*International Journal of Current Research in Multidisciplinary (IJCRM)* *ISSN: 2456-0979*
Vol. 3, No. 9, (September'18), pp. 08-11

# Requirement Based Intrusion Detection In Addition To Prevention via Advanced Metering Infrastructure

## ABSTRACT

*An intrusion detection system (IDS) is designed 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 IDS essentially reviews your network traffic and data and will identify probes, attacks, exploits and other vulnerabilities. IDSs can respond to the suspicious event in one of several ways, which includes displaying an alert, logging the event or even paging an administrator. In some cases the IDS may be prompted to reconfigure the network to reduce the effects of the suspicious intrusion. The proposed protocol called Password Guessing Resistant Protocol (PGRP), helps in preventing such attacks and provides a pleasant login experience for legitimate users. PGRP limits the number of login attempts for unknown users. In additional we propose an attack detector for cloud spoofing that utilizes MAC (Media access Control) and RSS(Received Signal strength) analysis. Next, we describe how we integrated our attack detector into a real-time indoor localization system, which is also capable of localizing the positions of the attackers.*

**KEY TERMS***: Intrusion detection system (IDS), Advanced metering infrastructure (AMI), separation of duty (SOD).*

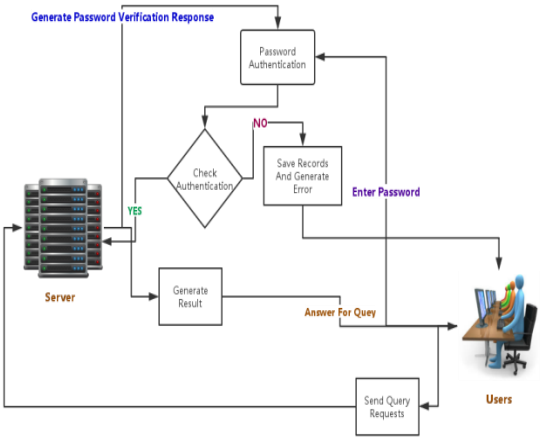
## INTRODUCTION

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces electronic reports to a management station. IDS is a monitoring system to detect any unwanted entity into a system (like AMI in our context). IDS can be signature-based, specification-based, and anomaly-based. It is important to understand the specific properties and constraints of this unique infrastructure in order to develop a relevant intrusion detection system (IDS).A signature-based IDS builds a back list of attacks. It is not suitable for AMI because new types of attacks are growing frequently since AMI is an emerging system.AMI can be conceived as an attachment for providing bidirectional communication between user domain to utility domain. This sophisticated infrastructure forms a high speed media to exchange information flow between these domains. The principle functionalities of AMI encompasses bidirectional communication and power measurement facilities, assisting adaptive power pricing and demand side management, self-healing ability, and providing interfaces for other systems.

Intrusion prevention is a preemptive approach to network security used to identify potential threats. Like an intrusion detection system (IDS) an intrusion prevention system monitors network traffic. Because an exploit may be carried out very quickly after the attacker gain access. The intrusion prevention system also has the ability to take immediate action based on the set of rule established by the administrator.

## ARCHITECTURE DIAGRAM




## RSA ALGORITHM:

RSA stand for Ron Rivest, Adi Shamir, and Leonard Adleman. It is used to encrypt and decrypt message. It is an asymmetric cryptographic algorithm .There are two different keys.Private key must be kept seceret. Public key is known to everyone.RSA algorithm used for securing sensitive data, particularly when being sent to over an insecure network such as internet. It assure the confidentiality, integrity, authenticity, and non-reputability of electronic communication and data storage.

## OPERATION:

RSA make use of public key and private key. Public key is used to encrypt the message. The encrypted message can be decrypted by using only private key. Four steps involved in RSA Algorithm.

## KEY DISTRIBUTION

To enable A to send his encrypted message, B transmit his public key (n,e)

## ENCRYPTION:

Suppose B would like to send message M to A. First turn M into an integer m, such that $0<m<n$ and gcd(m,n=1). This can be effectively done for 500 bit numbers using exponentiation. B then transmit c to A.

$$C=m^e \bmod n$$

## DECRYPTION:

A can recover m from c by using private key.

$$m=(m^e)^d=m \bmod n$$

Given m, we can recover the original message M by reversing the padding method.

## DESCRIPTION

### A) INTRUSION DETECTION SYSTEM:

It consists of two main elements, specially tailored to a DBMS, an anomaly detection (AD) system and 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 attacks. A user- request that does not conform to normal access profiles is characterized as anomalous. Profiles can record information of different level of details. After that we taking some action once an anomaly is detected.

