International Journal of Research Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

Comparable Decision-Based Expression on Association Model in node to node E-Commerce System

Mr. Kandunuri Ramakrishna
Ph.D. Research Scholar,
Sri Satya Sai University of Technology & Medical Sciences(SSSUTMS), Sehore, Madhya Pradesh, India.
Assistant Professor, KG Reddy College of Engineering and Technology, Hyderabad, India

Mr. Rokesh Kumar Y
Ph.D. Research Scholar,
Sri Satya Sai University of Technology & Medical Sciences(SSSUTMS), Sehore, Madhya Pradesh, India.

Mr. U.Rakesh, assistant professor,
Department of Computer Science Engineering and Technology
SV Engineering college for women, Andhra Pradesh, India

Abstract: In this paper, we work exploits the neighbor similarity trust relationship to deal with Sybil attack. In this procedure, duplicated Sybil attack friends can also be recognized because the neighbor nodes end up acquainted and for this reason further relied on to one another. In this project, I suggest the usage of neighbor similarity trust in a group node to node e-commerce established on interest relationships, to remove maliciousness between the nodes. The interest founded group infrastructure nodes have a neighbor similarity trust in the middle of each other. Therefore they are capable of preventing Sybil attack. Sybil Trust gives a better relationship in e-commerce transactions as the nodes create a link between node neighbors. This provides an important avenue for nodes to advertise their products to other interested nodes and to know new market destinations and contacts as well. Also, the group enables a node to join node to node ecommerce network and makes identity more difficult. The focus is on the active attacks in node to node e-commerce. When a node is compromised, all the information will be extracted. Security and efficiency evaluation suggest that Sybil attack can also be minimized with the proposed neighbor similarity belief.
Keywords- keywords: Sybil attack, anonymity, decentralized nature, scalability, encoder , decoder , node registration Find neighbor peer, Assign trust to neighbor, Sybil attacker, fault-tolerant, detector, tolerant memory.

*****

I. INTRODUCTION

node to node networks extend from verbal exchange structures like e-mail and instant messaging to collaborative content score, recommendation, and transport structures as with Face book, YouTube, and Bit-Torrent. They permit any person to sign up for the gadget without difficulty on the cost of belief, with very little validation manipulate. node to node overlay networks are acknowledged for their many preferred attributes like decentralized nature, openness, anonymity, decentralized nature, scalability, self-enterprise, and fault tolerance. Each node performs the dual position of the patron as well as server, which means that everyone has its very own manage. All of the resources that are made use of within the node to node infrastructure are contributed by the nodes themselves, not like conventional techniques wherein a central authority manipulation is used.

Nodes could collude and do all forms of malicious activities within the open-get entry to disbursed structures. Those malicious behaviors lead to service positivity degradation and economic loss amongst business partners. Nodes are at risk of exploitation, because of the open and near-zero prices of producing fresh identities. The identities of then dearer then utilized to influence the conduct of the system. But, if an individual faulty entity can gift a couple of identities, it can manage a significant fraction of the device, by that means undermining the redundancy. The variety of identities that an enemy can get into existence relies upon at the resources of the attacker consisting of memory, bandwidth, and operational energy. The aim of believe systems is to make certain that sincere nodes are accurately diagnosed as honest and Sybil nodes as unreliable which means that it is considered untrustworthy. To combine nomenclature, all the identities created by the malevolent users as Sybil nodes. In a node to node

e-trade software state of affairs, most of the belief concerns rely on the ancient factors of the nodes. The effect of Sybil identities may be reduced based totally on the ancient behaviour and references from different nodes. As an example, anode can deliver high-quality references to anode that is found out is a Sybil or malicious peer. This can decrease the effect of Sybil identities as a result reduces Sybil assault. Anode who has remained providing dishonest references will have its belief stage condensed. In case it reaches an expectant threshold point, then ode can be excluded from the collection. Each node has an identification, that is either genuine or Sybil.

