Protection In Cluster Distributed System Using TCP Protocol

Ranjane Suryakant, Patil Anup, Saravade Sunil, Bhalekar Abhijit
S.B. Patil Collage of Engineering, Indapur, Pune, Maharashtra, India.

***Abstract*—Self-protection refers to the ability for a system to detect illegal behaviors. These papers provides novel design, demonstrate the implementation and evaluates a self-protected system that targets clustered distributed applications over a locally designed clustered distributed system. Our approach is based on the structural knowledge of the cluster and various distributed applications running over it. This knowledge allows to detect known and unknown attacks and avoids any kind of data loss. Usually, an communication channel is used for having communication between two or more than two computer's during which if data loss occurred then our system generate a log file at server side which is further used for recovery and counter measures to protect and recover the losses. The prototype is designed using JEE infrastructure (Java 2 Enterprise Edition) and the result generated had achieved 90% recovery of lost data over UDP as compared with TCP Protocol.**

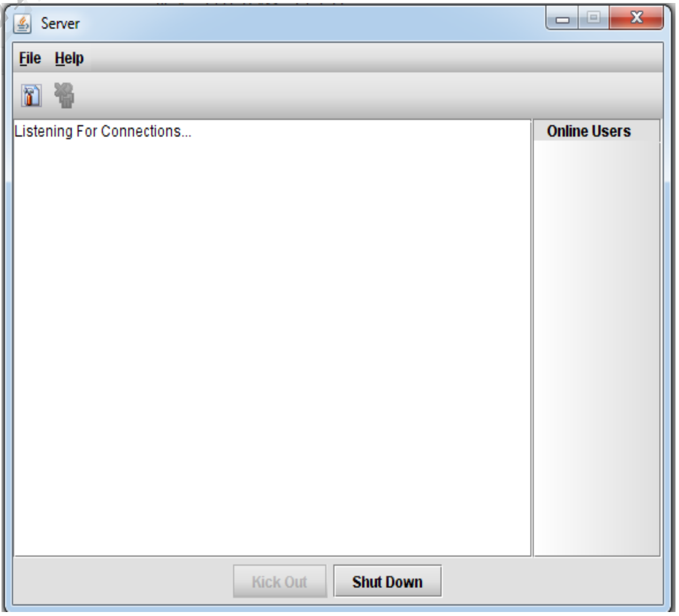
***Index Terms:* Authentication, Integrity, cluster Security, LAN Device.**

I. INTRODUCTION

The assumptions correspond to the point of view of a machine provider which rents his cluster infrastructure to different customers. We consider that each customer has a set of machines exclusively allocated to the applications. However, the local network and the Internet access are shared by all the applications. Therefore, the threat may come from outside of the cluster through the Internet .The approach is based on the principle of UDP Transformation applied to communication channels. Any attempt to use an undeclared communication channel is trapped and a recovery procedure is executed. Legal communication channels are automatically calculated from the hardware and software architectures of the system and are used to generate protection rules. Moreover, if the architecture of the system evolves, the protection rules are updated accordingly. The main characteristics of our system are: 1) minimize the workload of system administrator, 2) automate the conjuration of security components with system evolution. The main limitation relates to the scope of the detected attacks and to the supported communication protocol; the current system can only detect failure which uses illegal communication channels is based on the TCP/IP protocol.

