ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com

International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue I, August 2015 in association with VEL TECH HIGH TECH DR. RANGARAJAN DR. SAKUNTHALA ENGINEERING COLLEGE, CHENNAI
National Conference on Recent Technologies for Sustainable Development 2015 [RECHZIG'15] - 28th August 2015

Detection Of Blackholeattack In Heterogeneous WSN Using Honeypot

Karthick.k [1], Yogalakshmi.R[2], Mehajabeen.M.H[3], Anusuya.R[4]
[1]Assistant Professor 2ug scholar Department of Computer Science and Engineering
Vel Tech High Tech Dr. Rangarajan Dr. Sakunthala Engineering College, Avadi, Chennai-600 062
[1]karthivel.me@gmail.com [2]yogaravi94@gmail.com [3]jabeen.inar@gmail.com
[4]anucarol27@gmail.com

ABSTRACT:

Intrusion Detection in Wireless Sensor Network (WSN) is of practical interest in many applications such as detecting an intruder in internet application and parallel computer interconnection network. Intrusion Detection is defined as mechanism for a WSN to detect the existence of inapt, incorrect, or anomalous movement of attackers. In this paper, we consider this issue according to heterogeneous WSN models with the help of HONEYPOT. A compromised Honey pot offers a wealth of features that can assist with intelligence data gathering, incident response for a better understanding of who the attacker is, what method the attacker used to gain access and the results of the attacker's unauthorized attack for possible prosecution measures.

KEYWORDS:HONEY POT, HETEROGENEOUS, BLACKHOLE, WIRELESS SENSOR NETWORK (WSN).

I. INTRODUCTION:

An **Intrusion detection system** (**IDS**) is software and/or hardware designed to detect unwanted attempts at accessing, manipulating, and/or disabling of computer mainly through a network, such as the Internet. These attempts may take the form of attacks, as examples, by crackers,malware and/or disgruntled employees. IDS cannot directly detect attacks within properly encrypted traffic.

An intrusion detection system is used to detect several types of malicious behaviors that can compromise the security and trust of a computer system. This includes network attacks against vulnerable services, data driven attacks on applications, host based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and viruses

II. WIRELESS SENSOR NETWORK (WSN)

A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations the development of wireless sensor networks was originally motivated by military applications such as battlefield surveillance. However, wireless sensor networks are now used in

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com

International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue I, August 2015 in association with VEL TECH HIGH TECH DR. RANGARAJAN DR. SAKUNTHALA ENGINEERING COLLEGE, CHENNAI
National Conference on Recent Technologies for Sustainable Development 2015 [RECHZIG'15] - 28th August 2015

many civilian application areas, including environment and habitat monitoring, healthcare applications, home automation, and traffic control

The intrusion detection application concerns how fast the intruder can be detected by the WSN. If sensors are deployed with a high density so that the union of all sensing ranges covers the entire network area, the intruder can be immediately detected once it approaches the network area. However, such a high-density deployment policy increases the network investment and may be even unaffordable for a large area. In fact, it is not necessary to deploy so many sensors to cover the entire WSN area in many applications, since a network with small and scattered void areas will also be able to detect a moving intruder within a certain intrusion distance. In this case, the application can specify a required intrusion distance within which the intruder should be detected.

According to the capability of sensors, we consider two network types: homogeneous and heterogeneous WSNs We define the sensor capability in terms of the sensing range and the transmission range. In a heterogeneous WSN some sensors have a larger sensing range and more power to achieve a longer transmission range. Internet security is increasing in importance as more and more business is conducted there. Yet, despite decades of research and experience, we are still unable to make secure computer systems or even measure their security.As a result, exploitation of newly discovered vulnerabilities often catches us by surprise. Exploit automation and massive global scanning for vulnerabilities enable adversaries to compromise computer systems shortly after vulnerabilities become known.So, in this paper, we show that howheterogeneous WSN works well with secured honey pot structure in internet.