A Sybil identity can be an identification owned through a user who is malicious, or it may be an identity which is stolen or bribed, or it might be a bogus identification obtained through a Sybil assault. Those Sybil attack nodes are hired to goal sincere nodes and for subsequently subverting the system. In Sybil attack, a single malicious consumer creates a large wide variety of identities of a node known as Sybils.

Those Sybils are used to launch protection assaults, each the utility level and on the overlay stage. At the software degree, these Sybils can target other sincere nodes even when transacting for them, whereas at the overlay degree, Sybils can disrupt the offerings offered by the overlay layer like routing, statistics storage, lookup, and many others. In believe systems, colluding Sybil nodes might also artificially grow peer's rating. Credence is one of the systems that depend on a trusted crucial authority to save from maliciousness.

Protecting in opposition to Sybil assault is pretty a difficult task. A node can faux to be relied on with a hidden reason. Thenodecan infect the system with bogus information, which interferes with actual commercial enterprise transactions and functioning of the structures. This need to be counter avoided to defend the honest nodes. The link between a Sybil node and a sincerenodeis called an attacking edge. As every part concerned resembles a trust established by a human, it is difficult for the adversary to be able to introduce an immoderate quantity of attack edges. The most effective recognized promising protection in opposition to Sybil assault is to apply social networks to carry out person admission manipulate and restrict the quantity of bogus identities admitted to a machine. The usage of social networks among two nodes represents real-global accepts as true the relationship between customers. also authentication-primarily based mechanisms are used to confirm the identities of the nodes using information about location, or shared encryption keys.

Most previous work on Sybil assault makes use of social networks to remove Sybil attack, and the findings are based totally on defending Sybil identities. In this project, using neighbour similarity trust is suggested in a group node to node e-commerce based totally on hobby relationships, to get rid of maliciousness the various nodes. Here, it is termed as Sybil Trust. In Sybil Trust, the group infrastructure which is based on interest has a neighbour similarity believe among each other, with which they may be capable of defending against Sybil attack. Sybil Trust offers a good relationship in transactions that occur in e-commerce as the nodes create a link node associates. This presents an vital street for nodes to advertise their products to different involved nodes and to understand new market destinations and contacts properly. In addition, the institution allows anode to sign up for node to node e-commerce community and makes identification greater difficult. Nodes make use of self-certifying identifiers which can be exchanged after they get into contact initially. These identifiers can be utilized as public keys to confirm digital signatures on the messages despatched through their neighbours. It is found that all the communications that take place between the nodes are digitally signed. In this sort of courting, I consider neighbours as our point of connection to deal with Sybil attack. In a group, there are malicious, Sybil and sincere nodes. They are authenticated through an admission manipulate mechanism to enrol in the group.

Greater honest nodes are admitted as compared to malicious nodes, in which the association which is based on trust is geared toward high quality effects. The understanding of the graph may stay in an individual party, or be shared throughout every one of the users. In this project, I use the dispensed admission manipulate which only just needs each node to be first of all aware of its immediate depended neighbours, then to search for honest acquaintances. The associates assist to find different nodes which have similar interest in different levels.

II. LITERATURE SURVEY

ह , "Footprint: Detecting Sybil Attacks in Urban Vehicular Networks",

AUTHORS: S. Chang, Y. Qi, H. Zhu, J. Zhao, and X. Shen

In city vehicular networks, the place privatizes, primarily the field privacy of anonymous automobiles is incredibly worried, anonymous verification of automobiles is significant. For this reason, an attacker who accomplishes in the formation of a few adversarial identifies can with no trouble launch a Sybil attack, gaining a disproportionately big impact. On this project, a Sybil attack detection mechanism called Footprint is proposed which utilizes the vehicle trajectories for identification by still retaining their subject privations. More above all, when an auto system approaches a road-side unit (RSU), it needs an active licensed message from the RSU as the appearance proof at this RSU. Field-hidden approved message generation scheme is designed mainly for two ambitions. Firstly, RSU signatures on messages are signer ambiguous in order that the RSU vicinity skills are hid from the resulted licensed message. Secondly, two licensed messages signed through the same RSU within the equal given period of time are identifiable in such a way that they are also equipped for identification. With the difficulty on the linking ability of two authorized messages, authorized messages used for lengthy-time period recognition are prohibited. The generation of a vicinity-hidden trajectory by the vehicles for vicinity-privacy-preserved identification becomes possible with this approach through the collection of licensed messages successively, in a sequential manner. By making use of social relationship amongst trajectories in step with the similarity definition of two trajectories, Footprint can admire and therefore push aside "communities" of Sybil trajectories. Rigorous protection evaluation and immense hint-driven simulations showthe efficacy of Footprint.

