International Journal of Computing and Artificial Intelligence

E-ISSN: 2707-658X
P-ISSN: 2707-6571
www.computersciencejournals.com/ijcai
IJCAI 2024; 5(1): 96-101
Received: 05-01-2024
Accepted: 13-02-2024

Sadhna Devede
M. Tech Student,
Department of CSE, Oriental Institute of Science & Tech.,
State, Madhya Pradesh, India

Shivank Soni
Assistant Professor,
Department of CSE, Oriental Institute of Science & Tech.,
State, Madhya Pradesh, India

Corresponding Author:
Sadhna Devede
M. Tech Student,
Department of CSE, Oriental Institute of Science & Tech.,
State, Madhya Pradesh, India

A review intrusion protection system on the internet/network

Sadhna Devede and Shivank Soni

DOI: https://doi.org/10.33545/27076571.2024.v5.i1b.87

Abstract
Intrusion Protection System (IPS) defined as a Device or software application which monitors the internet/network or system activities and finds if there is any malicious activity occur. Outstanding growth and usage of internet raises concerns about how to communicate and protect the digital information safely. In today's world hackers use different types of attacks for getting the valuable information. Many of the intrusion Protection techniques, methods and algorithms help to detect those several attacks. The main objective of this paper is to provide a complete study about the intrusion Protection, types of intrusion Protection methods, types of attacks, different tools and techniques, research needs, challenges and finally develop the IPS Tool for Research Purpose That tool are capable of detect and prevent the intrusion from the intruder.

Keywords: Intrusion protection system, need, type of IPS, protection techniques, functioning of IPS, components, application based IPS, tools of IPS

Introduction
In today's world internet security has become a challenge for organisations. To protect credential data from the intruders. In process of safeguarding the data Web Firewalls, encryption, authentication and Virtual Private Internet/network s (VPN) have been deployed since a long time to secure the internet/network infrastructure and communication over the internet. Intrusion Protection is a relatively new addition to set of security technologies.
IPS is an evolution which enhance the internet/network security and safeguarding the data of the organisation. The IPS helps the internet/network administrator to detect any malicious activity on the internet/network and alerts the administrator to get the data secured by taking the appropriate actions against those attacks.
An intrusion refers to any unauthorized access or malicious utilization of information resources. An intruder or an attacker is a real world entity that tries to find a means to gain unauthorized access to information, causes harm or engage in other malicious activities.
The Intrusion Protection system is about the firewall security. The firewall protects an organization from the malicious attacks from the Internet and the IPS detects if someone tries to access in through the firewall or manages to break in the firewall security and tries to have an access on any system in the organization and alerts the system administrator if there is an undesired activity in the firewall.
Therefore, an Intrusion Protection system (IPS) is a security system that monitors internet/network traffic and computer systems and works to analyse that traffic for possible hostile attacks originating from outside the organization and also for misuse of system or attacks originating from inside the organization.

Need
Now a day's internet has become part of our daily life infect, the business world is getting connected to Internet. Number of peoples are getting connected to the Internet every day to take advantage of the new business model which is known as e-Business. Connectivity enhancement has therefore become very critical aspect of today's e- business.
There are two phases of business on the Internet. First phase is the Internet brings in outstanding potential to business in terms of reaching the users and at the same time it also brings a lot of risk to the business. There are both harmless and harmful users on the Internet. Whereas an organization makes its information system accessible to harmless

Internet users. Malicious users or hackers can also get an access to organization's internal systems in various reasons. These are,

- Software bugs called vulnerabilities in a system.
- Failure in administration security.
- Leaving systems to default configuration.

The intruders are use different types of techniques like Password cracking, peer-to-peer attack, Sniffing attack, Dos attacks, Eavesdropping attack, Application layer attack etc. to exploit the system vulnerabilities mentioned above and compromise critical systems. Therefore, there required to be some kind of security to the private resources of the organization from the Internet as well as from users inside the organization.

Types of intrusion protection systems

There are two types of Intrusion Protection systems. These are internet/network based Intrusion Protection System and host based Intrusion Protection System.