In this concept, the alternate path selecting is main factor for eliminate the intruder. We are also deployed the cryptographic procedure for maintains the security in the network and also utilize the networking in better manner.

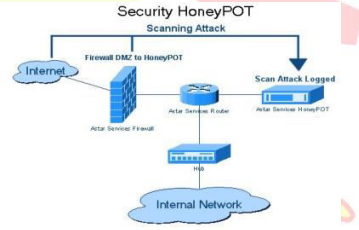

Fig 1: HoneyPOT Security

III. EXISTING SYSTEM

Many existing systems require manual definitions of normal and abnormal behavior (intrusion signatures). It is impossible to identify abnormalities automatically using machine learning or data mining techniques. These works analyze network or system activity logs to generate models or rules, which the system can use to detect intrusions that can potentially compromise the system integrity or reliability. However, previous work was according

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com

International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue I, August 2015 in association with VEL TECH HIGH TECH DR. RANGARAJAN DR. SAKUNTHALA ENGINEERING COLLEGE, CHENNAI
National Conference on Recent Technologies for Sustainable Development 2015 [RECHZIG'15] - 28th August 2015

to homogeneous single sensor in wireless sensor network. Single-sensing detection, the intruder can be successfully detected by a single sensor resulting in many false positives and undetected intrusions. In the existing an intruder can easily enter into system and access the system. So we have to prevent this intruder entry for the security purpose using Honey pot structure.

IV. PROPOSED SYSTEM:

The proposed system is based on the concept of using Intrusion Detection in Heterogeneous WSN's system by characterizing IDS with respect to network parameter.

Two detection models are:

- Single-sensing detection
- Multiple-sensing detection models

We are detecting the intruder both single sensor and multiple sensor heterogeneous wireless sensor network along with the concept of ticketing authority. The main idea of a ticketing authority is the use of issued tickets to allow clients to access network resources;

The proposed model utilizes this idea for assigning permissions to an authenticated client. The back-end server will compare the requested operation with the client's permissions to determine whether the requested operation is allowed. If the back-end server finds a discrepancy between permissions and requested operations, the back-end server will transfer the packet to the deployed honey pot for filtration.

Fig 2: Proposed Model

V. SYSTEM DESIGN:

a.Heterogeneous sensing:

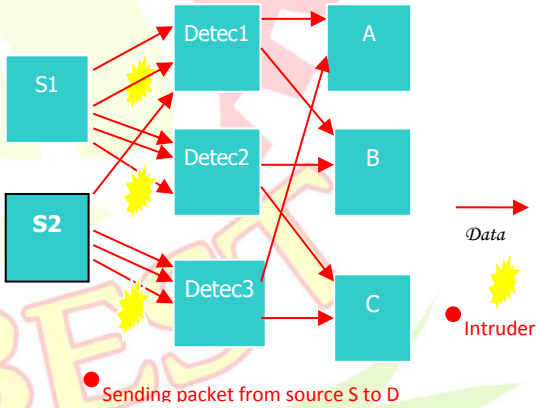

Fig 3: Sending packet from source S to D

b. Over all honey pot diagram:

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com

International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue I, August 2015 in association with VEL TECH HIGH TECH DR. RANGARAJAN DR. SAKUNTHALA ENGINEERING COLLEGE, CHENNAI
National Conference on Recent Technologies for Sustainable Development 2015 [RECHZIG'15] - 28th August 2015

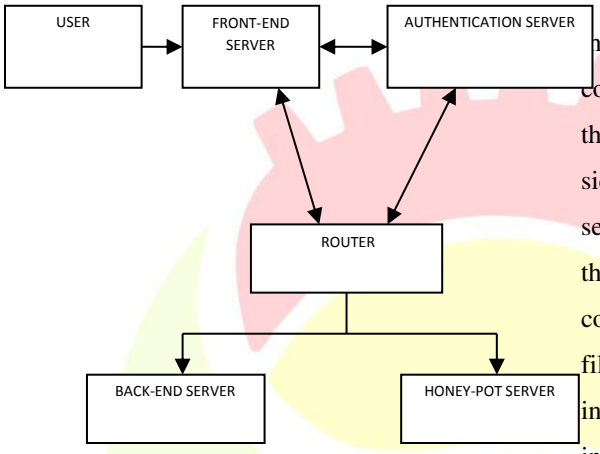

Fig 4: Overall HoneyPOT Structure

VI. MODULES DESCRIPTION:

MODULES:

Constructing sensor network

- Client module
- Front-end Server
- Authentication Server
- Router
- Back-end Server
- Honey Pot Server

a. Constructing sensor network

In this module, we are going to connect the network .Each node is connected the neighboring node and it is independently deployed in network area. And also deploy the each port no is authorized in a node.

b. Client Module:

In this module, the client sends the query to the server. Based on the query the server send the corresponding file to the client. Before this process, the client authorization step is involved. In the server side, it checks the client name and its password for security process. If it is satisfied and then received the queries form the client and search the corresponding files in the database. Finally, find that file and send to the client. If the server finds the intruder means, it set the alternative path to those intruders.

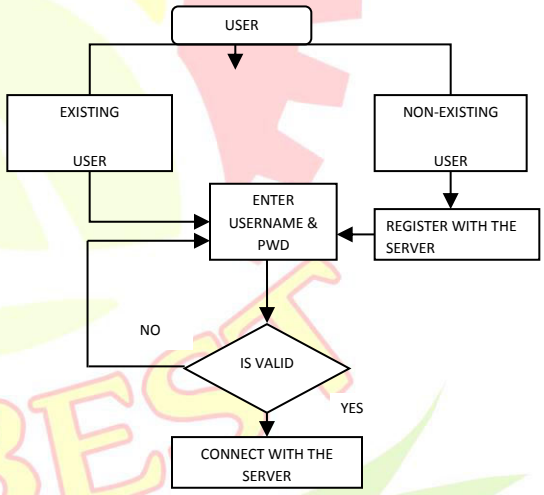

Fig 5: Structure of HoneyPOT

c. Front-End Server:

The front-end server (SF) is responsible for forwarding client requests to the router for processing. The existence of masquerading router is transparent to the client and even Front-end Server. The only load upon Front-end server is to forward the

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com

International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue I, August 2015 in association with VEL TECH HIGH TECH DR. RANGARAJAN DR. SAKUNTHALA ENGINEERING COLLEGE, CHENNAI
National Conference on Recent Technologies for Sustainable Development 2015 [RECHZIG'15] - 28th August 2015

client packet to the router and if the request involves back-end computation and to connect to AS to authenticate the client as a legitimate user. This basically involves forwarding the client request to the AS and accepting the client request or denying the client request based on the AS response contained in the reply messages

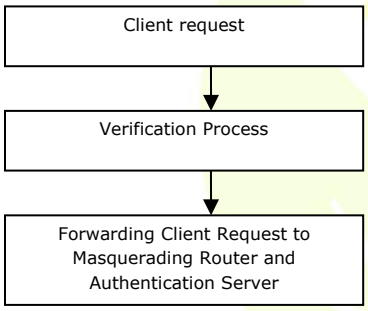

Fig 6: Flow Chart

d. Authentication Server:

The Authentication Server (AS) functions as any AS would with a few additional behaviors added to the typical client-authentication protocol. The first addition is the sending of the client authentication information to the masquerading router. The AS in this model also functions as a ticketing authority, controlling permissions on the application network. The other optional function that should be supported by the AS is the updating of client lists, causing a reduction in authentication time or even the removal of the client as a valid client depending upon the request.

e. Router:

The masquerading router is responsible for handling the clients destined to the back-end server and deciding which client is legitimate and which client should be deflected to the honey pot. The masquerading router is the only entity on the network that can automatically distinguish between the true back-end server and the honeypot.