ह "Sybil Defender: Defend Against Sybil Attacks in Large Social Networks",

AUTHORS: W. Wei, X. Fengyuan, C. T. Chiu, and L. Qun.

Dispensed systems without relied-on identities are in particular at risk of Sybil assaults, in which an adversary creates a couple of bogus identities to compromise the running of the system. SybilDefender proposed here is a defence mechanism on Sybils that leverages the community topologies to defend in opposition to Sybil assaults in social networks. Primarily based on appearing a confined number of random walks in the social graphs, SybilDefender is green and scalable to huge social networks. Their experimentations on two 3,000,000 node real-international public topologies show that SybilDefender outdoes the country of the art through the use of more than 10 occurrences in both accurateness and walking time. SybilDefender can efficaciously perceive the Sybil nodes and locate the Sybil community around a Sybil node, even when the quantity of Sybil nodes brought by means of each attack aspect is near the theoretically detectable lower bound.

Except, they advise two processes to restricting the variety of assault edges in on-line social networks. The survey outcomes of our Facebook utility display that the idea made by means of previous paintings that every one of the relationships in social networks are trusted does no longer observe to on line social networks, and it is feasible to restrict the number of assault edges in on line social networks by means of rating score.

III. SYSTEM OVERVIEW

Here, focus is on the active attacks in node to node e-commerce. When a node is compromised, all the information will be extracted. Security and efficiency evaluation suggests that Sybil attack can also be minimized with the proposed neighbour similarity believe.

ADVANTAGES:-

- Safety and performance study shows that Sybil attack can be reduced.
- Proposed method identifies more malicious nodes when matched to existing methods
- Sybil Trust is efficient and scalable to group NODE TO NODE e-commerce network.

MODULES DESCRIPTION:

ह्रSYSTEM ARCHITECTURE

Neighbor Similarity Computational Model

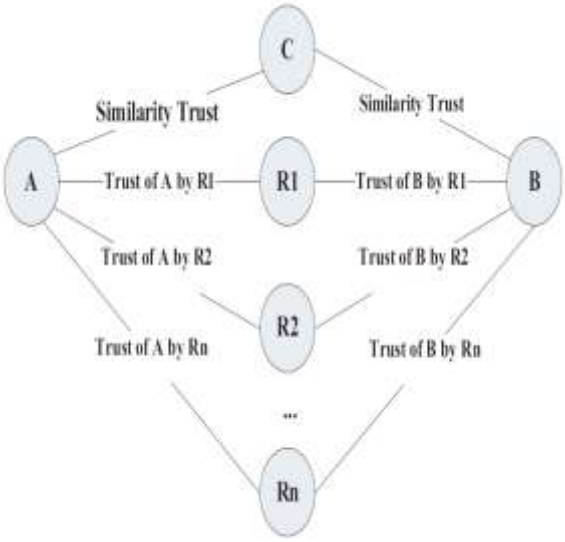


Fig. 1 The Neighbor Similarity Computational Model.

