Journal of Theoretical and Applied Information Technology
10th February 2014. Vol. 60 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AN EFFICIENT ALGORITHM FOR FAULT CLASSIFICATION AND IDENTIFICATION IN ONLINE TRANSACTION MANAGEMENT

[1]JAVID ALI, [2]ANANDHAMALA

[1]Research scholar, Sathyabama University, Dept of Computer Science and Engineering, St.Joseph's College of Engineering, Jeppiaar nagar, OMR, Chennai, Tamilnadu, India

[2] Professor, Department of Computer science and Engineering, St.Joseph's College of Engineering, Jeppiaar nagar, OMR, Chennai, Tamilnadu, India
E-mail: [1]javidinaug77@gmail.com , [2]gs.anandhamala@gmail.com

ABSTRACT

Nowadays the customer demand for accessing a web based application has grown enormously as everything is available in the Internet. Sensitive application providers retain their resources in safe from unauthorized access by using single signon technique. In this technique if a user gives an irrelevant information in a particular session, he may be asked to continue the session by using sign on technique once again irrespective of whether the user is a sensitive user. This paper proposes a new strategy which classifies the sensitive user and allows him to continue the session even if the user does a mistake (fault) that could be tolerated to some level. The proposed method focuses on the fault identification and classification in order to keep the sensitive user for assigning some tolerance level for accessing the web application. The users are classified based on the access level by setting the tolerance level for the type of fault identified. An efficient algorithm is proposed for handling the fault tolerance in the web application more efficiently. In future the fault tolerance can be extended by AI based technique with multi-level security for improving the performance over online transaction.

Keywords: *Fault Tolerance, Web Application, Fault Tolerant Techniques, Classification, Access Policy*

1. INTRODUCTION

The users need a web based application for performing the sensitive online transaction. During this session he/she may commit a mistake while selecting the sensitive services which leads to service unavailable i.e., session timeout. These faults need to be handled properly in order to satisfy the most valuable customer. The users are classified into basic, normal and valuable user and the threshold value is set to ZERO, MIN and MAX respectively. Once the fault is identified, it will be classified based on the user access level. Sensitive faults are handled carefully where as other faults that are tolerable are handled based on user access level.

The sensitive information is managed in heterogeneous environment by deploying the collaborative information systems. The Community Anomaly Detection System (CADS) introduces an unsupervised framework for detecting the threats based on the access log [1]. A distributed fault tolerant control scheme is used to perform fault functions and to interconnect the unknown systems. The Lyapunov analysis has been introduced to track the errors and also stops the subsystems at certain time instant [2]. The investigation is carried out using the data aggregation (DA) survivability for Partially Connected Networks (PCN) in synchronous system in the presence of hybrid fault modes to identify the network faults by setting a predefined threshold [3]. The web site graph structure has been proposed to identify the flooding attacks on the website by using a new Web Referral Architecture for Privileged Service ("WRAPS"). It allows the clients to get the privilege URL from the trusted websites or from the targeted websites. One of the important security properties of WRAPS is to protect the small websites form DoS attacks [4] [15].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The pervasive computing requires identifying the best service provider by selecting the service which is based on user requirements. The service disruptions occur due to various faults during the service execution. The important challenge in the pervasive environment is to execute the service without the service disruptions. This goal is achieved by using a novel Fault tolerant Service Selection Framework (FTSSF) which will give efficient fault tolerance technique [5]. The important issue of network management and traffic analysis over VoIP can be overcome by using the new traffic identification scheme to identify the VoIP traffic at the transport layer of the Internet. The flexibility and accuracy can also be improved at the maximum level [6] [13]. The efficient usage and control of the bandwidth is needed by the ISP in order to satisfy the customer needs. The file-aware P2P traffic classification method is proposed to identify the files and related flows [7]. The risk factors can be divided into two types namely network risk and service risk. The service risk depends on the services and software running over the host or system whereas the network risk depends on the hardware over the entire network. The service and policy perspective is used to handle the security and management objectives. The risk framework is called Risk based prOactive security COnfiguration maNAger (ROCONA) that uses the security configuration management of services and policies in a system [8]. The enterprise information infrastructures are built on hardware elements in network architecture, installation of software and information assets. The enterprise accesses these assets using the policies. The threats are detected in the enterprise level and the disruptions are overcome in the information processing systems [9] [14].