Internet / network Based Intrusion Protection and Prevention System

A Internet/network Based IPS (NIPS) present in a computer or device connected to a segment of an organization's internet/network and monitors internet/network traffic on that internet/network segment, looking for ongoing attacks. In internet/network for maintain security to files many various Hashing algorithms are used like MD5. When a circumstances occurs that the internet/network -based IPS is planned to know an attack, it responds by sending notifications to administrators. NIPS looks for attack patterns within a internet/network traffic, such as large collections of related items that are of a certain type that could specify that a denial-of-service attack is ongoing, or it looks for the exchange of a sequence of related packets in a certain pattern, which could indicate that a port scan is in progress. NIPSs are installed at a specific place in the internet/network (router is one of example) from where it is possible to watch the traffic going in and out of a particular internet/network segment and it can be used as watch the specific host computers on a internet/network segment, or it can be installed to monitor all traffic between the systems that make up an entire internet/network.

Host Based Intrusion Protection System

A Host Based Intrusion Protection System (HIPS) is placed on a particular computer or server, known as the host, and monitors activity only on that system. Host based intrusion Protection systems can be further divided into two categories: signature-based (i.e. misuse Protection) and anomaly based Protection techniques. HIPS monitor the status of key system files and detect when an intruder creates, modifies, or deletes the monitored files. Then the HIPS triggers an alert when one of the following changes occurs: file attributes are changed, new files are created, or existing files are deleted. The main difference between NIPS and HIPS is that the NIPS can access information that is encrypted when traveling through the internet/network.

A. Usefulness of HIPS

HIPS can detect local events on host systems and also detect attacks that may avoid internet/network -based IPS.

HIPS encrypted traffic will have been decrypted and is available for processing.

The use of switched internet/network protocols does not affect a HIPS.

Intrusion protection techniques the two types of IPS Techniques are

Anomaly Based Protection Technique: An anomaly-based intrusion Protection system, is a technique for detecting both internet/network and computer intrusions and misuse by monitoring system activity and classifying it as either normal or anomalous. The classification is based on some rules, rather than patterns or signatures, and attempts to detect any type of malicious activity that falls out of normal system operation. While the signature- based systems can only detect attacks for which a signature has previously been created.

A. Advantages of this anomaly Protection method

The possibility of Protection of novel attacks as intrusions; anomalies are recognized without getting inside their causes and characteristics; less dependence of IPS on operating environment (a compared with attack signature- based systems); ability to detect abuse of user privileges.

B. Signature based intrusion protection: Signature-based IPS refers to the Protection of attacks by looking for specific patterns, such as byte sequences in internet/network traffic, or known malicious instruction sequences used by malware. The terminology is generated by anti- virus software, which refers to these detected patterns as signatures. Even though signature-based IPS can easily detect known attacks, it is impossible to detect new attacks, for which no pattern is available. This technique automatically possess the signature to detect the intruder. Misuse Protection technique is created automatically and the works are more complicated and accurate than manually done. It will Depending on the robustness and seriousness of a signature that is activated within the system, some alarm response or notification should be sent to the right authorities.

Functions of IPS

The IPS consist of four main functions namely, data collection, feature selection, analysis and action,

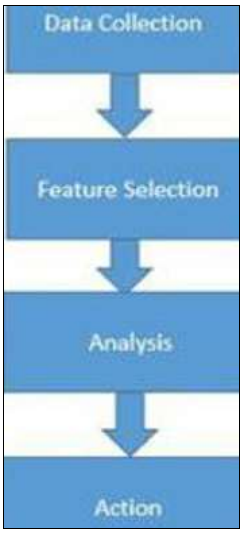


Fig 1: Functionality of IPS

Data collection: This module passes the data as input to IPS. The data is recorded into a file and then analysed. Internet/network based IPS collects and alters the data packets and in host based IPS collects details like usage of the disk and processes of system.

Feature Selection: To select the particular feature large data is available in the internet/network and they are usually evaluated for intrusion. For example, the Internet Protocol (IP) address of the source and destination system, protocol type, header length and size could be taken as a key for intrusion selection.

Analysis: The data is analysed to find the correctness. Rule based IPS analyse the data where the incoming traffic is checked against predefined signature or pattern. Another method is anomaly based IPS where the system behaviour is studied and mathematical models are employed to it.

Action: It defines about the reaction and attack of the system. It can either inform that the system administrator with all the required data through an email/alarm icons or it can play an active part in the system by dropping packets so that it does not enter the system or close the ports.