Detection of Sybil attack

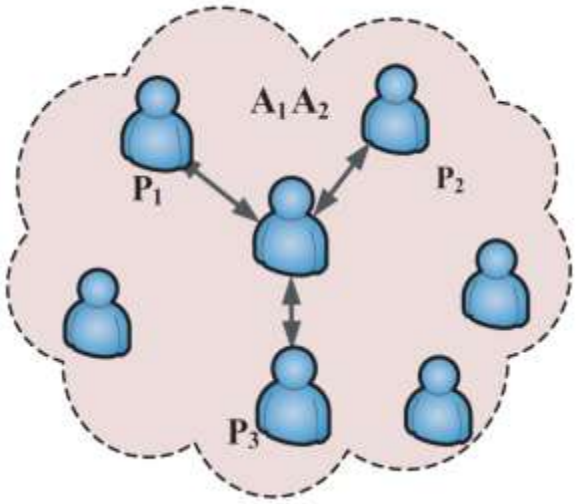


Fig.2: Detection of Sybil attack

The Recommendation Trust Relationship among Nodes

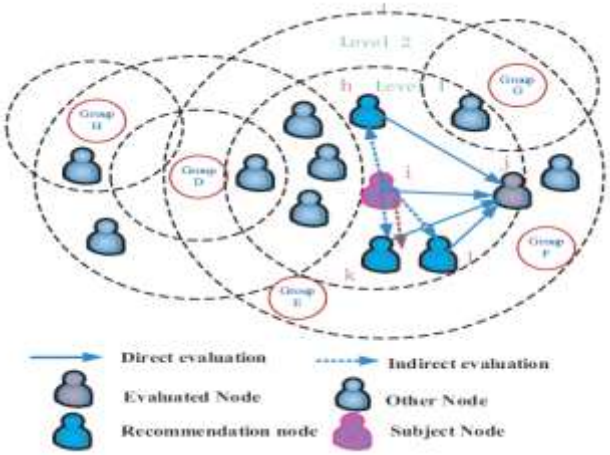


Fig. 3: The Recommendation Trust Relationship among Nodes.

ह्र MODULES

1.noderegistration
2. Find neighbour peer
3. Assign trust to neighbour
4. Sybil attacker
5. Sybil attack identification

Peer registration

Each one of the nodes registers with their location details. Each node in a NODE TO NODE network is given a unique identity.

- The connection between an honest node and a node which is Sybil is called an attack edge. Each of the edges involved looks similar to a human-established trust.
- So, it is difficult for an opponent to introduce a multiple number of attack edges.
- The use of social networks between two nodes represents real-world trust relationship between users.

Find neighbour peer Each node can identify its neighbours based on node location . Here it is assumed as if the location to be split into groups.

- For example, 100, 200 etc. are assigned as node locations .
- Peer that is between 0 and 100 comes as its neighbour nodes for the first group and node between 101 and 200 becomes the next group to cooperate.

Assign trust to neighbour

- Each node in a group can assign trust value to its neighbour node in a group. Trust value like 0 or 1, represents normal node or attack peer. The neighbourhood of anode v in a NODE TO NODE e-commerce is N(v)={z/(v,z)€E}.
- Each node v keeps a set of identifiers of its neighbours N(v), in which everyone is distinctive.

Sybil attacker

- Sybil attack is an attack where maliciousnodetries to present multiple dissimilar identities. This can be achieved by either generating authorized identities or by acting like other normal nodes.
- Certain nodes might present random attacks to restrict with NODE TO NODE e-commerce operations, or the usual functioning of the network.

Sybil attack identification

- If then ode trades with very few unsuccessful transactions, it can be decided that thenodeis a Sybil peer. Anodeu and a Sybilnodev can trade with each other whether one is Sybil or not.
- Being in a group, comparison can be done to determine the number of nodes which trade with peer.

IV. IMPLEMENTATION OF THE SYSTEM

Java Technology:

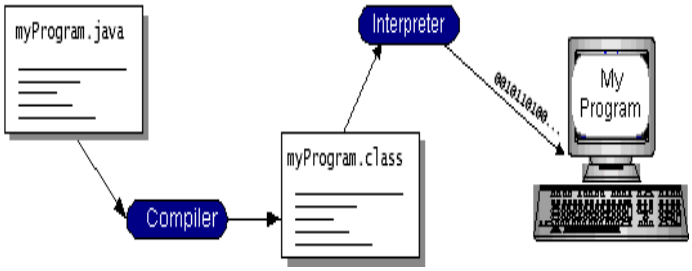
Java science is a programming language and a platform.

