ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

Intrusion Detection & Prevention Using Anomaly Behaviour

Dhanesh B.S[1], Gowtham.M[2], Muhammad Afridi[3], Manickavasagan.G[4]

Student, Department of Computer Science & Engineering, Velammal Institute of Technology, Chennai, Tamil Nadu, India [1,2,3]

Asst. Professor, Department of Computer Science &Engineering, Velammal Institute of Technology, Chennai, Tamil Nadu, India [4]

ABSTRACT: An intrusion detection system (IDS) is developed to monitor all inbound and outbound network activity and identify any suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. IDS is considered to be a passive-monitoring system, since the main function of an IDS product is to warn you of suspicious activity taking place − not prevent them.an attack detector for cloud spoofing that utilizes MAC(Media access Control) and RSS(Received Signal strength) analysis. the protocol called Password Guessing Resistant Protocol (PGRP) helps in preventing attacks.In additional, an attack detector for cloud spoofing that utilizes MAC(Media access Control) and RSS(Received Signal strength) analysis. The attack detector will be integrated into a real-time indoor localization system, which is also capable of localizing the positions of the attackers. then the positions of the attackers can be localized using either area-based or point-based localization algorithms with the same relative errors as in the normal case. results shows that it is possible to detect cloud spoofing with both a high detection rate and a low false positive rate.

KEYWORDS: Monitoring system, identifying suspicious patterns, prevention of attacks, detect cloud spoofing

I.INTRODUCTION

The Intrusion Detection System consists of two main elements, specifically tailored to a DBMS: an anomaly detection (AD) system and an anomaly response system. The first element is based on the construction of database access profiles of roles and users, and on the use of such profiles for the Adtask. A user-request that does not conform to the normal access profiles is characterized as anomalous. An anomaly based detection is A two-step approach that involves first training a system with data to establish some notion of normality and then use the established profile on real data to flag deviations. we are going to create a search engine for accessing database.The separationof dutyconsist of duty separation, where the duty is separated to K- administrators..Petri net and its variations have been powerful tools for studying various types of asynchronous and concurrent processes [4], [5]. McDermott [6] was likely the first one to point out the usefulness of Petri nets for cyber attack modeling and observed that Petri nets are good at capturing concurrent actions of an attack [6]. Dalton et al. [7] presented a generalized stochastic Petri net to model and analyze attack trees with the ultimate goal of automating the analysis. Wu et al. [8] suggested colored Petri nets for hierarchical attack modeling to describe attacks in two levels, those being generally and specifically. When it comes to the electrical power system, Petri nets have been applied to show interdependencies between the preexisting electrical power and communications infrastructures [9]–[11]. In addition, Calderaro et al. [12] presented a Petri net-based method to identify and localize failures in the smart grid. Chen et al. intrusion detection often detects the crucial features or behaviors of the node. The trust-based model has been widely used in WSNs and P2P networks as an effective means of guarding against internal attacks [4-5], and it is often used in WSNs for security routing, which selects a secure path according to the trust evaluation of the neighbors of nodes [6]. The first trust model for WSNs is a distributed reputation-based framework described in [7], which could be used for detecting compromised or faulty

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

nodes, and the estimation of reputation is according to transactional data between nodes indicating the cooperativeness of partner nodes.However, the "cooperativeness" in [7] refers to a node's ability to deliver information or the quality of data delivered; i.e., the reputation-based framework merely focused on data accuracy or data authentication in sensor networks. An intrusion detection mechanism using trust for clustered WSNs is implemented in [8]

II.LITERATURE SURVEY

In 2017,Kaixing Huang, Qi Zhang, Chunjie Zhou, Naixue Xiong and Yuanqing Qinproposed An Efficient Intrusion Detection Approach for Visual Sensor Networks Based on Traffic Pattern Learning. In that HSOM used for intrusion detection is designed to correlate relevant features in the lower layers and integrate the low-layer SOMs into a single final view of the whole system. Specifically, a two-layer HSOM is employed here. Fig. 4 shows the proposed HSOM architecture. In layer 1, the number of SOMs is equal to the number of the nodes connected with the CH; the node-level traffic features of each node are fed into each SOM. The outputs of the layer-1 SOMs, coupled with the network-level traffic features, are the inputs of the only one SOM in layer 2.

