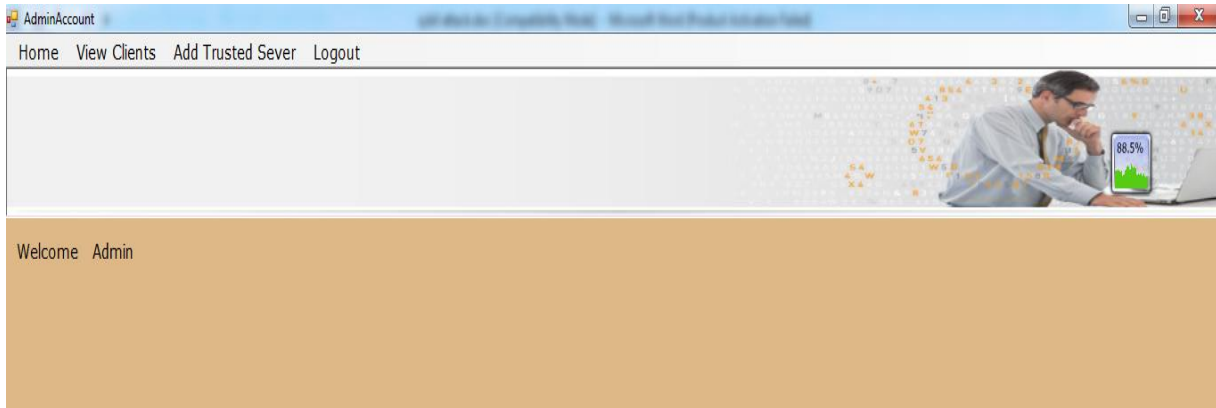


Fig 4.1 Home Page



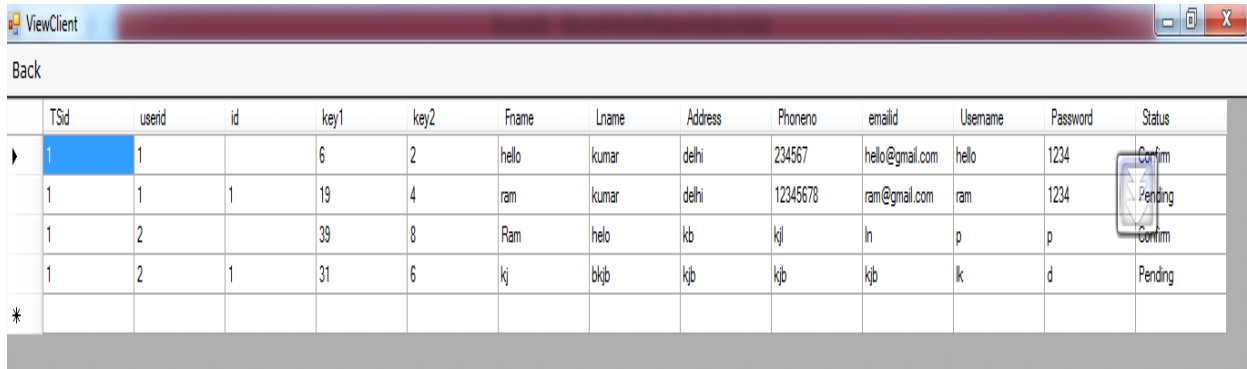
The image shows a web browser window titled "Adminlogin". The main heading is "Admin Login". Below the heading, there is a section titled "Login details" which contains two input fields: "UserId :" and "Password :". Below these fields are two buttons: "login" and "Cancel".

Fig 4.2 Admin Login Page



The image shows a web browser window titled "AdminAccount". The navigation menu includes "Home", "View Clients", "Add Trusted Sever", and "Logout". Below the menu is a banner image of a man in a white shirt and tie sitting at a desk with a laptop, with a tablet displaying "88.5%". Below the banner, the text "Welcome Admin" is displayed.

Fig 4.3 Admin Page



The image shows a web browser window titled "ViewClient" with a "Back" button. Below the button is a table with 13 columns: TSid, userid, id, key1, key2, FName, Lname, Address, Phoneno, emailid, Username, Password, and Status. The table contains 5 rows of data, with the first row highlighted in blue. A "Confirm" button is visible over the table.

TSid	userid	id	key1	key2	Fname	Lname	Address	Phoneno	emailid	Username	Password	Status
1	1		6	2	hello	kumar	delhi	234567	hello@gmail.com	hello	1234	Confirm
1	1	1	19	4	ram	kumar	delhi	12345678	ram@gmail.com	ram	1234	Pending
1	2		39	8	Ram	helo	kb	kj	ln	p	p	Confirm
1	2	1	31	6	kj	blkb	kjb	kjb	kjb	lk	d	Pending
*												

Fig 4.4 View Chart



The image shows a web browser window titled "Trusted Server". It has a "Back" button. Below the button are three input fields: "Id :", "UserId :", and "Password :". Below these fields are three buttons: "Save", "Update", and "Delete". At the bottom, there is a table with 3 columns: "Trusted Server Id", "UserName", and "Password".