The Java Programming Language

The Java programming language is an excessive-measure language that may be characterized through the whole following buzzwords:

- Easy
- Constitution impartial
- Object oriented
- Transferable
- Dispersed
- High efficacy
- Understood
- At ease

With a lot of programming languages, one both accumulate or adapt software to be able to run it on one's computer. The Java programming accent is able in that a appliance is anniversary aggregate and interpreted. With the compiler, aboriginal one construe a account into an average accent referred to as Java byte codes —the platform-impartial codes interpreted through the analyst on the Java platform. The analyst parses and runs every Java byte cipher adviser on the laptop. Compilation occurs calmly as bound as; estimation happens at any time if the software is agitated out. The afterward actuate illustrates how this works.



That one would artlessly anticipate of Java byte codes because the computer cipher recommendations for the Java basic accretion accessory (Java VM). Every Java interpreter, whether or not it's a development accessory or a web based browser that may run applets, is an accomplishing of the Java VM. Java byte codes aid accomplish "write as immediately as, run anyplace" feasible. One would be able to backpack calm one's appliance into byte codes on any place that has a Java compiler.

SAMPLE CODE

1. admin_all_sel.jsp

```
<%@page
import="com.oreilly.servlet.*,java.sql.*,java.lang.*,databaseco
nnection.*,java.text.SimpleDateFormat,java.util.*,java.io.*,jav
ax.servlet.*, javax.servlet.http.*" %>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0
Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-
transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en"
lang="en">
<head>
<meta http-equiv="content-type" content="text/html;
charset=iso-8859-1" />
<title>Sybil Attack Detection</title>
<link href="style.css" rel="stylesheet" media="all"
type="text/css" />
</head>
<body>
<div id="wrapper">
  <div id="container">
    <div id="header">
      <div id="logo"><br>
        <br>
        <br>
        &n
bsp;  <strong><font color="#FFFFFF" size="+2"
face="Georgia, Times New Roman, Times, serif">
      Neighbor Comparable Decision Based Expression
        &n
bsp;        
       On Sybil
Attack in NODE TO NODE E-Commerce<br>
```

International Journal of Research Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

```
      </font></strong></div>
   </div>
   <!-- /header -->
   <div id="navbar">
    <ul>
      <li><a  href="admin_home.jsp">Home</a></li>
      <li><a  href="admin_seller.jsp"
class="active">Seller</a></li>
      <li><a  href="admin_all_users.jsp">Users</a></li>
      <li><a  href="index.html">Logout</a></li>
      <!-- <li><a  href="#">Admin</a></li>
      <li><a  href="#">Link</a></li>
      <li><a  href="#">Link</a></li>
      <li><a  href="#">Link</a></li>-->
    </ul>
   </div>
   <!-- /navbar -->
   <div id="main">
    <div id="intro">
      <!-- <div id="sellerpic">
      </div>-->
      <!-- /jakepic -->
      <div id="text"> </div>
      <!-- /text -->
      <table height="350"  align="center" width="700">
       <tr bgcolor="#CC3300">
```

2. admin_all_users.jsp

```
<%@page
import="com.oreilly.servlet.*,java.sql.*,java.lang.*,databaseco
nnection.*,java.text.SimpleDateFormat,java.util.*,java.io.*,jav
ax.servlet.*, javax.servlet.http.*" %>
<!DOCTYPE  html PUBLIC  "-//W3C//DTD XHTML  1.0
Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-
transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml"  xml:lang="en"
lang="en">
<head>
<meta http-equiv="content-type" content="text/html;
charset=iso-8859-1"  />
<title>Sybil  Attack Detection</title>
<link  href="style.css" rel="stylesheet" media="all"
type="text/css" />
</head>
<body>
<div id="wrapper">
  <div id="container">
    <div id="header">
      <div id="logo"><br>
        <br>
        <br>
        &n
bsp;  <strong><font color="#FFFFFF" size="+2"
face="Georgia,  Times New Roman,  Times,  serif">
       Neighbor Comparable  Decision Based Expression
        &n
bsp;        
       On Sybil
Attack in NODE  TO NODE  E-Commerce<br>
      </font></strong></div>
</div>
```

V. SYSTEM DESIGN

The unified modelling language (UML) is a recognized language for outlining, visualizing, building and documenting the artefacts of program techniques, additionally to the commercial corporation modelling and other non-software software methods. The UML represents a group of excessive-first-rate engineering practices which have validated triumphant inside the modelling of enormous and difficult methods. The UML is a fully central a part of establishing objects oriented software program and the software improvement process. The UML makes use of within the most important graphical notations to specific the design of program program duties. The use of the UML helps challenge agencies communicate, discover ability designs, and validate the architectural design of the application program.