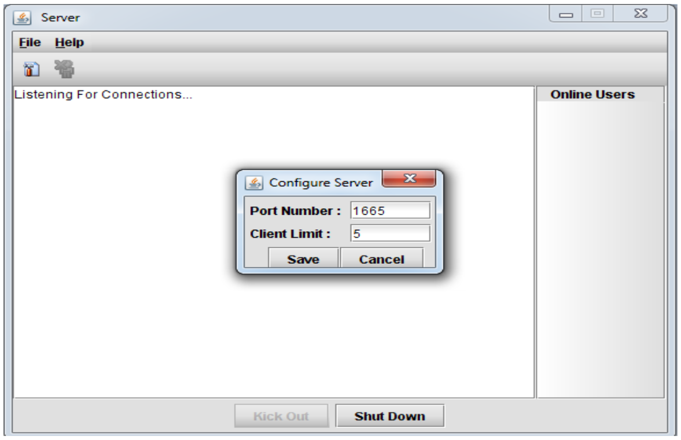
II. System Design

Our approach relies on the capacity to maintain a consistent view of the global architecture of the cluster in terms of machines, software and their interconnections (the sense of self in Forrest's terminology). For that purpose, system administrators use a deployment manager provided by the infrastructure to remotely install and interconnect software in the cluster. This deployment manager is the only way to add or remove software in the cluster. Therefore, this manager initializes the view of the global architecture and traps all modifications to maintain the consistency of the view. The self-protection manager relies on this view of the global architecture. Self-protection manager is deployment-aware: the protection rules that guard the system in terms of legal communication channels are configured automatically from the architecture and are updated accordingly when this architecture evolves. At any time, only the minimal set of communication channels is opened.



Listening For Connections...

Fig 1: Server Login (Login in the server is a done by using Authentication).



Listening For Connections...

Port Number : 1665
Client Limit : 5

Fig 2.System Configuration

Here, do enter the Port details and Client limit. This is done by the system administrator.

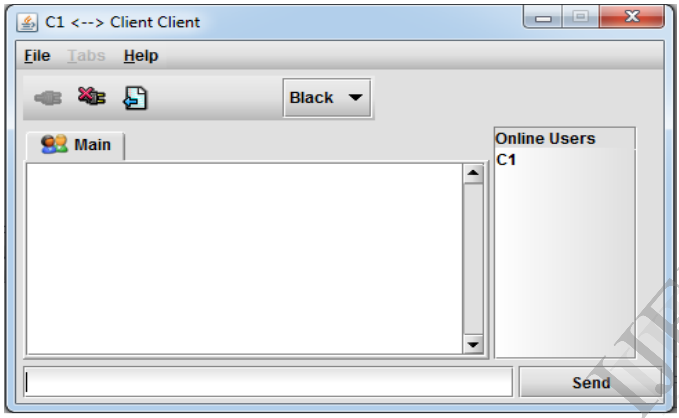
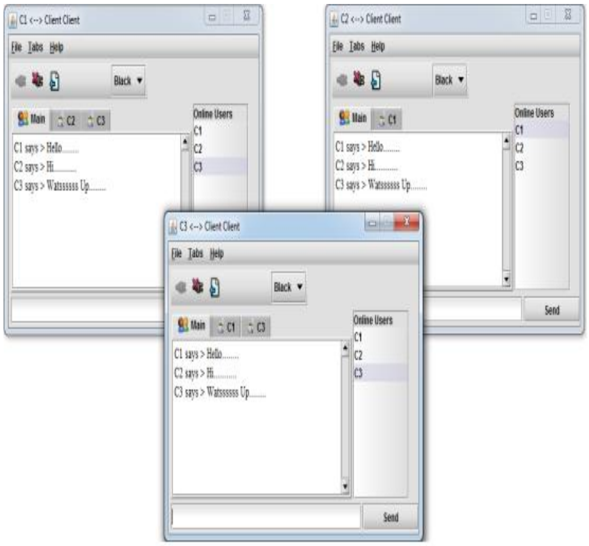


Fig.3: Client Login



C1 says > Hello.......
C2 says > Hi.........
C3 says > Watssssss Up.......

C1 says > Hello.......
C2 says > Hi.........
C3 says > Watssssss Up.......

C1 says > Hello.......
C2 says > Hi.........
C3 says > Watssssss Up.......

Fig.4: Client Communication

Above figure indicates client communication over the channel.