A botnet is a network of computer robots (bots) which is used to collect information from the Internet for performing tasks such as helping the search engines. All search servers use this robot networks to collect and update the information to or from the Internet. The P2P botnets imitate the P2P software which has the categories such as avoiding the single-point failure, misuse of detection techniques and anomaly detection [10]. The Information Technology over commercial purpose needs the effective technique for solving the dispute. The AI based online dispute resolution (ODR) platforms have been introduced to confirm a new virtual environment through an efficient tool for resolving the dispute among the information that is available among the parties [11]. The main features of intelligent interactive environment (IIE) are intelligence, interactivity and location. These environments are implemented in variety of platforms and also in service-oriented systems. The tools have been developed for monitoring and implementing the real time, multimodal and multimedia activities [12].

The traffic analysis and classification are related to the fault classification and identification in the online access over web transaction. There are various techniques used for effective access of network, traffic and other resources which are suitable for accessing the web based application. None of these methods focus on the fault committed by the web user and retain the customer in the active state in order to improve the performance of the web application. The survey focuses on fault management and classification with user access policies rather than session sign out mechanism. A new technique has been proposed in this paper for identifying and classifying the faults over online transaction system. The rest of the paper organized as follows,

This paper begins with the review of fault tolerance techniques in the field of online transaction processing. The proposed system is explained in section 2. The algorithm related to proposed system is described in section 3. Implementation and results are explained in section 4. Conclusion and future work is contained in section 5.

2. FAULT MANAGEMENT AND CLASSIFICATION SYSTEM

Initially the web user requests the resources and uses the web application for sensitive online transactions. The users are classified into various category namely basic user, normal user and valuable user. The basic user is a user who can

Journal of Theoretical and Applied Information Technology
10th February 2014. Vol. 60 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