Class diagram : Class diagrams are used in each the analysis and the design phases. Throughout the analysis segment, an extraordinarily excessive-degree conceptual design is created. Presently, a category diagram possibly created with simplest the category names shown or potentially some pseudo code-like phrases is also introduced to explain the obligations of the class. The category diagram created in the course of the analysis segment is used to explain the courses and relationships within the difficulty area, but it surely does not advise how the approach is applied. By using the tip of the design segment, class diagrams that describe how the method to be carried out should be developed. The class diagram created after the design segment has certain implementation expertise, together with the category names, the approaches and attributes of the courses, and the relationships among classes.

The class diagram describes the varieties of objects in a process and the various forms of static relationships that exist amongst them. In UML, a category is represented by a rectangle with one or more horizontal cubicles. The higher compartment holds the identity of the category. The title of the category is the one required subject in a class diagram. By convention, the name of the class starts with a capital letter. The center compartment of the class rectangle holds the record of the class attributes/information participants, and the lower section holds the list of methods/operations.

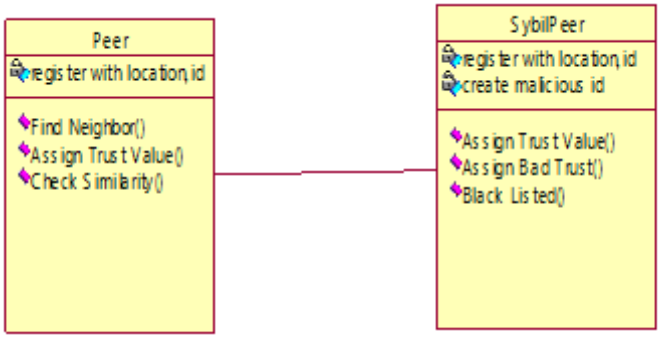


Fig. Class Diagram

Use case diagram : Use case diagrams are used throughout necessities elicitation and evaluation as a graphical method of representing the realistic requisites of the process. Use instances are developed for the duration of specifications elicitation and are extra subtle and corrected as they're reviewed (via stakeholders) during evaluation. Use cases are additionally very helpful for writing acceptance experiment instances.

A use case mainly represents a principal piece of performance that's complete from establishing to finish. In UML, a use case is represented as an ellipse. A use case diagram is a visible representation of the relationships between actors and use circumstances together that files the approach's meant habits. Arrows and contours are draw between actors and use circumstances and between use cases to exhibit their relationships. The default relationship between an actor and a use case is the «communicates» relationship, denoted by way of a line.

There are two different varieties of relationships between use instances that you might valuable. These are «incorporate» and «prolong». The «comprise» relationship is used when a piece of conduct is identical across more than one use case, and one does now not want to keep copying the description of that behavior.