A. *Flowchart of proposed system:*

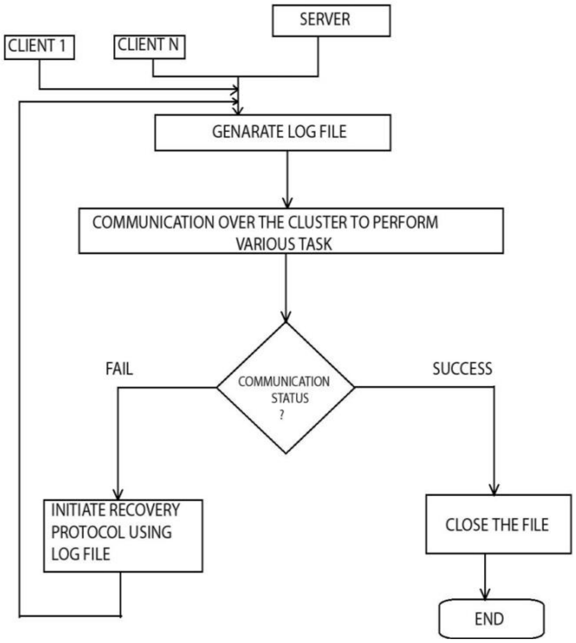

CLIENT 1
CLIENT N
SERVER
GENARATE LOG FILE
COMMUNICATION OVER THE CLUSTER TO PERFORM VARIOUS TASK
FAIL
COMMUNICATION STATUS ?
SUCCESS
INITIATE RECOVERY PROTOCOL USING LOG FILE
CLOSE THE FILE
END

Fig.5: Flowchart of the System

B. *Intrusion Detection*

There are two main approaches to detect the intrusion detection: misuse intrusion detection and anomaly intrusion detection. These are mainly use in the case of Firewalls and Intrusion Detection-Systems (IDS). Firewalls are used to Filtering gateways to detect and to block illegal communication in, IDS mainly work online perform monitoring to system .misuse intrusion detectionMain work to identify the well identified attack.Intrusion Detection-Systems (IDS) in cluster system they identify the attack .if any case the firewall is fail then the Intrusion Detection-Systems (IDS) in the action. Any attack is find out the Intrusion Detection-Systems (IDS) then this remove from the system or the block this attack. it such of the false positive and can not detect the unknown attack.

III. Design Of the Self-Protected System

Our approach of cluster system to relies on the capacity to maintain a consistent view of the global architecture of the cluster in terms of machines, software and their interconnections. For that purpose, reduce the human administrators use a deployment manager provided by the infrastructure to remotely install and interconnect software in the cluster. This system manager is the only the monitoring the system. And add or remove software in the cluster and add or remove client in the system. Therefore, this manager initializes the view of the global architecture and traps all modifications to maintain the consistency of the view.The self-protection manager relies on this view of the global architecture. It is able 1) to compute from this architecture the legal communication channels, 2) to detect and block any deviation from these communication channels

A. Self-Protected Systems

Self-protected systems are avoiding the miss communications between systems and provide the security to system which are autonomously fight back intrusions in real time. In that system we specify the cluster system. means the declare the specific user. In that system any unknown user or client can enter the system then they detect and remove or block it. Self protection manager monitoring all system performance and do it any action when any problem will be occur. Suppose in our system two user can communicate each other and any failure can occur and in that reasons information is loss in system .then requirements of other client and system manager they resend the application and the security and recovery purpose we add the Log file.

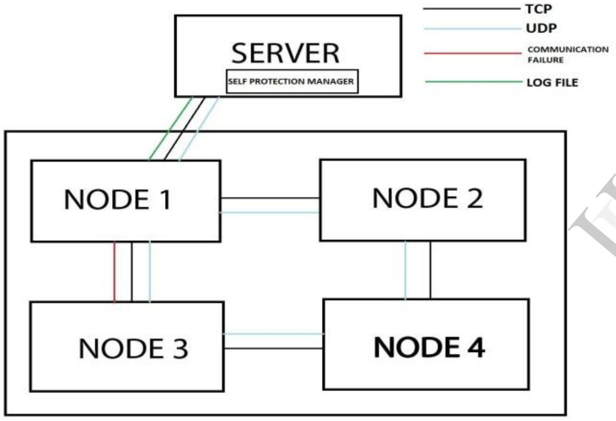


Fig.6 Self protection in cluster distributed system

in cluster communication information can transfer one client to other or multiple client. This transaction goes to secure manner we add some application like encryption and decryption for better security for cluster communication. The jhanalysis of data comparison UDP and TCP we find out the loss of information in UDP transaction. And remove it from TCP transaction. Another system is **self protection in cluster system** is tf the data loss with communication then they generated log file for the backup as well as security purpose for the database or server side

B. Self-Protection Manager

The self-protection manager is responsible of the management of the System Representation and their uses to detect illegal communications and failure information over the cluster system Self-protection manager are responsible for monitoring the system and security of the system. Manager can monitor the transaction over the cluster system. if any problem there or failure can occurs (failure communication over the client).then as backup purpose regenerate log file of this communication and again save in server site. And depend upon the client requirement they resend the application.