Components of an intrusion

Protection system: There are three basic components of an IPS - Sensor (Activity or packet capture engine, Behavioural or signature Protection engine), Backend (Event recording of database, alerting the engine) and the Frontend (User interface, Command & control).A sensor forms the primary component of an IPS for detecting intrusions on a computer or a internet/network. It capture a packet to perform Protection activities. It can employ the signature based or anomaly based intrusion Protection techniques. The backend of the IPS is concerned with logging of events which is detected by the sensors. Additionally, it performs the function of alerting. The backend can alert the administrator in frequent ways - logging events in the database, sending an e-mail, block a connection, reset a TCP connection, and display the alert on the administrator's console. The frontend forms the IPS user interface. The user can view events that the sensor has detected, configure the IPS, update the signature database and behavioural Protection engine.

Working of an intrusion

Protection System

The components of an IPS work in a structured manner to alert the administrator of an intrusion.

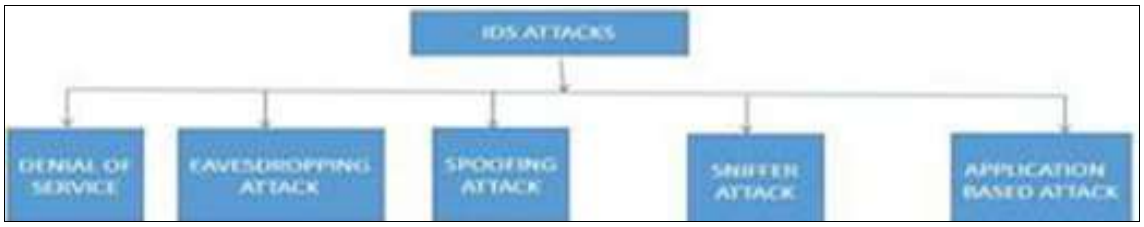
a) **Sensor:** It has two interfaces firstly, the capture internet/network interface and secondly, the management internet/network interface. Its main function is Detect and Report. As the sensor listens to internet/network traffic by tapping into the internet/network, the capture interface passes on all the captured data into a buffer. Then the Protection engine examines the buffer contents and executes internet/network protocol analysis. Signature based and anomaly based intrusion based Protection also happened here.

b) **Backend:** The backend is also termed as the main function of an IPS. Its main function is collect and alert. The events detected by the sensor are recorded in the event repository database system. Then the backend determines how each event has to be responded to E-mails, displays, blocking are used to respond to critical events.

c) **Frontend:** Command and Control the IPS can be setup, configured and updated from the frontend by the user. All events collected by the backend are presented on the frontend. Thus, the frontend provides a convenient interface through which the user can now manage these logged events. To obtain maximum benefit from an IPS, it has to be fined tune to report only significant events. Hence, the user can fine-tune the Protection and response of an IPS through this console. If done with accuracy, the IPS will provides the user with adequately early warning from any intrusion.

Application Based IPS (APIPS)

APIPS will check the functional behaviour and event of the protocol. The system or agent is placed between a process and group of servers that monitors and analyses the application protocol between devices. Intentional attacks are the hostile attacks carried out by malcontent employees to cause harm to the organization and Unintentional attacks causes financial damage to the organization by deleting the important data file. There are numerous attacks have been taken place in OSI layer.



Denial-of-Service (DOS) Attacks: DOS refers to Denial-of- Service and is best defined as an attempt to make a computer(s) or internet/network (s) unavailable to its intended users or also a Denial of Service attack is when an attacker is trying to generate more traffic than you have resources to handle.

DOS and DDOS: In a DOS attack, one computer and one internet connection also is established to overwhelm a server or internet/network with data packets, with the only intention of overloading the bandwidth of victim and available resources. A Distributed Denial of Service (DDOS) attack is the same, but it is amplified. Rather than one computer and one internet connection a DDOS is, and often involves millions of computers all being used in a distributed manner to have the effect of hitting a web site, web application or internet/network offline.

In both cases, either by the DOS or the DDOS attack, the target is bombarded with data requests that have the effect of disabling the functionality of the victim.

SYN Attack: SYN attack is also defined as Synchronization attack. Here, the attacker sends the flood of SYN request to the destination to use the resources of the server and to make the system unresponsive.