In 2016,Alexander Kott,Richard Harangproposed an Burstiness of Intrusion Detection Process: Empirical Evidence and a Modeling Approach .The conclude that burstiness is always present, in a general case, or can be observed in all networks and in all intrusion detection processes. In other words, we only show that burstiness is present in some cases, but not necessarily in all generic cases. It is entirely possible that there may exist classes of networks, and/or associated intrusion processes, and intrusion detection processes where burstiness is either absent in principle, or cannot be detected from the available data. Identifying conditions under which burstiness exists, and can be observed, is a topic of future research. Burstiness and memory parameters suggest that the nature of the process under considerations is more reminiscent of natural processes such as earthquakes than of anthropogenic processes such as sending emails. Unlike anthropogenic processes, intrusion detection exhibits strong memory. We propose the hypothetical mechanism the Analyst Knowledge Threshold of the burstiness we observe in intrusion detection

In 2015,Xiaoxue Liu, Peidong Zhu, Yan Zhang, , and Kan Chen proposed an efficient intrusion detection mechanism, considering the constrained computation and memory resources of the smart meters. Intrusion detection is the process that monitors the events occurring in a computer system and analyzes the events to find out possible incidents. Traditional detecting technologies on malicious codes applied to computers are very power-hungry. Our proposed intrusion detection mechanism can achieve collaborativedetection of false data injection attack by setting spying domain randomly in physical memory in combination with using secret information and event log. Once the spying domain is modified, illegal reading or writing is identified.

In 2015,B´ela Genge, Member, IEEE, Piroska Haller, Member, IEEE, Cristian-Dragos¸ Dumitru, and C˘alin En˘achescuproposed an Designing Optimal and Resilient Intrusion Detection Architectures for Smart Grids. They developed two IDS network design problems for Smart Grids that accommodate traditional design requirements pertaining to shortest path routing and budgetary limitations, alongside modern security requirements including the monitoring of communication flows and the provisioning of resilient infrastructures. In order to reduce the computation time, a heuristic approach that separately solves the path selection and the IDS device distribution sub-problems was presented. The IDS design problems have been extensively analyzed in twoscenarios. The results showed the superior performance of the heuristic methodology in terms of computation time and its applicability to large problem instances
In 2013,Nikos Tsikoudis, Antonis Papadogiannakis , Evangelos P. Markatos proposed LEoNIDS: A Low-Latency and Energy-Efficient Network-Level Intrusion. In that An attacker could try to exploit the flow cutoff mechanism used for priority assignment in order to increase detection latency and impede a timely reaction. Thus, we aim to protect LEoNIDS against such attacks. One way to exploit the cutoff mechanism would be to overburden the system with highpriority packets, *e.g.*, by sending a large number of small flows. However, as we explain in the following sections, LEoNIDS properly adapts to the traffic load by increasing frequency and active cores so that the latency of high-priority packets remains always low. In the worst case, *e.g.*, a fully utilized system only with high-priority packets,

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

LEoNIDS will approach the behavior of the original system: it may spend the maximum available power to keep latency of high-priority packets low.

III.PROPOSED SYSTEM

In proposed system, an administration model that is based on the well-known security principle of separation of duties (SoD). SoD is a principle whereby multiple users are required in order to complete a given task. As a security principle, the primary objective of SoD is prevention of fraud (insider threats), and user generated errors. Such objective is traditionally achieved by dividing the task and its associated privileges among multiple users. Our approach instead applies the technique of threshold cryptography signatures to achieve SoD. a novel Joint Threshold Administration Model (JTAM) that is based on the principle of separation of duty with the existing Intrusion Response System. The key idea in JTAM is that a policy object is jointly administered by at least k database administrator (DBAs), that is, any modification made to a policy object will be invalid unless it has been authorized by at least k DBAs. the design details of JTAM which is based on a cryptographic threshold signature scheme, and show how JTAM prevents malicious modifications to policy objects from authorized users. the implementation of JTAM in the PostgreSQL DBMS is also done. so the report experimental result techniques used are proved to be efficient.