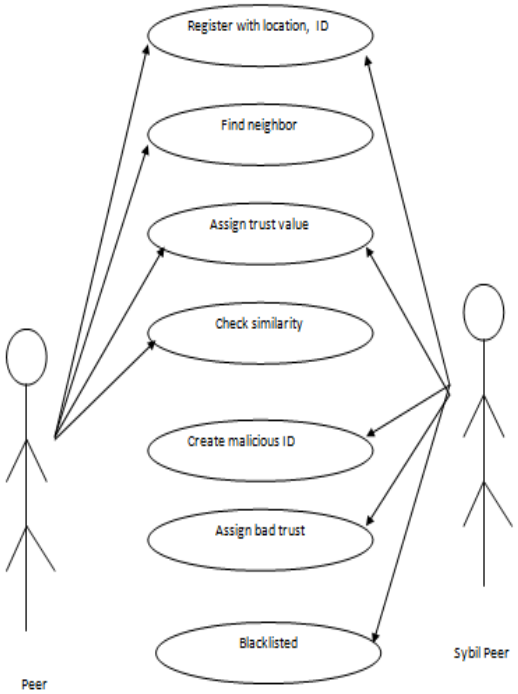


Fig. Use Case Diagram

SYSTEM TESTING: The purpose of checking out is to realize errors. Testing is the method of seeking to realize every possible fault or weakness in a work product. It supplies a solution to investigate the functionality of accessories, sub-assemblies, assemblies and/or a completed product it's the method of exercising program with the intent of guaranteeing that the software process meets its requirements and consumer expectations and does no longer fail in an unacceptable manner. There are various varieties of test. Each and every scan type addresses a specified checking out requirement.

With the intention to make certain that the process does now not have blunders, the certain phases of trying out methods which are utilized at differing phases of program progress are:

Unit Testing: Unit trying out involves the design of experiment cases that validate that the inner application common sense is functioning thoroughly, and that application inputs produce legitimate outputs. All selection branches and inside code waft should be validated. It's the checking out of individual software units of the applying .It is achieved after the completion of a character unit earlier than integration. This can be a structural trying out, that relies on talents of its building and is invasive.

Unit assessments participate in basic tests at element degree and scan a specific business approach, utility, and/or procedure configuration. Unit checks make sure that every designated route of a industry systemperforms properly to the documented requirements and contains clearly outlined inputs and expected results.

Experiment method and procedure

Subject testing shall be performed manually and useful tests can be written in detail.

Experiment ambitions

- All area entries have got to work correctly.
- Pages have to be activated from the identified hyperlink.
- The entry reveal, messages and responses have to now not be delayed.

Features to be verified :

- Verify that the entries are of the right structure
- No duplicate entries must be allowed
- All hyperlinks will have to take the consumer to the right page.

VI. VI. CONCLUSION

In this project, I suggest SybilTrust, a safeguard in the direction of Sybil attack in NODE TO NODE e-commerce. In evaluation with different approaches, proposed method is headquartered on neighborhood similarity feel in a bunch NODE TO NODE e-commerce local. This method exploits the connection between associates in a regional environment. Our outcome on actual-world NODE TO NODE e-commerce confirmed quick-mixing property, thus validated the predominant assumption at the back of Sybil shield's system. I additionally describe defense forms just like key validation, distribution, and function verification. This tactics may also be achieved at in concurrently with neighbour similarity suppose which offers higher defence mechanism. For the long run work, I intend to implement Sybil think within the context of friends which exist in tons of organizations. Neighbour similarity believes helps to weed out the Sybil friends and isolate maliciousness to septic Sybilnodeorganizations

alternatively than allow attack in sincere firms with all sincere associates.