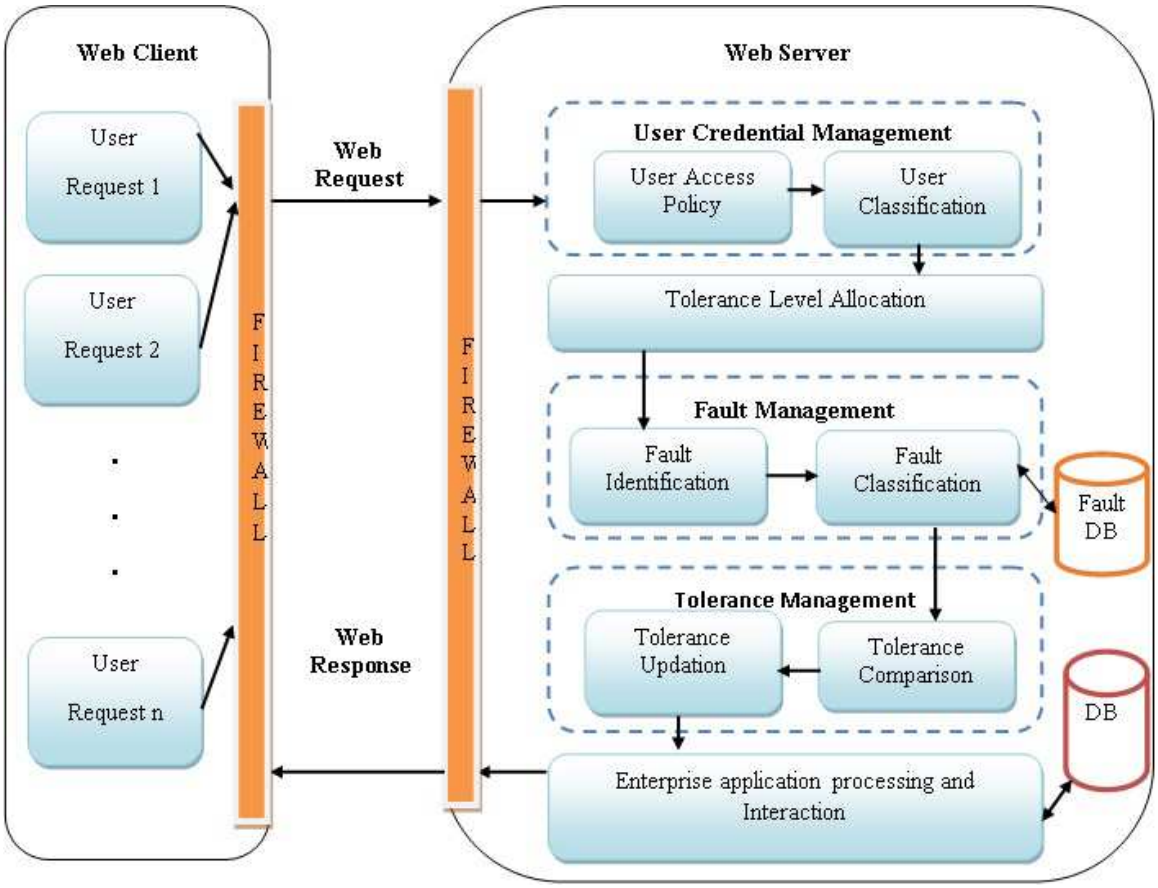


Figure 1. Proposed System For Fault Management

access the application only for the reference of web page i.e., one who does not indulge in the online transactions. The normal user can refer web information and also participate in the online transactions. The valuable user always performs the sensitive online transactions. The access policies are assigned for each users based on the level of access. The tolerance limit is set for each user based on the access policies. The tolerance level for basic user, normal user and valuable user is ZERO, MIN and MAX respectively. The fault is identified and then the faults are classified based on the fault level namely tolerable access or sensitive access. If the fault status is tolerable then the users are treated as valuable user. If the fault status is sensitive then the users are treated as normal user. For each fault committed by the normal and valuable user, the tolerance value is decreased to some level. Once the tolerance value reaches zero, the current session will be closed for accessing the web application. The threshold status is used to give the status of the sensitivity which is measured during the web application interaction. The main objective of this proposed method is to retain the valuable customer for efficient access during online transaction. Figure 1 shows the fault management and classification system of the proposed method.

3. ALGORITHM

Fault_Classification_Identification ()
Begin
Let User Request is UR i.e., the users interaction with web application;
Let Signout Mode is SIM i.e., mode of access;
Let Fault identification and Fault classification is FI and FC respectively;
Let Threshold value is THRES_VALUE;
Let ISF and SF are Insensitive Fault and Sensitive Fault respectively;
Let THRES_MIN and THRES_MAX are minimum and maximum threshold respectively;
for each $ur_i \varepsilon$ UR do // User Classification
for each $sim_i \varepsilon$ SIM do
Label L1: if (sim_i = = Signout_ONCE) then

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

```
                User_Level= Basic_User;
          else if (sim_i = = Signout_NULL) then
                User_Level= Valuable_User;
          else
                User_Level= Normal_User;
        end;
      end;
end;
Label L3:for each tr_i ε THRES_VALUE
                                        do
 //User Classification
    if ( User_Level = = Basic_User) then
         tr_i value is set to 0;
    else if (User_Level = = Valuable_User)
                                        then
         tr_i value is set to maximum;
    else
         tr_i value is set to minimum;
    end;
end;
for each fi_i ε FI do // Fault Identification
if ( fi_i = = Authentication_Level) then
        Fault_Type ←—— Fault_Type
                              U { ISF};
          else if(fi_i = = View_Level)
        Fault_Type ←—— Fault_Type
                              U { ISF};
          else if(fi_i = = Interaction_Level)
        Fault_Type ←—— Fault_Type
                              U { SF};
          else
        Fault_Type ←—— Fault_Type
                              U { SF};
        end;
end;
Label L2: for each ft_i ε File_Type do
// fault comparison
  if (ft_i = =ISF) then
goto L1;
 else if(ft_i = =SF and User_Level
                 = = Normal_User) then
  THRES_MIN—
else
THRES_MAX--;
end;
end;
 if (THRES_MIN !=0) then
        Alert the user for the fault;
        goto L2;
else
    get away from the web application access
                      i.e sign out;
end;
if (THRES_MAX!=0) then
    alert the user for the fault and ignore
                                  the fault;
keep the login session for further web application
                                  access;
       goto L3;
  end
end: Fault_Classification_Identification
```