### B) SEPERATION OF DUTY:

This module consists of duty separation, where the duty is separated to 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.

### C) ANOMALY DETECTION:

The main goal of our project is to detect anomaly to prevent database hacking. So in this module, we are going to establish the planning for finding those anomaly exactly using separation of duty.

### D) DATABASE QUERY:

In this module, we are 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.
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.

### E) DATABASE AUTHENTICATION:

After giving query, the user has to give password for accessing those databases. This module is developed mainly for preventing insider intruder.

### F) 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. We present two efficient algorithms that take as input the anomalous request details, and search through the policy database to find the matching policies. The issues that we address is that of administrator of response policies. 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.

### G) POLICY ADMINISTRATOR:

In this we are going to use administrator model as the joint Threshold Administration Model (JTAM) for managing response policy objects. The advantage of JTAM are it requires no changes to the existing acces control mechanisms of a database for achieving seperation of duty. It also allows an organization to utilize existing man power resources to address the problem of insider threats since it no longer required to employ additional users as policy administrators.

### H) SECURITY ATTRIBUTES:

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.

## DATABASE ATTRIBUTE:

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

## I) 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.

## CONCLUSION

In this paper we have introduced new approach for detecting malicious activities in AMI. Securing information is become an legitimate concern for organization and computer user. Many different techniques is used to secure the information of an organization against inner threats and attacks. So, in this paper we have exploited inner threats attacks, and database hacking. We have achieved confidentiality and avoiding from corruption of information. We identify that specification based intrusion detection technology has potential to meet the hackers and constraints of an AMI.

## REFERENCE


[1] A. Conry-Murray, "The Threat from within. Network Computing (Aug. 2005)," http://www.networkcomputing.com/showArticle.jhtml?articleID=166400792, July 2009.

[2] R. Mogull, "Top Five Steps to Prevent Data Loss and Information Leaks. Gartner Research (July 2006)," http://www.gartner.com, 2010.

[3] M. Nicolett and J. Wheatman, "Dam Technology Provides Monitoring and Analytics with Less Overhead. Gartner Research (Nov. 2007)," http://www.gartner.com, 2010.

[4] R.B. Natan, Implementing Database Security and Auditing. Digital Press, 2005

[5] J.-C. Laprie, K. Kanoun, and M. Kaaniche, "Modellinginterdependen- cies between the electricity and information infrastructures," in *Proc. 26th Int. Conf. Comput. Safety Rel. Security (SAFECOMP)*, Nuremberg, Germany, 2007, pp. 54–67.

[6] V. Calderaro, C. N. Hadjicostis, A. Piccolo, and P. Siano, "Failure iden- tification in smart grids based on petri net modeling," *IEEE Trans. Ind. Electron.*, vol. 58, no. 10, pp. 4613–4623, Sep. 2011.

[7] T. M. Chen, J. C. Sanchez-Aarnoutse, and J. Buford, "Petri net modeling of cyber-physical attacks on smart rid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 741–749, Apr. 2011.

[8] R. Berthier and W. H. Sanders, "Specification-based intrusion detection for advanced metering infrastructures," in *Proc. Pac. Rim Int. Symp. Depend. Comput. (PRDC)*, Pasadena, CA, USA, 2011, pp. 184–193.

[9] M. LeMay, G. Gross, C. A. Gunter, and S. Garg, "Unified architecture forlarge-scale attested metering," in *Proc. 40th Annu. Hawii Int. Conf. Syst. Sci. (HICCS)*, Waikoloa, HI, USA, 2007, pp. 126–135.

[10] F. M. Tabrizi and K. Pattabiraman, "A model-based intrusion detection system for smart meters," in *Proc. IEEE 15th Int. Symp. High-Assur. Syst. Eng. (HASE)*, Miami Beach, FL, USA, 2014, pp. 17–24.

[11] M. A. Faisal, Z. Aung, J. R. Williams, and A. Sanchez, "Securing advanced metering infrastructure using intrusion detection system with data stream mining," in *Proc. Pac. Asia Workshop Intell. Security Informat.*, Kuala Lumpur, Malaysia, 2012, pp. 96–111.

[12] Y. Chongyi, *Principles and Applications of Petri Net*, Beijing, China: Electron. Ind. Press, 2005, p. 16.

[13] J. Peterson, "Petri nets," *ACM Comput. Surv.*, vol. 9, pp.223–252, Sep. 1977.

[20] M. Diaz, *Petri Nets: Fundamental Models, Verification and Applications.* Hoboken, NJ, USA: Wiley, 2009.

[14] V. Kordic, *Petri Net Theory and Applications*. Vienna, Austria:I-Tech Educ., 2008.