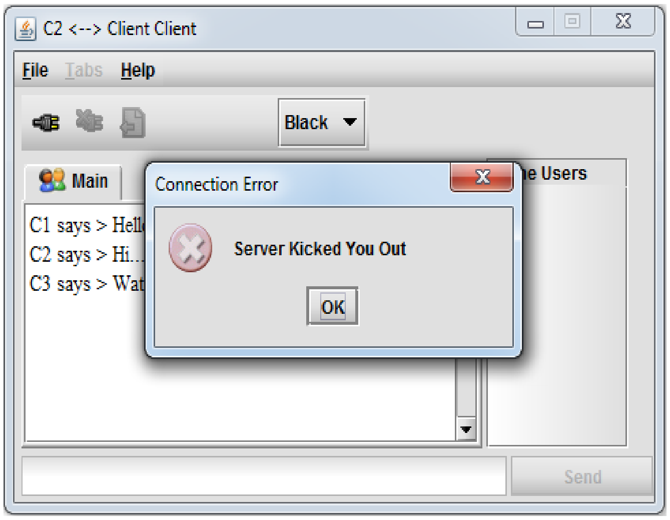
C. Backtracking Tools

Backtracking tools record detailed data about the system activity so that once an intrusion attempt has been detected, it is possible to determine the sequence of events that led to the intrusion and the potential extent of the damage (e.g., data theft/loss).ours system provides the ability to restore the system in a trusted state. It enhances the file system with a selective self-recovery capability. Logs all file system access for each process .If a process is compromised, computes illegal access for each file and is able to rollback illegal modifications. Such backtracking tools can help automate parts of this process but human expertise is still required for an accurate understanding of the attack.

D. Experimental Environment and result

We have chosen JEE clusters to evaluate our self protection system. Show in fig 2.This platform allows the construction of web application services. We modify the old cluster system in that system we add some basic application to protect the system or you can say self protection system. In that cluster system suppose any miss communication can occur or any outsider node can enter ours system then ours system can detect. Basically transaction between two server in udp connection .In that connection there are some change to data lose .we fine him how many data lose to packet counter remove this drawback with tcp connection.

Fig 7: Video information loss (Original Video size 8.56 MB. Received Video size 8.49 MB. Loss of 7 MB over UDP).



C1 says > Hell
C2 says > Hi...
C3 says > Wat

Connection Error

Server Kicked You Out

Fig .8: Connection get closed when problem occurs.

IV. *Management Of The System Representation*

In order to manage such a System Representation, we rely on the services associated with the component framework we used (Log File). Traditionally, a component framework provides services for the deployment of a component architecture and the modification (reconfiguration) of this architecture. Therefore, any administration action (machine or software installation or startup) is achieved as an action on the component architecture and reflected on the real environment, which implicitly maintains consistency between the two levels. In order to install a software, a component is deployed in the System Representation. Similarly ,to uninstall a software, its associated component is removed from the System Representation. Therefore, all the changes in the system are first performed on the System Representation which then reflects them on the legacy system. If we consider /that the communication between cluster system and they failure then analysis of the system performances and generated Log file OR the resend the application .then less change to loss system information.

V. *Level of Protection*

A. UDP PROTOCOL

UDP means the user datagram protocol it is connection less protocol.. UDP connection is simple, high speed, low functionality, it send data without setup sending data with package. it widely us access information across the internet Transmission some chance to data losses or package loss. So its better to use any other protocol To communication between two or more server .

UDP is

- Connectionless
- Does *not* guarantee delivery
- Does *not* send acknowledgments
- Unreliable, but faster than TCP
- Does *not* provide sequencing
- Does *not* resend dropped segments
- Does *not* provide flow control
- Also uses port numbers

The **Transmission Control Protocol (TCP)** is a **connection-oriented .**transport protocol, providing reliable delivery over an Internet Protocol (IP) network. Together, TCP and IP provide the core functionality for the **TCP/IP** or **Internet protocol suite**.TCP was originally defined in RFC 675, and initially designed to perform both Network and Transport layer functions. When this proved to be an inflexible solution, those functions were separated - with IP providing Network layer services, and TCP providing Transport layer services. This separation was formalized in **version 4** of TCP, defined in RFC 793.Because TCP is connection-oriented, parameters must be agreed upon by both the sending and receiving devices before a connection is established.