Peer-to-peer attacks: A peer-to-peer or P2P internet/network is a distributed internet/network in which individual nodes in the internet/network called "peers" act as both suppliers (Seeds) and consumers (Leeches) of resources, in contrast to the centralized client- server model where the client server or operating system nodes request access to resources provided by central servers.
Ping of Death: A type of DOS attack in which the attacker sends a ping request that is larger than 65,536 bytes, which is the maximum size that IP allows onto the internet/network. While a ping larger than 65,536 bytes is too large to fit in one packet that can be transmitted through, TCP/IP allows a packet to be fragmented, essentially splitting them in smaller segments that are reassembled at the end. Attacks took advantage of this limitation by fragmenting packets that when received packet would total more than the allowed number of bytes and would effectively cause a buffer overload on the operating system at the receiving end then the system could crash.
Eavesdropping Attack: It is the scheme of interference in communication by the attacker. This attack can be done over by telephone lines, instant message or through email.

Identity Spoofing (IP Address Spoofing): Most operating systems and internet/network s use the IP address of a computer to identify a valid entity on the internet/network. In certain cases, it is possible for an IP address to be falsely assumed have spoofing identity. An attacker might also use special programs to construct IP packets that are originate from valid IP addresses inside the corporate intranet. After gaining access to the internet/network with a valid IP address, the attacker can modifying, re- routing, or deleting your data.

Man-in-the-Middle Attack: As the name suggests, a man-in-the-middle attack occurs when someone between you and the person with whom you are communicating is actively monitoring, capturing, and controlling your communication transparently. For example, the attacker can re-route a data exchange. When computers are communicating at lowest levels of the internet/network layer such as physical layer, the computers might not been able to decide with whom they are exchanging the data. Man-in-the-middle attacks are like someone assuming your identity in order to read your message. The person on the other end might believe as it is you because the attacker might be actively replying as you to keep exchanging the information. This attack is capable of the same damage as an application layer attack, which is described below.

Application Layer Attack: An application-layer attack targets the application servers by intentionally causing a fault in a server's OS or applications. This results in the attacker gaining the ability to bypass accessing normal controls. The attacker takes advantages of this situation, gaining control of your application, system, or internet/network, and can do any of the following:
Read, add, delete, or modify your data or operating system.

- Can introduce a virus program that uses your computers and software applications to copy viruses throughout entire internet/network.
- Can introduce a sniffer program to analyze your internet/network and gain information that can be used to crash or to corrupt your systems and internet/network.
- Abnormally terminate your data applications or operating systems and Disable other security controls to enable future attacks.

Sniffer Attack: A sniffer is an application or device that can monitor, read, and capture internet/network data exchanges and read internet/network packets. If the packets are not encrypted, a sniffer provides a full view of the data inside the packet.

Tools of intrusion protection
An intrusion Protection product available today addresses a range of organizational security goals. The security tools.
SNORT: Snort is lightweight and open source software. Snort uses a flexible rule-based language to describe the traffic from an IP address; it records the packet in human readable form through protocol analysis, content searching, and various pre-processors Snort detects thousands of worms, vulnerability exploit attempts, port scans, and other suspicious behaviour.
OSSEC-HIPS: OSSEC (Open source security) is free open source software. It will run on major operating systems and uses a Client/Server based architecture. OSSEC has the ability to send OS logs to the server for analysis and storage the data. It is used in many powerful log analysis engine, ISPs, universities and data centres Authentication logs, firewalls are monitored and analysed by HIPS.
KISMET: It is a guideline for WIPS (Wireless intrusion Protection system).WIPS compromises with packet payload and happenings of WIPS. It will find the burglar access point.

Research of ips tool software name: RAJ IPS
Integrated development environment (IDE): Visual Studio.

2015 Language used: Visual Basic.

Brief Description about the Project
Intrusion Protection System (IPS) defined as a Device or software application which monitors the internet/network or system activities and finds if there is any malicious activity occur.

Need of IPS
Outstanding growth and usage of internet raises concerns about how to communicate and protect the digital information safely. In today's world hackers use different types of attacks for getting the valuable information. Many of the intrusion Protection techniques, methods and algorithms help to detect those several attacks.

Log-Based Intrusion Protection SYSTEM
Log Analysis for intrusion Protection is the process or techniques used to detect attacks on a specific environment using logs as the primary source of information.

Attacks and IPS Types: Types of DoS attack, Volume based attacks Includes UDP floods, ICMP floods and Protocol based attacks Includes SYN floods, fragmented packet attacks, Ping of Death.