SYSTEM DESIGN

The system design contains 3 layers namely :Application Layer, Business Layer, Data Layer. The Application Layer consists of Home page, Registration, Order, Material Required,Labor Registration, Transaction , Sale and Feedback. The Application Layer's main role is the design of the user interface which is used by the users to interact with the system. The Business Layer consists of Customer Registration, Register new product, Materials purchase, Register for delivery etc. It's main role is to act as a communication link between application layer and data link layer.

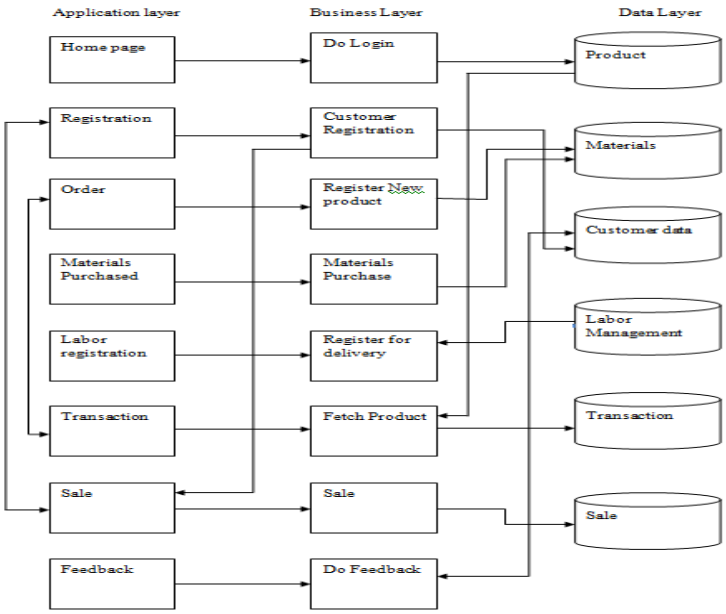

FIG 1.SYSTEM DESIGN

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

1.INTRUDER DETECTION SYSTEM:

It consists of two main elements, specifically tailored to a DBMS: an anomaly detection (AD) system and an anomaly response system. The first element is based on the construction of database access profiles of roles and users, and on the use of such profiles for the Adtask. A user-request that does not conform to the normal access profiles is characterized as anomalous. Profiles can record information of different levels of details. After that we taking some actions once an anomaly is detected.

1.1 **SEPARATION OF DUTY**

In this module , it consist of duty separation, where the duty is separated into K- administrators. Our main goal is to detect the inside hackers who is having the DBA roles in an organization, so the separation of duty process is based on preventing those malicious activity held by inside hackers.

1.2 **ANOMALY DETECTION:**The main goal of the project is to detect anomaly to prevent database hacking. So in this module, the planning will be esthablished for finding out those anomaly exactly by using the separation of duty.

2.DATABASE QUERY:

In this module, it is going to create a search engine for accessing database. If a user want to access the database, they should give their query in this search engine. This search engine is made for secure access of database. For accessing database, the user has to give query as the format of SQL query.

3. PASSWORD GENERATION:

After giving query, the user has to redirect to the respective database which they want to access. The user has to provide database password for accessing. If the user don't have password, then they will be redirected to password generation process.

4.DATABASE AUTHENTICATION: After giving query, the user has to give password for accessing those database. This module is developed mainly for preventing inside intruder.