4. IMPLEMENTATION

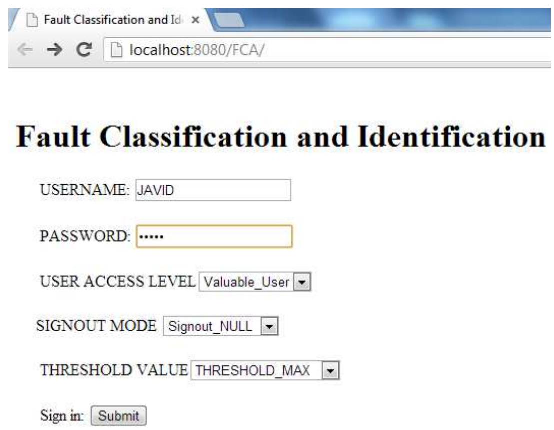
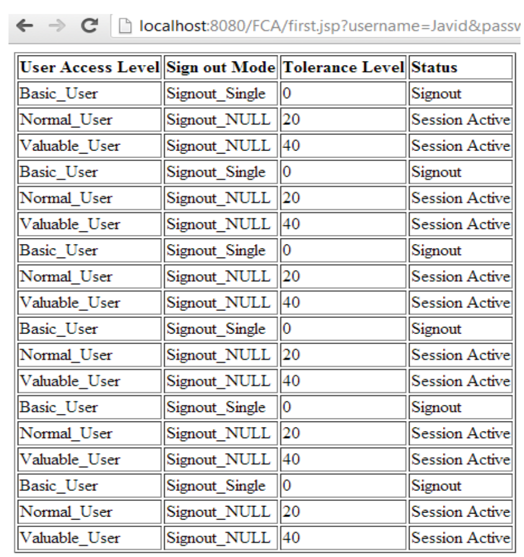


Figure 2.Setting up of User Access Policy-

Fig 2 shows the set up of User Access Policy on fault classification and identification. The fault classification and identification techniques are implemented by using Java Server Pages, Servlets with Glassfish server as a web server and MySql database. The users are assigned a user access level with sign-out mode and threshold value. These parameters are used for interacting the online transaction application management in order to achieve the reliability.


localhost:8080/FCA/first.jsp?username=Javid&passv

User Access Level	Sign out Mode	Tolerance Level	Status
Basic_User	Signout_Single	0	Signout
Normal_User	Signout_NULL	20	Session Active
Valuable_User	Signout_NULL	40	Session Active
Basic_User	Signout_Single	0	Signout
Normal_User	Signout_NULL	20	Session Active
Valuable_User	Signout_NULL	40	Session Active
Basic_User	Signout_Single	0	Signout
Normal_User	Signout_NULL	20	Session Active
Valuable_User	Signout_NULL	40	Session Active
Basic_User	Signout_Single	0	Signout
Normal_User	Signout_NULL	20	Session Active
Valuable_User	Signout_NULL	40	Session Active
Basic_User	Signout_Single	0	Signout
Normal_User	Signout_NULL	20	Session Active
Valuable_User	Signout_NULL	40	Session Active
Basic_User	Signout_Single	0	Signout
Normal_User	Signout_NULL	20	Session Active
Valuable_User	Signout_NULL	40	Session Active

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Figure 3. User Classification and Tolerance level setup

User Access Level	Tolerance Level	Number of Faults	Fault Status
Basic_User	0	1	Signout
Normal_User	20	15	Tolerable
Valuable_User	40	18	Tolerable
Basic_User	0	1	Signout
Normal_User	20	10	Tolerable
Valuable_User	40	25	Tolerable
Basic_User	0	1	Signout
Normal_User	20	11	Tolerable
Valuable_User	40	30	Tolerable
Basic_User	0	1	Signout
Normal_User	20	16	Tolerable
Valuable_User	40	35	Tolerable
Basic_User	0	1	Signout
Normal_User	20	21	Signout
Valuable_User	40	41	Signout

Figure 4. Fault Classification and Identification

Figure 3 shows the user access level which is used to classify the user according to the capability of the interaction. Signout mode is a session timeout based on user access level with tolerance level. The tolerance level is assigned for all the users and also to verify whether the status is active or not. For example, if the user access level is normal and the sign out mode is set to NULL then the fault status is set to be tolerable. The tolerance level is 20 and the session is in an active state which leads the user to continue the current session to access the application.