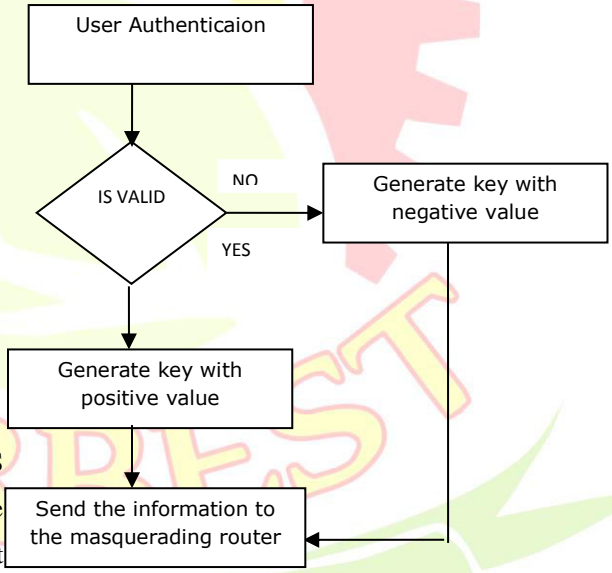

Fig 7: Authentication flow chart

It verify the key of each client, based on the key forward them to either the true back-end server or the honeypot. It is therefore suggested that the communication between the back-end server, the honeypot.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com

International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue I, August 2015 in association with VEL TECH HIGH TECH DR. RANGARAJAN DR. SAKUNTHALA ENGINEERING COLLEGE, CHENNAI
National Conference on Recent Technologies for Sustainable Development 2015 [RECHZIG'15] - 28th August 2015

f. Honey-pot Server:

The honeypot server is charged with handling illegitimate client from either an external source or a misbehaving insider. The honeypot is a simulated production environment that can perform an imitation of as small or broad functionality as required. Its messages are handled in the same way as the back-end server messages. The standard request and reply messages are processed by the honeypot without any change. The benefit of this system comes in the fact that honeypot messages are sent to the application network along with the back-end server messages. A client has no way to discern whether the message is being sent from the legitimate back-end or the honeypot. This makes the honeypot undetectable and unavoidable unless the attacker can authenticate as a legitimate client.

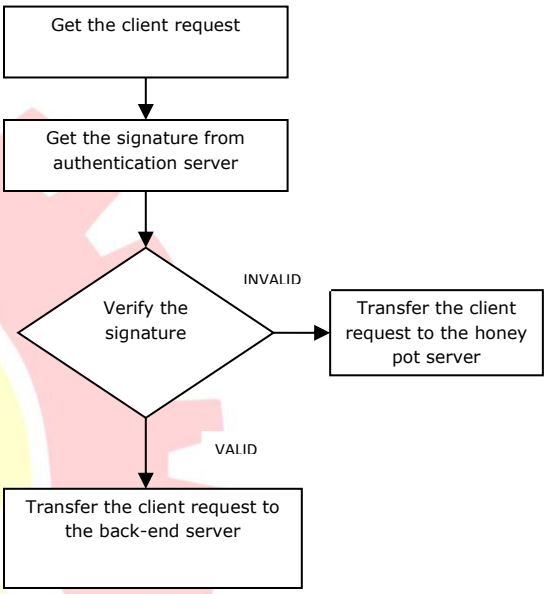

Fig 8: Router flow chart

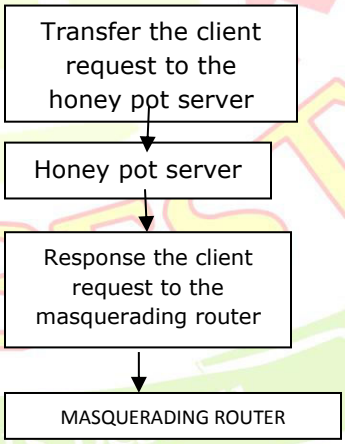

Fig 9: HoneyPot Server flow chart

g. Back-End Server:

The back-end server handles request and reply messages normally used in the security system; it provides the functionality for the more complex

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com

International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue I, August 2015 in association with VEL TECH HIGH TECH DR. RANGARAJAN DR. SAKUNTHALA ENGINEERING COLLEGE, CHENNAI
National Conference on Recent Technologies for Sustainable Development 2015 [RECHZIG'15] - 28th August 2015

operations. The client information is not stored within the back-end server. Instead, permissions are assigned to accessed objects or queries and compared to the permissions assigned to the client to test whether the client is able to legitimately access the desired information. The indirection between the client and the back-end server is therefore kept confidential via use of the masquerading router, so that the back-end server is much more insulated from corruption by the malicious user.

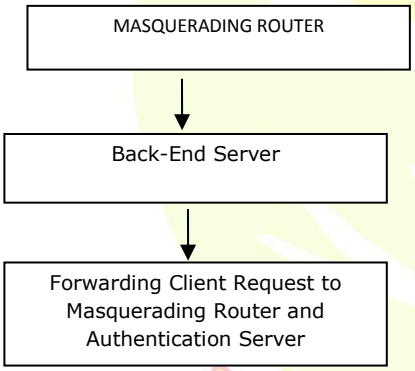

Fig 10: Back-End Server Flow Chart

VII. OVERALL DATA FLOW DIAGRAM:

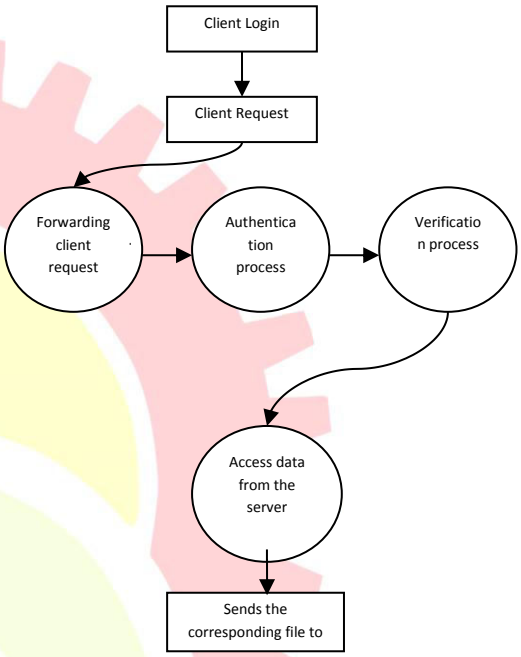

Fig 11: Overall Data Flow Diagram

VIII. FLOW CHART:

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue I, August 2015 in association with VEL TECH HIGH TECH DR. RANGARAJAN DR. SAKUNTHALA ENGINEERING COLLEGE, CHENNAI
National Conference on Recent Technologies for Sustainable Development 2015 [RECHZIG'15] - 28th August 2015