5.POLICY MATCHING:

Policy matching is the problem of searching for policies applicable to an anomalous request. When an anomaly is detected, the response system must search through the policy database and find policies that match the anomaly. to present two efficient algorithms that take as input the anomalous request details, and search through the policy database to find the matching policies. We implement our policy matching scheme in the PostgreSQL DBMS,and discuss relevant implementation issues. We also report experimental results that show that our techniques are very efficient. The second issue that we address is that of administration of response policies. Intuitively, a response policy can be considered as a regular database object such as a table or a view. Privileges, such as create policy and drop policy, that are specific to a policy object type can be defined to administer policies. However, a response policy object presents a different set of challenges than other database object types. Recall that a response policy is created to select a response action to be executed in the event of an anomalous request.

6.POLICY ADMINISTRATION:

In this module, we are going use administration model as the Joint Threshold Administration Model (JTAM) for managing response policy objects, The three main advantages of JTAM are as follows: First, it requires no changes to the existing access control mechanisms of a DBMS for achieving SoD. Second, the final signature on a policy is nonrepudiable, thus making the DBAs accountable for authorizing a policy operation. Third, and probably the most important, JTAM allows an organization to utilize existing man-power resources to address the problem of insider threats since it is no longer required to employ additional users as policy administrators.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

6.1 SECURITY ADMINISTRATION:
In policy administration, the authentication is performed based on the security attributes. The security attributes is in the form of question pattern. The first set of question pattern having basic type of questions like user personal information, and system personal information.

6.2 DATABASE ATTRIBUTES:
The database attribute is another set of question pattern where, the user has to provide answer for database attributes like database schema, data relation and etc...
.

7.RESPONSE ACTION SELECTION:
We propose the following two rank based selection options that are based on the severity level of the response actions:

7.1 MOST SEVERE POLICY:
The severity level of a response policy is determined by the highest severity level of its response action. This strategy selects the most severe policy from the set of matching policies.It categorized according to their severity levels. Also, in the case of interactive ECA response policies, the severity of the policy is taken as the severity level of the Failure Action.

7.2 LEAST SEVERE POLICY:
This strategy, unlike the Most Severe Policy strategy, selects the least severe policy. The response action is selected based on the severity level of the intruder. The severity level is decided based on the database which the intruder tries to access.

8. ACCESSING DATABASE:
Finally, the user will be authenticated, and if the user is administrated as valid user, they will be allowed to accessing the database. The details given by the user like user id ,password is verified by the data which has been already stored in the database. The query provided by the user to access the database is checked by the administrator whether it is a valid query and whether the user has the authorization to access the database mentioned in the query.After the user has been authenticated and authorized,the user is granted access to the database.

IV.RESULTS

The proposed framework is being simulated in a simple network environment with one server and minimum of two systems. The software for each type of agent was written in JAVA JDK Version 1.2 on a Microsoft Windows environment. The building of user profile deals with the essential details like user identification, user authentication and level of user. This simulation manages the user profile in three levels. All the users in this simulation are associated with information about the software application. The following are the some of the snapshots of the simulation which gave most efficient and effective results