Trusted Server Id	UserName	Password
1	h	h

Fig 4.5 Trusted Server

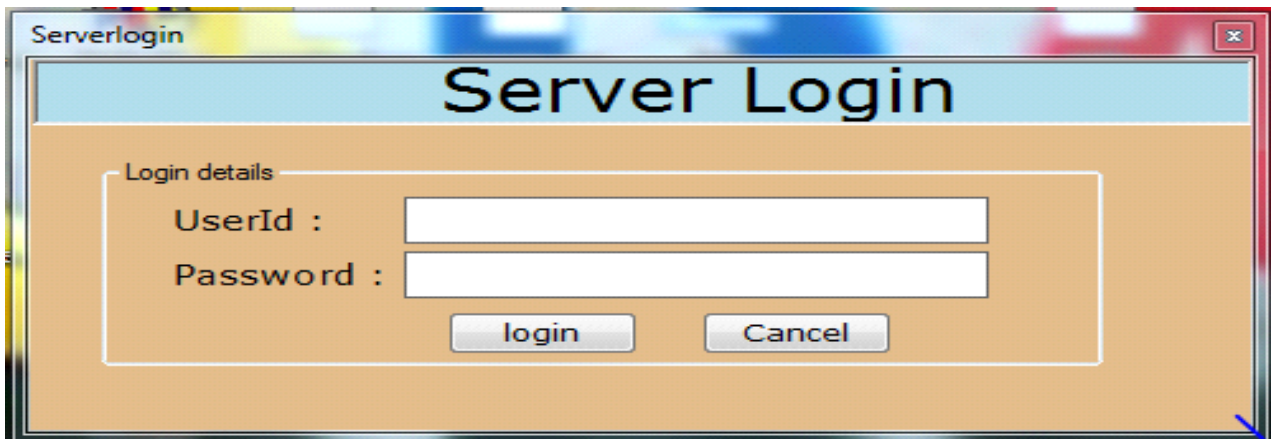


Fig 4.6 Server Login



Fig 4.7 Server Page

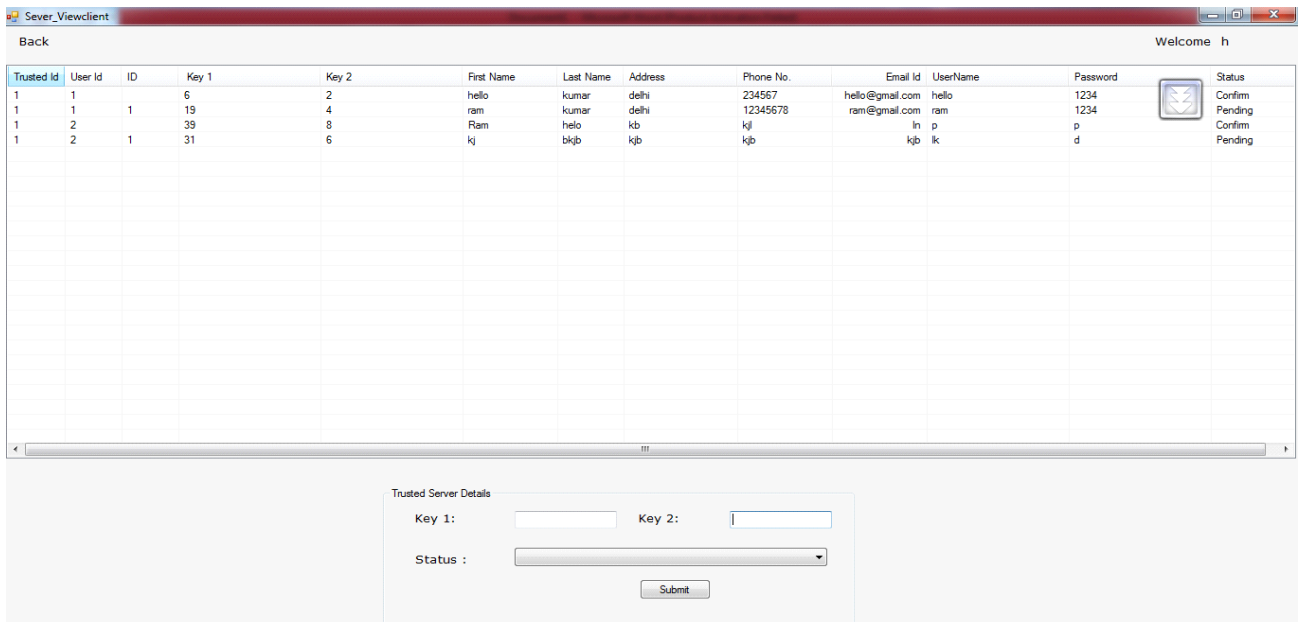


Fig 4.8 Details of Trusted Server



Fig 4.9 Add User Page

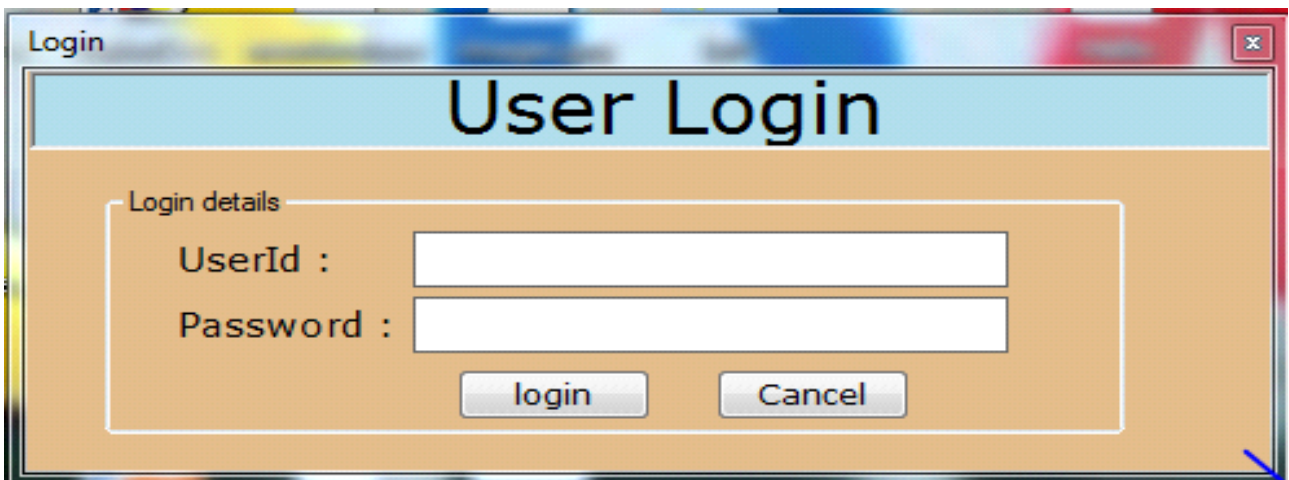


Fig 4.10 User Login Page



Fig 4.11 User Account Page

## 5. CONCLUSION

This idea behind the observation was taken when we are concerning that how to secure the structured P2P overlay network from the attack i.e. security attack without any coordination. We are completely certain about the knowledge about systems which had failed can help us to build the system that fight against the failure. This work explain us an overview about different categories of hierarchical P2P

system. It then took an extensive vital security attacks, frightening the function of structured P2P networks. We categories these attacks in two major main groups: Specific structured P2P network attacks and the General network attacks. Finally, we close this observation and survey with the conversation of different links between- attacks and thus we confirm ensuring that the structured P2P overlay network will be suitable and sufficient involves, the balancing of different

factors such as trust, privacy and security. Therefore, the evolution of appropriate, security measures are mandatory. In this study, we could affirm that, existing structured P2P overlay networks had still away from the safe utilization.