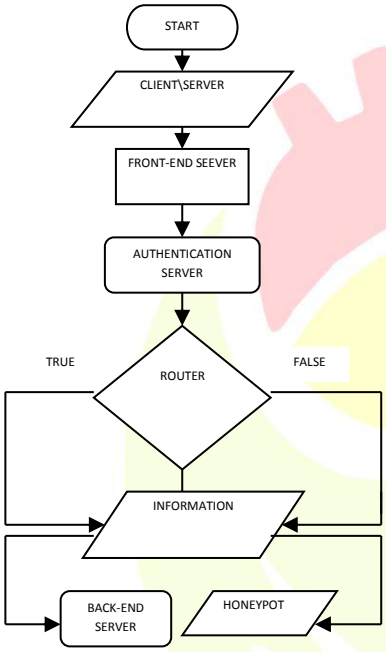

Fig 12: Flow Chart

IX. OVERVIEW:

In order to suppress malicious attacks against a back-end server, this paper proposes a network model that allows for isolation from unauthorized traffic, blacklisting of misbehaving clients, and limitation on the effectiveness of back-end DOS attacks. These objectives are accomplished by using four components within a network labeled I through IV. The first of these is the (I) back-end server itself that manages the sensitive data and operations of a web application. The overhead required of the back-end server is consistent with any Role-Based Access Control (RBAC) system in which the server must simply compare the permissions of a client with the request to access a certain resource or perform a specific operation; the only change to this system is the handling of an unauthorized request. This back-end server is isolated from the network by a separate connection to a (ii) masquerading router; this is a router that performs its function in a specialized way and changes all IP and MAC entries on packets exiting the router to the current values for the router itself. In effect, this router functions as a blinder to any traffic sent through its other network connections; this is assumed to occur only on packets destined to the network on which the back-end server is supposed to reside. This layer of indirection prevents the discovery of the actual MAC address of the back-end server's network card.

This indirection facilitates the decision process of the masquerading router to allow traffic to pass to the back-end server or deny it. This will protect the backend server from unauthorized traffic, but further measures can be taken to improve the security of the network. To that end, a (iii) honeypot should be deployed on the separate network connected by the masquerading router; a honeypot is a decoy system used to attract attack traffic for intrusion detection and analysis. More details of honeypots are provided. The router can then decide whether traffic is legitimate or not and re-transmit it to either the attached back-end server or to the attached honeypot. Since the router masquerades as the back-end server, any communication traffic out of the honeypot will

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com

International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue I, August 2015 in association with VEL TECH HIGH TECH DR. RANGARAJAN DR. SAKUNTHALA ENGINEERING COLLEGE, CHENNAI
National Conference on Recent Technologies for Sustainable Development 2015 [RECHZIG'15] - 28th August 2015

also appear to be from the masquerading router and hence appear to be from the back-end server, blinding attackers to the fact that they are in reality communicating with a honeypot.

The problem remains of deciding which traffic is legitimate. Therefore, the final component necessary for this model is an (IV) Authentication Server (AS). This server has the responsibility of authenticating legitimate clients and allowing them to utilize the sensitive information on the network via a connection to the front-end servers. This is the standard function of an AS with the additional responsibility of assigning tickets based on client permissions for use by the backend server. As part of each client's authentication, the ID and the IP address of the client are forwarded to the masquerading router for storage in its routing table. Therefore, the masquerading router will be able to determine which traffic originated from legitimate clients and which traffic has been inserted into the network or sent through a front-end server by an unauthenticated client.

X. ARCHITECTURAL DESIGN:

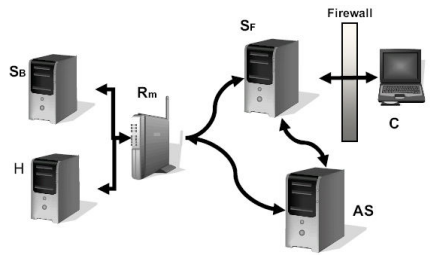

Fig 13: Architectural design

The network components required for the proposed. SB is the back-end server containing sensitive data. H is the deployed honeypot for SB. RMis the masquerading router forwarding traffic to and from H and SB, acting as a single location on the application network. SF is the front-end server connecting directly to client C through the trust boundary (in this case the firewall). AS is the authentication server (trusted).The firewall is detected between the client and server, based on the queries sent the firewall is justified. The Front-End server connects to the authentication server where authentication is only for prescribed users entering the network rather than unauthorized access. The authentication server connects to the masquerading router which decides whether the prescribed information depends on the user is to be sent to the back-end server or honeypot.