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

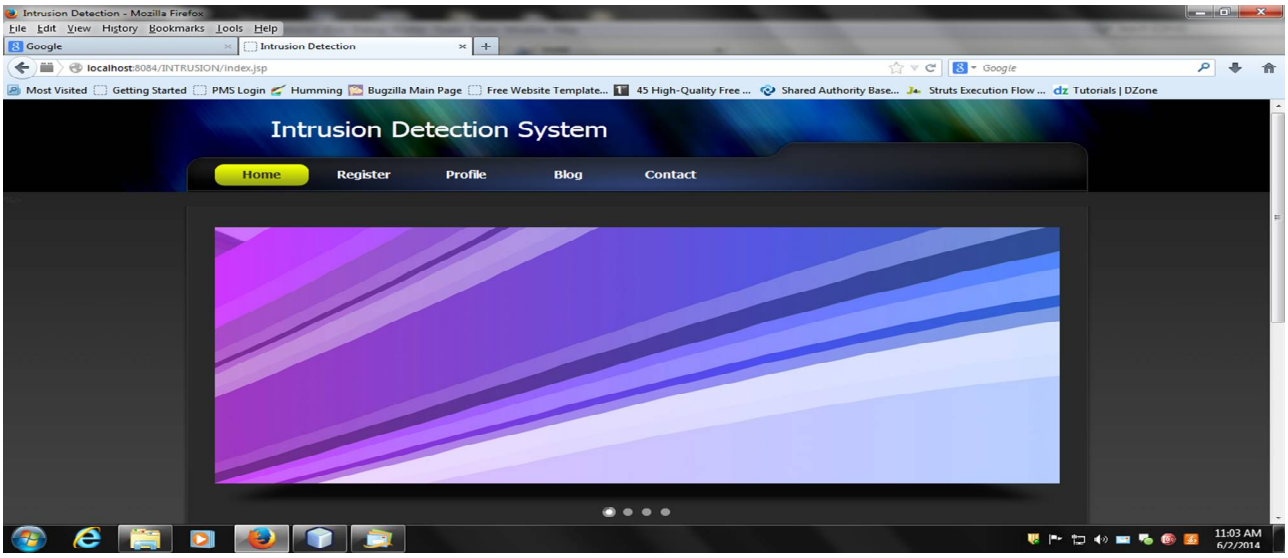

FIGURE 2-Home Page

The figure 2 shows the home page of the application where the details about the organization is displayed.

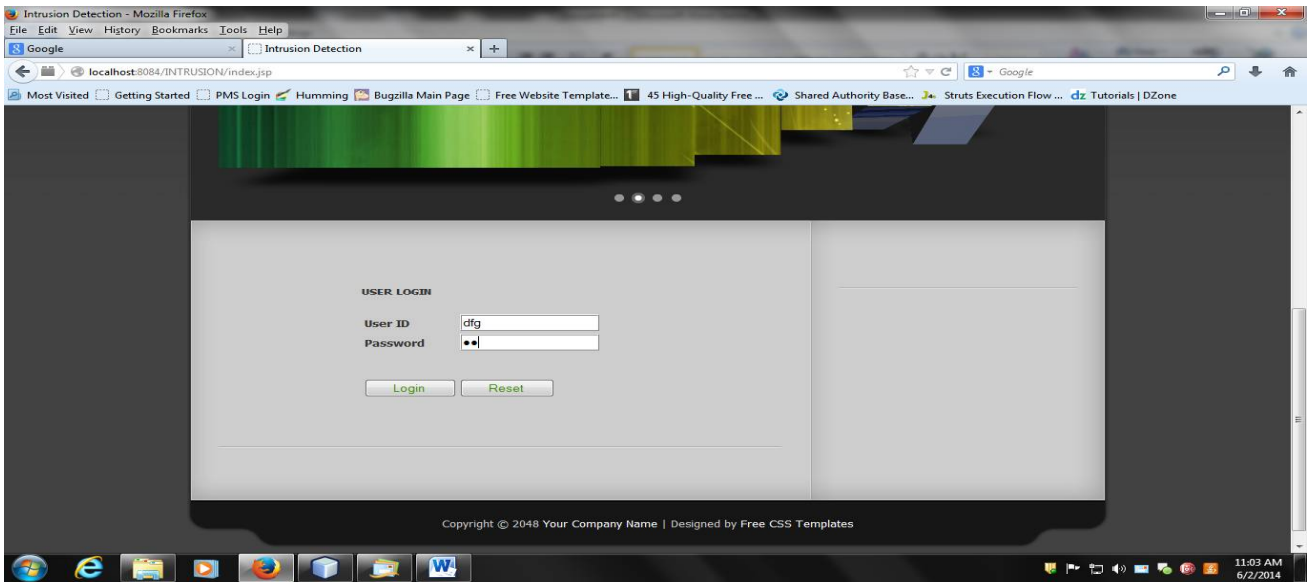

FIGURE 3-User login

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

The figure 3 shows the user login where the user needs to enter the login details like user id and password. The user id and password is unique for each user.