Types of IPS

1. **Host based IPS:** Software (agent) installed on computers to monitor input and output data packets from device and it performs log analysis, file integrity checking real time alerting and active response.
2. **Internet / network based IPS:** Connected internet/network segments to monitor, analyse and respond to internet/network traffic and a single IPS sensor can monitor many hosts.

Installing RAJ IPS: Simple and easy we implement RAJ IPS in two models which is.

Two models are

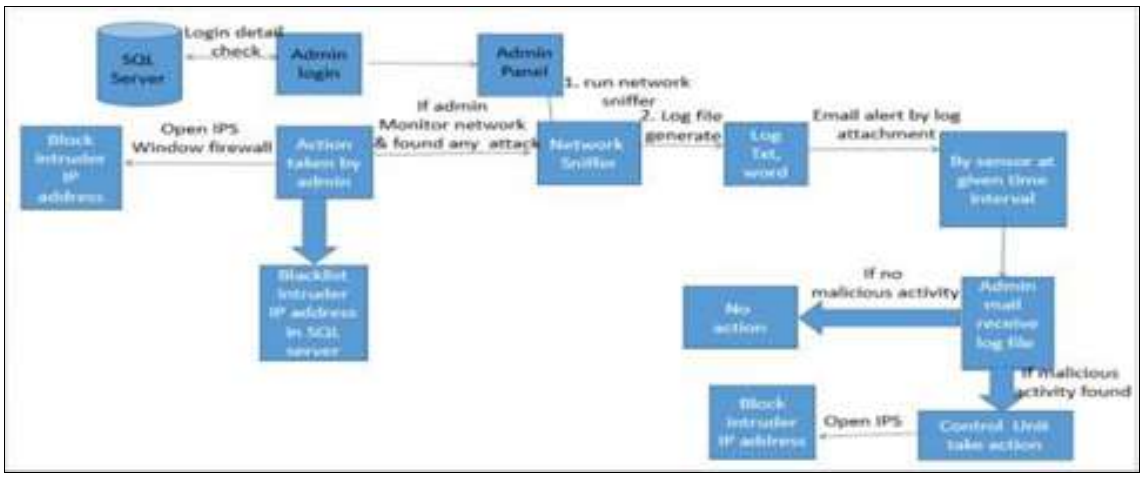
- Local (when you have just one system to monitor).
- Client/Server for centralized analysis (Recommended!).

Functioning of RAJ IPS Tool: Raj IPS is a Host based IPS (intrusion Protection System)/IPS (intrusion prevention System) Tool in which we can monitor input and output data packets or traffic from the device and using this tool administrator also performs log analysis they find the pattern of attack into the logs if any malicious attack pattern found like UDP FLOOD which is the type of Dos Attacks so administrator inform to control unit they will take action against those attack they will block the IP address of intruder and store the intruder information in SQL Server and also trace the intruder IP Address so finally we detect and prevent the intrusion.

Component of RAJ IPS

1. **Internet/network sniffer:** A packet analyzer (also known as a packet sniffer) is a piece of software or hardware designed to intercept data as it is transmitted over a internet/network and decode the data into a format that is readable for humans. As data streams flow across the internet/network, the sniffer captures each packet and, if needed, decodes the packet's raw data, showing the values of various fields in the packet.
2. **Identify intrusion using log based analysis:** Those packets which is received by internet/network sniffer is stored in a log file. These log file are used for analyse the internet/network traffic by the administrator if any malicious activity or attack found in this log file then administrator inform control unit they will take action against those attacks and these log file will be used for forensic purpose in future.
3. **Sensor:** Sensor reports the administrator by sending email with log file and admin analyse those log file and take action if any attack will found so they inform to the control unit and they will take action against those attacks.
4. **Control Unit:** The Control Unit takes action against intruder attack they will block the IP address of the intruder in the firewall of the system and store the information about intruder in SQL server and blacklisting the intruder IP address by using SQL server and also trace the intruder IP address.

RAJ IPS Architecture



Conclusion

IPS are becoming the main part for many organizations after deploying firewall technology at the internet/network perimeter.

IPS can offer protection from external users and internal attackers, where traffic doesn't go past the firewall at all.

However, the following points are must to always keep in mind.

If all of these points are not attached to, an IPS implementation along with a firewall alone cannot make a highly secured infrastructure.

Strong identification and authentication: An IPS uses very good signature analysis mechanisms to detect intrusions or potential misuse; however, organizations must still ensure that they have strong user identification and authentication mechanism in place.