XI. PERFORMANCE EVALUATION:

System Testing

The system testing is actually series of different tests whose primary purpose is to fully exercise the computer base system. It is divided into the following

a. Recovery Testing

The recovery testing is a system testing that forces the software to fail in a variety of ways and verifies that the recovery is properly performed. While running this software, if there is no proper

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue I, August 2015 in association with VEL TECH HIGH TECH DR. RANGARAJAN DR. SAKUNTHALA ENGINEERING COLLEGE, CHENNAI
National Conference on Recent Technologies for Sustainable Development 2015 [RECHZIG'15] - 28th August 2015

connection to the backend, error message will be fired and on debugging this error could be detected and rectified.

b. **Security Testing**

The security testing is done to verify the protection mechanisms built in, to avoid improper penetration. Database security is ensured by means of restricting the update / delete and insert options and giving only read rights to the users. The "XML Query processing" is secured through the "User id" and "Password". Access rights are given to the users. The programs verify these rights. If the user has the rights, then manipulations are allowed, otherwise the program generates an error message and quits the system.

XII. FUTURE ENHANCEMENTS:

Our Future enhancements are intrusion detections in parallel computer interconnection network.

XIII. CONCLUSION:

This paper analyzes the intrusion detection problem by characterizing heterogeneous WSN with respect to the ticketing authority(i.e. honey pot)and the network parameters. We are implementing in b on client and server technology And We are also deployed the cryptographic procedure for maintaining the security level.

REFERENCES

[1]Intrusion detection in Homogeneous and Heterogeneous Wireless Sensor Network (WSN)

[2] R. Hemingway, R. Grzybowski, C. Minkenberg, and R. Luijten, "Optical-packet-switched interconnect for supercomputer applications,"OSA J. Opt. Netw., vol. 3, no. 12, pp. 900–913, Dec. 2004.

[3] C. Minkenberg, F. Abel, P. Müller, R. Krishnamurthy, M. Gusat, P.Dill, I. Iliadis, R. Luijten, B. R. Hemenway, R. Grzybowski, and E.Schiattarella, "Designing a crossbar scheduler for HPC applications,"IEEE Micro, vol. 26, no. 3, pp. 58–71, May/Jun. 2006.

[4] E. Oki, R. Rojas-Cessa, and H. Chao, "A pipeline-based approach formaximal-sized matching scheduling in input-buffered switches," IEEE Commun. Lett., vol. 5, no. 6, pp. 263–265, Jun. 2001.

[5] C. Minkenberg, I. Iliadis, and F. Abel, "Low-latency pipelined crossbar arbitration," in Proc. IEEE GLOBECOM 2004, Dallas, TX, Dec. 2004, vol. 2, pp. 1174–1179.

[6] C. Minkenberg, R. Luijten, F. Abel, W. Denzel, and M. Gusat, "Current issues in packet switch design," ACM Comput. Commun. Rev., vol. 33, no. 1, pp. 119–124, Jan. 2003.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com

International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue I, August 2015 in association with VEL TECH HIGH TECH DR. RANGARAJAN DR. SAKUNTHALA ENGINEERING COLLEGE, CHENNAI
National Conference on Recent Technologies for Sustainable Development 2015 [RECHZIG'15] - 28th August 2015

[7] C. Minkenberg, F. Abel, P. Müller, R. Krishnamurthy, and M. Gusat,"Control path implementation of a low-latency optical HPC switch," inProc. Hot Interconnects 13, Stanford, CA, Aug. 2005, pp. 29–35.

[8] C.-S. Chang, D.-S. Lee, and Y.-S. Jou, "Load-balanced Birkhoff-von Neumann switches, part I: One-stage buffering," Elsevier Comput.Commun., vol. 25, pp. 611–622, 2002.

[9] A. Tanenbaum, Computer Networks, 3rd ed. Englewood Cliffs, NJ: Prentice Hall, 1996.

[10] R. Krishnamurthy and P. Müller, "An input queuing implementation for low-latency speculative optical switches," in Proc. 2007 Int. Conf.Parallel Processing Techniques and Applications (PDPTA'07), Las Vegas, NV, Jun. 2007, vol. 1, pp. 161–167.

[11] H. Takagi, Queueing Analysis, Volume 3: Discrete-Time Systems. Amsterdam: North-Holland, 1993.