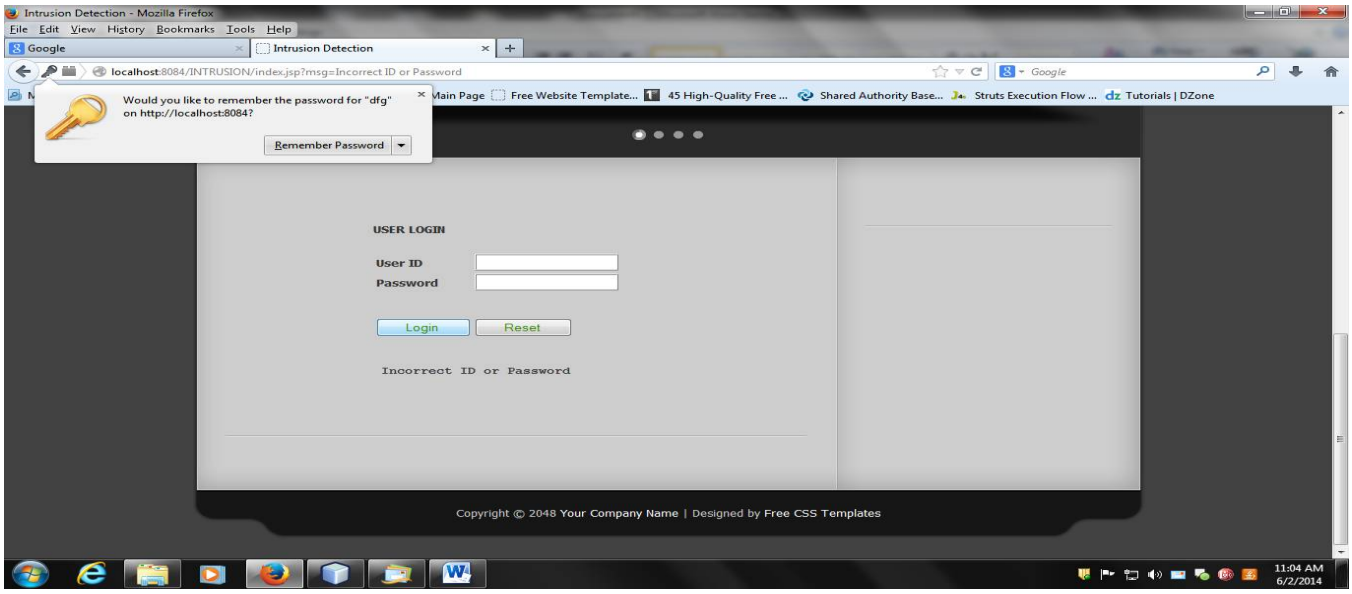

FIGURE 4Unauthorized user

The figure 4 shows, when the user has entered a wrong user id or password the user will be prompted with a message "Incorrect ID or Password". The user is allowed a maximum of 3 attempts only. After that the users will be directed to another page where the user will be authorized.