REFERENCES

[1] J. Douceur, "The Sybil Attack, " Proc. of IPTPS, 2002, pp. 251- 260.
[2] A. Mohaisen, N. Hopper, and Y. Kim, "Keep your Friends Close: Incorporating Trust into Social Network-based Sybil Defenses, " Proc. of IEEE INFOCOM, 2011, pp. 1-9.
[3] K.Walsh and E. G. Sirer, "Experience with an Object Reputation System fornodetonodeFilesharing, " Proc. of USENIX NSDI, 2006, pp. 1-14.
[4] S. Chang, Y. Qi, H. Zhu, J. Zhao, and X. Shen, "Footprint: Detecting Sybil Attacks in Urban Vehicular Networks, " IEEE Transactions on Parallel and Distributed Systems, Vol. 23, No. 6, June 2012, doi:10.1109/TPDS.2011.263, pp. 1103-1114.
[5] B. Yu, C.Z. Xu, and B. Xiao, "Detecting Sybil attacks in VANETs," Journal of Parallel and Distributed Computing (JPDC - Elsevier), Vol. 73, No. 3, June 2013, Pp. 746-756.
[6] T. Nguyen, L. Jinyang, S. Lakshminarayanan, and S. M. Chow, "Optimal Sybil-ResilientnodeAdmission Control," Proc. of IEEE INFOCOM, 2011, pp. 3218-3226.
[7] K. Wang, M. Wu, and S. Shen, "Secure Trust-Based Cooperative Communications in Wireless Multi-hop Networks," Communications and Networking, Book chapter 18, Book edited by: Jun Peng, September 2010, ISBN 978-953-307- 114-5, pp. 360-378.
[8] H. Yu, P. Gibbons, M. Kaminsky, and F. Xiao, "SybilLimit: A Near-Optimal Social Network Defense against Sybil Attack," IEEE/ACM Transactions on Networking, Vol. 18, No. 3, June 2010, pp. 3-17.
[9] H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman, "Sybil- Guard: Defending against Sybil Attack via Social Networks," IEEE/ACM Transactions on Networking, Vol. 16, No. 3, June 2008, pp. 576-589.
[10] A. Tversky, "Features of Similarity, " Psychological Review, Vol. 84, No. 2, 1977, pp. 327-352.
[11] F. Musau, G. Wang, and M. B. Abdullahi, "Group Formation with Neighbor Similarity Trust in NODE TO NODE E-Commerce," Proc. Of Joint Conference of IEEE TrustCom/IEEE ICESS/FCST, November 2011, pp. 835-840.
[12] G. Danezis and P. Mittal, "SybilInfer: Detecting Sybil Attack Nodes using Social Networks," Proc. of NDSS, San Diego, CA, February 2009, pp.1-15.
[13] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis and Defenses," Proc. of IPSN, ACM, April 2004, pp.1-10.
[14] W. Wei, X. Fengyuan, C. T. Chiu, and L. Qun, "SybilDefender: Defend Against Sybil Attacks in Large Social Networks," Proc. of IEEE INFOCOM, 2012, pp.1951-1959.
[15] L. Xu, S. Chainan, H. Takizawa, and H. Kobayashi, "Resisting Sybil Attack by Social Network and Network Clustering," International Symposium on Applications and the Internet IEEE/IPSJ SAINT, 2010, pp.15 - 21
[16] N. Tran, B. Min, J. Li, and L. Subramanian, "Sybil-Resilient Online Content Voting," Proc. of the 6th USENIX, Symposium on Networked Systems Design and Implement, USENIX Association, 2009, pp. 15-28.

Biography:

Mr.K.Ramakrishna,(Ph.D.)Research Scholar in Sri Satya Sai University of Technology and Medical Sciences, Sehore (M.P) India . Working as a Assistant Professor in computer science and engineering department in KG Reddy college of engineering and technology, Hyderabad, India . He received the master of technology degree in VNR Vignana Jyothi Institute of Engineering and Technology- Jawaharlal Nehru Technological University Hyderabad, India. He received the bachelor of technology degree in The Vazir Sultan College of Engineering And technology, kakatiya university , Warangal, India.His Research Interests Include Soft computing, Soft computing, Software testing, mobile ad-hoc networks,Data Mining, Information Security, Software Testing, Software Engineering, mobile communication and cloud computing.

Mr. Y. Rokesh Kumar, (Ph.D.) Research Scholar in Sri Satya Sai University of Technology and Medical Sciences, Sehore (M.P.) India. He Has 5+ Years Teaching Experience;His Research Interests Include cloud computing, Data Mining, Information Security, Software Testing, mobile communication and mobile ad-hoc networks.

Mr. U.Rakesh , presently working as an assistant professor in computer science engineering and technology department, SV Engineering college for women's, India. He received the master of technology degree in VNR Vignana Jyothi Institute of Engineering and Technology-Jawaharlal Nehru Technological University Hyderabad, India. He received the bachelor of technology degree in Jawaharlal Nehru Technological University Hyderabad, India. He Has 6+ Years Teaching Experience; His Research Interests Include mobile ad-hoc networks, Data Mining, Information Security, Software Testing, mobile communication and cloud computing.