## **6. REFERENCES**

- [1] Rakesh G.V , Shanta Rangaswamy , Vinay Hegde , Shoba G,” A Survey of Techniques to Defend Against Sybil Attacks in Social Networks”, *International Journal of Advanced Research in Computer and Communication Engineering* Vol. 3, Issue 5, May 2014 .
- [2] R. Amuthavalli, dr. R. S. Bhuvaneshwaran,” detection and prevention of sybil attack in wireless sensor network employing random password comparison method”, *journal of theoretical and applied information technology* 10th september 2014. Vol. 67 no.1.
- [3] Roopali Garg , Himika Sharma,” Proposed Lightweight Sybil Attack Detection Technique in MANET”, *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (An ISO 3297: 2007 Certified Organization)* Vol. 3, Issue 5, May 2014 .
- [4] Himadri Nath Saha , Dr. Debika Bhattacharyya , Dr. P. K.Banerjee,” Semi-Centralized Multi-Authenticated RSSI Based Solution to Sybil Attack”, *International Journal of Computer Science & Emerging Technologies (E-ISSN: 2044-6004)* 338 Volume 1, Issue 4, December 2010.
- [5] Anuja Motarwar, Prof. Amresh Kumar,” Study on Detection of Sybil Attack in Wireless Sensor Network”, *International Journal of Advanced Research in Computer Science and Software Engineering* Volume 3, Issue 12, December 2013.
- [6] A. Muruganandam1 , R. Anitha,” Passive Adhoc Identity for Sybil Attack Detection Using NDD Algorithm”, *International Conference on Computing and Intelligence Systems* Volume: 04, Special Issue: March 2015.
- [7] Rasheed Hussain, Heekuck oh, “On Secure and Privacy Aware Sybil Attack Detection in Vehicular Communication”, *In Journal of Wireless Personal Communication*, DOI: 10.1007/s11277-014-1659-5.
- [8] [https://en.wikipedia.org/wiki/Sybil\\_attack](https://en.wikipedia.org/wiki/Sybil_attack)