Figure 4 shows the fault status of the proposed method. Suppose the user commits a fault during online transaction the tolerance level will be changed and the fault status will be updated. For example, if the valuable user has done a fault, the tolerance level is reduced. This does not lead to the user to session timeout instead it remains in the current session. If the tolerance level reaches ZERO for normal and valuable user then the session gets closed whereas the current session will be closed in single sign on if the user level access is basic. This technique is used to improve the reliability and fault tolerance over the online web application.

Figure 5 shows the fault mangement with classification of various faults. If an user commits a mistake in many ways which are not relevent to the current interaction, then the transaction will lead to session timeout. The source of the fault is related to the current web page and browser which exists in the client end. The users are identified and the policies are assinged based on the level of access. The faults are committed by the user either by selecting the options like hyperlink, browser level buttons, form level controls and captcha etc.,

The fault code is assigned for each fault along with the description. The objective of maintaining the fault code and description is to identify and correlate the faults whenever the report is generated by the administrator. The fault code is a combination of two characters followed by any number. The number is described as a type of fault that is commited from the same source i.e., for example the hyperlink can be activated in various ways like selecting the options from advertisement, social networking and so on. The fault code HL01 is for advertisement hyperlink selection,HL02 for social networking hyperlink selection and so on. Fault type gives the actual source of fault i.e HL means HyperLink, BF means Browser Forward button etc., All Faults are maintained at the database to keep the fault tolerance level stable and maintain the session status. The session status are updated for each fault committed by the user and keep the session in proper state.

If a basic user commits a fault, the session goes into an inactive state where as a normal user can continue with restricted access according to the tolerance level for the type of fault committed. A valuable user, on the other hand gets free access with his tolerance level getting reduced
according to the type of fault committed. Such type of fault classification and granting of access permissions, improve the performance of web application to a considerable level.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Fault Type	Fault Code	Fault Description	User Access Level	Fault Status
HL	HL01	Hyperlink	Basic_User	Session Inactive
BF	BF01	Button Forward	Valuable_User	Session Active
BB	BB01	Button Backward	Basic_User	Session Inactive
CB	CB01	Checkbox Selection	Normal_User	Session with Access Limit
HL	HL03	Hyperlink	Normal_User	Session with Access Limit
HL	HL02	Hyperlink	Valuable_User	Session Active
LB	LB01	List Selection	Basic_User	Session Inactive
IU	IU01	Input Username	Normal_User	Session with Access Limit
IU	IU01	Input Username	Basic_User	Session Inactive
IU	IU01	Input Username	Valuable_User	Session Active
IP	IP01	Input Password	Basic_User	Session Inactive
IP	IP01	Input Password	Valuable_User	Session Active
IC	IC01	Captcha Selection	Basic_User	Session Inactive
IC	IC01	Captcha Selection	Valuable_User	Session Active
IC	IC01	Captcha Selection	Normal_User	Session with Access Limit

Figure 5. Fault Management with user access policies

5. CONCLUSION AND FUTURE WORK

Every customer demands the web interaction for accessing any resources on the Internet as a web application. The applications are classified into various categories in order to satisfy the customer. The customers (users) interact with the web application by using their own credentials. The proposed technique improves the fault tolerance level of the user based on their access level. The users are classified into basic user, normal user and valuable user. The sign-out mode and tolerance level is needed to be applied over the users who are accessing the web application in an efficient manner. The fault of the valuable user could be tolerated up to some extent whereas the basic user immediately gets a session time out. The fault is classified and its status is verified. The normal and valuable user may remain in the same session until the tolerance level reaches ZERO. Each fault reduces the tolerance level to some extent, so these status are maintained for improving the performance of the sensitive web based application. In future this technique will be extended to tolerate the fault with multiple levels in the online transaction.

REFRENCES:

[1]. You Chen, Steve Nyemba, and Bradley Malin, "Detecting Anomalous Insiders in Collaborative Information Systems",*IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING*, VOL. 9, NO. 3, MAY/JUNE 2012, Page 332-344.

[2]. Panagiotis Panagi and Marios M. Polycarpou, Fellow, IEEE,"A Coordinated Communication Scheme for Distributed Fault Tolerant Control",*IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS*, VOL. 9, NO. 1, FEBRUARY 2013,page 386-393

[3]. Satish Srinivasan, Azad Azadmanesh "Survivable Data Aggregation in Multi-Agent Network Systems with Hybrid Faults ",*IEEE TRANSACTIONS ON COMPUTERS*,Digital Object Indentifier 10.1109/TC.2012.122 0018-9340/12/$31.00 © 2012,page 1-26

[4]. XiaoFeng Wang, Member, IEEE, and Michael K. Reiter, Senior Member, IEEE,"Using Web-Referral Architectures to Mitigate Denial-of-Service Threats",*IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING*, VOL. 7, NO. 2, APRIL-JUNE 2010,page 203-216.