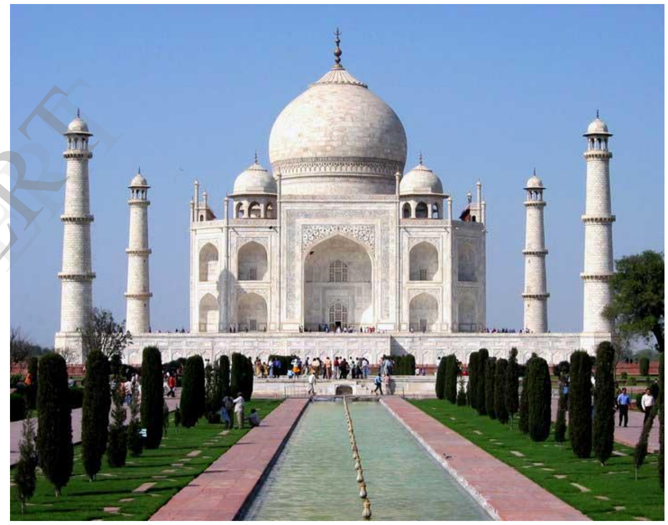


Fig 9: System 1(This is original image. Size: 51 KB)

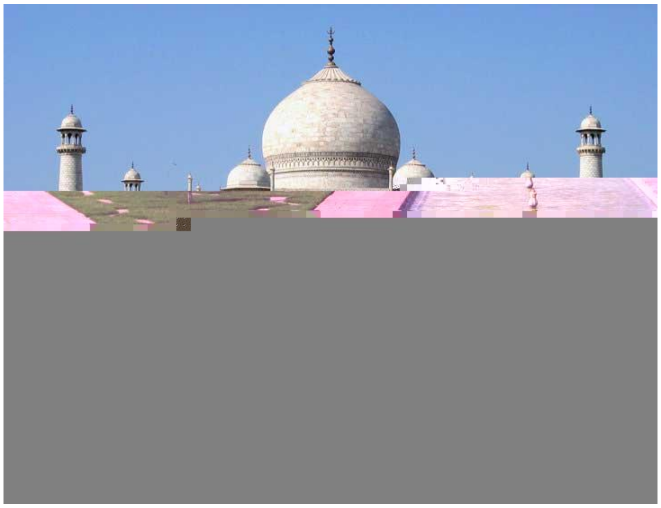


Fig.10: System 2(This image is after transmission over UDP. Size: 16 KB. Loss of 35 KB)

B. Transmission Control Protocol

TCP is

- ✓ Connection-oriented
- ✓ Guarantees delivery
- ✓ Sends acknowledgments
- ✓ Reliable, but slower than UDP
- ✓ Segments and sequences data
- ✓ Resends dropped segments
- ✓ Provides flow control
- ✓ Performs CRC on data
- ✓ Uses port numbers

TCP means transmission control protocol. It is reliable and connection oriented. It is one important protocol of transport layer, It requires connection establishment for communication. It is slower than UDP. It offers reliability by providing connection oriented end-to-end reliable packet delivery through an internetwork. It is process to process protocol. It uses flow and error control mechanisms to remove the drawbacks of data losses we add this connection in our project.

Fig .11 System 1(This is original image. Size: 51 KB)

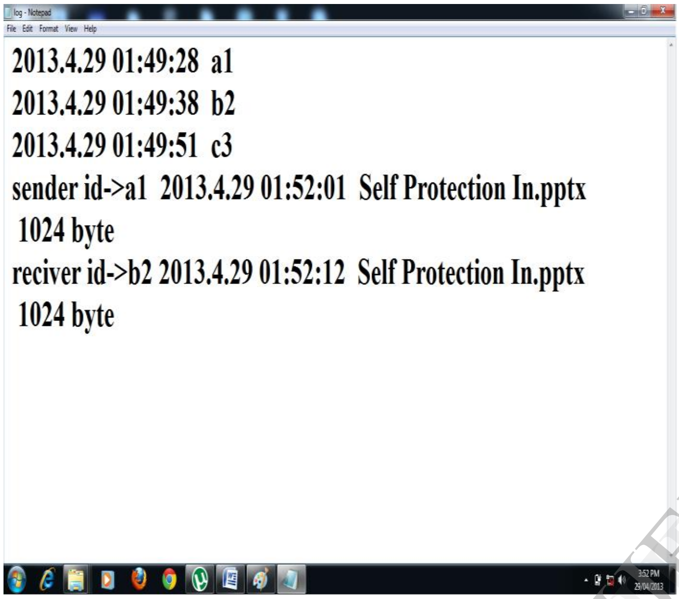
Fig.12: System 2(This is original image. Size : 51 KB Over TCP. No Loss)

C. RESEND APPLICATION

In cluster system they communicate each other with any media suppose in that any failure can occure then fail the communication or the the transmission then remove this data losses we add some application to save the information as well as time through log file. If some time problem to log file then in this information can be resend to other side or receiver side. So we can add this application in our project.