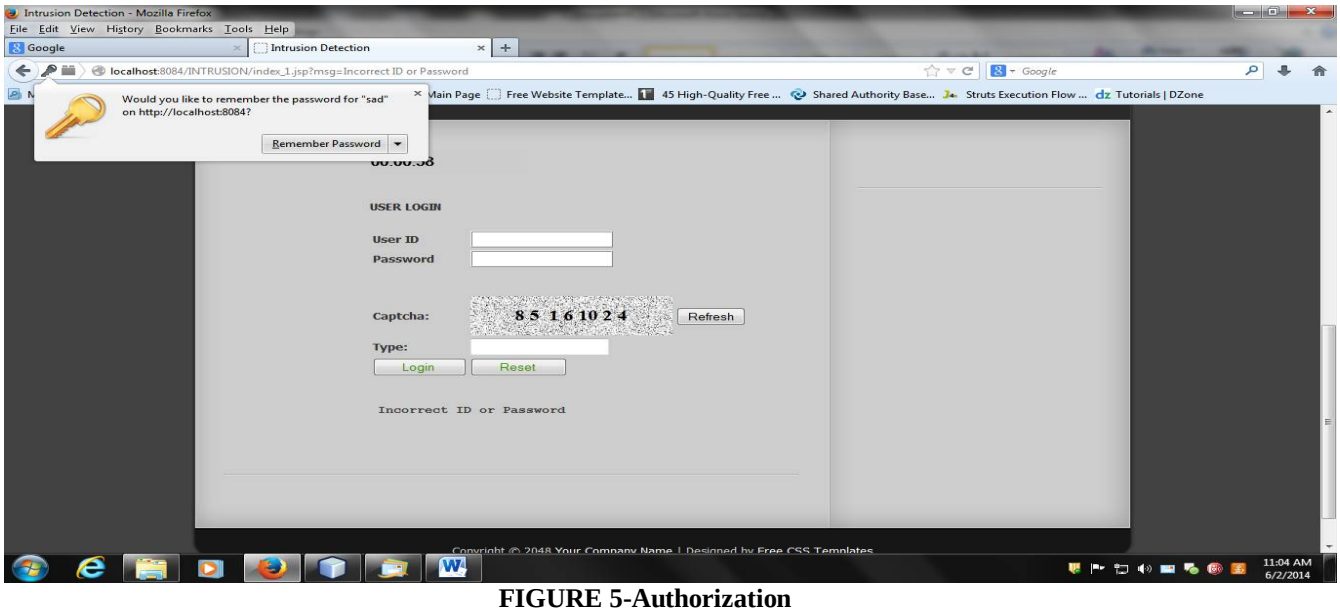

FIGURE 5-Authorization

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

The figure 5 shows the authorization of the proposed system which will be executed when the user has exceeded the number of attempts allowed per login (3 attempts). After the user has exceeded the number of attempts he needs to enter the randomly generated captcha.The captcha is an Automated Turing Test used to check whether it's a intruder or an authorized user. The captcha is used to prevent the Brute force attack by the intruder.