[5]. Salaja Silas,Kirubakaran Ezra,Elijah Blessing Rajsingh,"A novel fault tolerant service selection framework for pervasive computing",Silas et al. *Human-centric Computing and Information Sciences* 2012,page 1-14

[6].Bing Li,Maode Ma,Zhigang Jin,"A VoIP Traffic Identification Scheme Based on Host and Flow Behavior Analysis", *Jouranl Network System Management (2011)* 19:111–129,DOI 10.1007/s10922-010-9184-7, Springer Science+Business Media, LLC 2010,page 1-19

[7].Tian Song , Zhou Zhou,"File-aware P2P traffic classification: An aid to network management', *Peer-to-Peer Netw. Appl.* DOI 10.1007/s12083-012-0172-4.page 1-15

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[8].Mohammad Salim Ahmed, Ehab Al-Shaer,Mohamed Taibah, Latifur Khan,"Objective Risk Evaluation for Automated Security Management",*J Netw Syst Manage (2011)* 19:343–366, DOI 10.1007/s10922-010-9177-6.page 343-366.

[9].Anirban Sengupta ,Chandan Mazumdar ,Aditya Bagchi,"A Formal Methodology for Detecting Managerial Vulnerabilities and Threats in an Enterprise Information System",*J Netw Syst Manage (2011)* 19:319–342DOI 10.1007/s10922-010-9180-y,page 319-342.

[10].Shu-Chiung Lin,Patrick S. Chen,Chia-Ching Chang,"A novel method of mining network flow to detect P2P botnets",*Peer-to-Peer Netw. Appl*.DOI 10.1007/s12083-012-0195-x,page 1-10.

[11]. Davide Carneiro,Paulo Novais,Francisco Andrade,John Zeleznikow,José Neves,"Using Case-Based Reasoning and Principled Negotiation to provide decision support for dispute resolution",*Knowl Inf Syst* DOI 10.1007/s10115-012-0563-0,page 1-38.

[12].Flavio Soares Correa da Silva,"Knowledge-based interaction protocols for intelligent interactive environments",*Knowl Inf Syst* (2013) 34:219–242 DOI 10.1007/s10115-011-0464-7,page 220-224.

[13].Roberto Perdisci, Igino Corona, and Giorgio Giacinto,"Early Detection of Malicious Flux Networks via Large-Scale Passive DNS Traffic Analysis",*IEEE TRANSACTIONS ON DEPEDABLE AND SECURE COMPUTING*,Digital Object Indentifier 10.1109/TDSC.2012.35 1545-5971/12/$31.00 © 2012,page 1-14

[14]. Dianxiang Xu, Senior Member, IEEE, Manghui Tu, Michael Sanford, Lijo Thomas,Daniel Woodraska, and Weifeng Xu, Senior Member, IEEE, "Automated Security Test Generation with Formal Threat Model",*IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING*, VOL. 9, NO. 4, JULY/AUGUST 2012,page 526-540

[15]. Sanjeev Khanna, Santosh S. Venkatesh, Member, *IEEE*, Omid Fatemieh, Fariba Khan, and Carl A. Gunter, Senior Member, IEEE, Member, ACM,"Adaptive Selective Verification: An Efficient Adaptive Countermeasure to Thwart DoS Attacks",*IEEE/ACM TRANSACTIONS ON NETWORKING*, VOL. 20, NO. 3, JUNE 2012,page 715-728.

[16]. Jeff Barr, Attila Narin, and Jinesh Varia,"Building Fault-Tolerant Applications on AWS",*Amazon Web Services – Building Fault-Tolerant Applications on AWS*,october 2011,page 1-15

[17]. Lingxia Liu, Yuming Meng, Bin Zhou, Quanyuan Wu,"A Fault-Tolerant Web Services Architecture",*Advanced Web and Network Technologies, and Applications Lecture Notes in Computer Science* Volume 3842, 2006, pp 664-671