D. LOG FILE

An event log or log file consists of several independent lines of text data, which contain information that pertains to events that occur within a system. A log file might contain events from one service or different services which may come from one node or several nodes on the network. The actual setup is usually at the discretion of the administrator For this reason the contents of event logs are an important indication of the current status of the system(s) that they monitor. This makes them indispensable in systems administration and network management, are used by administrators in their general monitoring tasks. The individual nodes in a cluster report on the operation of their hardware and software by sending messages to their system log server. Recorded in the log files maintained by the system log server are indications of problems and of the various components functioning properly log file analysis program, such as Log surfer may be used to identify and, if possible, correct problems found within a cluster. In this role, the log analysis too becomes something of a “virtual system administrator”. The larger the cluster is, the more likely that one or more of its components will fail and, therefore, the more valuable these virtual administrators' become Log file analysis programs detect problems by looking for symptoms of the problem to manifest in the log files. Symptoms that can be explained unambiguously by a particular problem are known as a signature. What is to be done with a particular line or set of lines from the log file depends upon the particular signature.Log analysis programs capable of detecting complex signatures are of particular interest in cluster environments where interactions among nodes are often complex. Problems within the cluster are often not apparent when looking at these symptoms individually.



```
2013.4.29 01:49:28 a1
2013.4.29 01:49:38 b2
2013.4.29 01:49:51 c3
sender id->a1 2013.4.29 01:52:01 Self Protection In.pptx
 1024 byte
reciver id->b2 2013.4.29 01:52:12 Self Protection In.pptx
 1024 byte
```

Fig.13: log File shows events of even log-in & log-out details.

VI. CONCLUSION

Today, distributed computing environments are increasingly complex and difficult to secure. Following the autonomic computing vision, a very promising approach to deal with this issue is to implement a self-protected system The detection of an illegal communication and prevent further damages. In this vein, we have designed and implemented a self-protected system whose main characteristics are:

1) Monitoring the legal communication between cluster,

2)To automate the configuration (and reconfiguration) of security components when the system evolves,

3) To keep the protection manager (which implements the protection policy) independent from the protected legacy system. We showed how to take advantage of the knowledge of component-based application to provide a means of distinction between legal and illegal operations. We implemented prototype system for a realistic use case, a clustered JEE application. When an illegal communications detected, the self-protection manager quickly isolates the compromised nodes.

4) If any error can occur during communication between two or more computer then generated log file data are send to server.

Here, we tried successfully to improve the security over the Clustered Distributed System using TCP with testing some application and hence reduced the human effort to monitor the channel continuously.

REFERENCES

[1] S.T.King and P.M.Chen,"Bavktracking Intrusion," ACM Trans. Computer Systems, vol. 23, no. 1, pp, 51-76, 2005.

[2] L. Ertoz, E. Eilertson, A. Lazarevic, P. Tan, J. Srivastava, V. Kumar, and P. Dokas, The MINDS-Minnesota Intrusion Detection System Next Generation Data Mining. MIT Press, 2004.

[3] Self Protection In Clustered Distributed System, Noel De Palma, Daniel Hagimont, Fabienne Boyer, and Laurent Broto, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23, NO. 2, FEBRUARY 2012

[4] L. Ertoz, E. Eilertson, A. Lazarevic, P. Tan, J. Srivastava, V. Kumar, and P. Dokas, The MINDS-Minnesota Intrusion Detection System Next Generation Data Mining. MIT Press, 2004.

[5] S.Forrest, S.A.Hofmevr,A.Somayaji and T.A.Longstaff,"A Sense of Self For Unix Processes,"Proc.IEEE Symp, Research in Security and Privacy,1996.

[6] www.google.com

[7] www.dl.acm.org

[8] www.explore.ieee.org