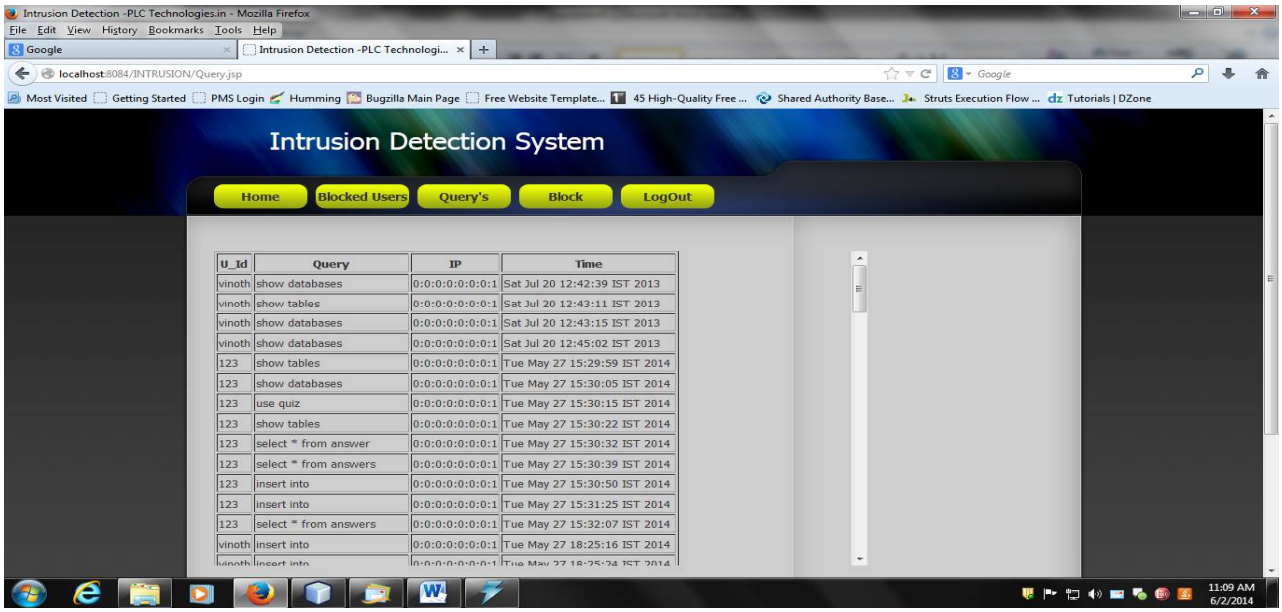

FIGURE 6- User details

The figure 6 shows the details with which the user tries to access the data resource like user id , query , IP address and the time of login of the user. It gives details like the user id , the query used to access the database , user's IP address and the time when the request was made. The administrator monitors these details to find anomalies in the user access.

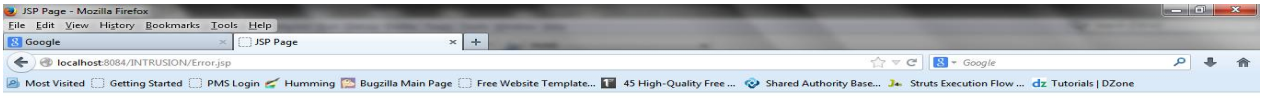

FIGURE 7- Blocked User

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

The figure 7 shows that if an unauthorized user who has been blocked by the administrator tries to access the data resources in the database. The administrator blocks the user if tries to access the resources for which the user hasn't been granted access.

V.CONCLUSION

The main objective of this paper is to provide the necessity and utility of the intrusion detection system.The model that has been used is Joint Threshold Administration Model (JTAM) that is based on the principle of separation of duty with the existing Intrusion Response System. JTAM is that a policy object is jointly administered by at least kdatabase administrator (DBAs), that is, any modification made to a policy object will beinvalid unless it has been authorized by at least k DBAs. The design details of JTAM which is based on a cryptographic threshold signature scheme, and show howJTAM prevents malicious modifications to policy objects from authorized users. implement JTAM in the PostgreSQL DBMS, and report experimental results.

REFERENCES

[1] J. Zhong, R. Zheng, and W. Yang, "Construction of smart grid at information age," Power Syst. Technol., vol. 33, no. 13, pp. 12–18, 2009.
[2] Y. Yu, "Technical composition of smart grid and its implementation sequence," South. Power Syst. Technol., vol. 3, no. 2, pp. 1–5, 2009.
[3] W. Wang, Y. Xu, and M. Khanna, "A survey on the communication architectures in smart grid," Comput. Netw., vol. 55, no. 15, pp. 3604–3629, 2011.
[4] R. David and H. Alla, Discrete, Continuous, and Hybrid Petri Nets. Berlin, Germany: Springer-Verlag, 2005, pp. 289–294.
[5] K. Jensen and L. Kristensen, Coloured Petri Nets: Modelling and Validation of Concurrent Systems. Berlin, Germany: Springer-Verlag, 2009, pp. 193–198. [6] J. McDermott, "Attack net penetration testing," in Proc. Workshop New Security Paradigms (NSPW), Cork, Ireland, 2000, pp. 15–21.
[7] G. Dalton, R. Mills, J. Colombi, and R. Raines, "Analyzing attack trees using generalized stochastic Petri nets," in Proc. IEEE Workshop Inf. Assur., West Point, NY, USA, 2006, pp. 116–123.
[8] R. Wu, W. Li, and H. Huang, "An attack modeling based on hierarchical colored Petri nets," in Proc. IEEE Int. Conf. Comput. Elect. Eng. (ICCEE), Phuket, Thailand, 2008, pp. 918–921.
[9] K. Schneider, C.-C. Liu, and J.-P. Paul, "Assessment of interactions between power and telecommunications infrastructures," IEEE Trans. Power Syst., vol. 21, no. 3, pp. 1123–1130, Aug. 2006.
[10] O. Gursesli and A. Desrochers, "Modeling infrastructure interdependencies using Petri nets," in Proc. IEEE Int. Conf. Syst., vol. 2. Washington, DC, USA, 2003, pp. 1506–1512.