Intrusion Protection Systems are not a solution to all security concerns: IPS perform an excellent job of ensuring that intruder attempts are monitored and reported. In addition, companies must employ a process of system testing, employee education, and development of and attached to a good security policy in order to minimize the intrusions risks.

An IPS is not a substitute for a good security policy: As with good security and monitoring products, an IPS

functions is one element of a corporate security policy. Successful intrusion Protection requires that a well- defined policy must be followed to ensure that vulnerabilities, intrusions and virus outbreaks, etc. are handled according to corporate security policy guidelines.

Human intervention is required: The security administrator or internet/network manager must investigate the attack once. It is detected and reported, determine how it has occurred, correct the problem and take the necessary actions to prevent the occurrences of the same attacks in future that might happen.

Acknowledgement
I would like to express my sincere gratitude to Mr SHIVANK SONI., Assistant Professor, Department of CSE, OIST BHOPAL, M.P. India, for giving me the much needed encouragement to translate my in-depth research into a survey paper.

References

1. Pontarelli S, Bianchi G, Teofili S. Traffic-aware Design of a High Speed FPGA Internet/network Intrusion Protection System. IEEE Transactions on computers; c2012. DOI: 10.1109/TC.2012.105.
2. Kazienko P, Dorosz P. Intrusion Protection Systems (IPS) Part I - (Internet/network intrusions; attack symptoms; IPS tasks; and IPS architecture). [Cited 2024 May 7]. Available from: https://www.windowsecurity.com › Articles & Tutorials.
3. Kumar S. Survey of Current Internet/network Intrusion Protection Techniques. [Cited 2024 May 7]. Available from: http://www.cse.wustl.edu/~jain/cse571-07/ftp/IPS.pdf.
4. Chebrolu S, Abrahama A, Thomas JP. Feature deduction and ensemble design of intrusion Protection systems. Elsevier Ltd. DOI: 10.1016/j.cose.2004.09.008.
5. Aickelin U, Greensmith J, Twycross J. Immune System Approaches to Intrusion Protection - A Review. [Cited 2024 May 7]. Available from: http://eprints.nottingham.ac.uk/619/1/04icaris_IPS review.pdf.
6. Available from: http://www.intechopen.com/download/get/type/pdfs/id/869 5.
7. Roesch M. Snort - Lightweight Intrusion Protection for Internet/network s. © 1999 by The USENIX Association.
8. The Snort Project. Snort User Manual 2.9.5, May 29, 2013. Copyright 1998-2003 Martin Roesch, Copyright 2001-2003 Chris Green, Copyright 2003-2013 Sourcefire, Inc.
9. Chapter 3, Working With Snort Rules. Pearson Education Inc.
10. Daya B. Internet/network Security: History, Importance, and Future. University of Florida Department of Electrical and Computer Engineering; c2013. [Cited 2024 May 7]. Available from: http://web.mit.edu/~bdaya/www/Internet/network%20Security.pdf.
11. CHEN L. Web Security: Theory and Applications. School of Software, Sun Yat-sen University, China.
12. Canavan JE. Fundamentals of Internet/network Security. Artech House Telecommunications Library; 2000.
13. Hamedani ARF. Internet/network Security Issues, Tools for Testing. School of Information Science, Halmstad University; c2010.
14. Khayam SA. Recent Advances in Intrusion Protection. Proceedings of the 26th Annual Computer Security Applications Conference, Saint-Malo, France; c2009. p. 224-243.
15. Pikoulas MMBW. Software Agents and Computer Internet/network Security. Napier University, Scotland, UK.
16. Mahan RE. Introduction to Computer & Internet/network Security. Washington State University; c2000.
17. Gu Q, Liu P. Denial of Service Attacks. Texas State University, San Marcos.
18. Shibli MA. MagicNET: Human Immune System & Internet/network Security. IJCSNS International Journal of Computer Science and Internet/network Security, 2009, 9(1).
19. Eian M. Fragility of the Robust Security Internet/network: 80211. Norwegian University of Science and Technology; c2011.
20. Acemoglu D. Internet/network Security and Contagion. National bureau of economic research; c2013.
21. Xu J, Wang J, Xie S, Chen W, Kim J. Study on Intrusion Protection Policy for Wireless Sensor Internet/network s. International Journal of Security and Its Applications. 2013 Jan;7(1):1-6.
22. Akyildiz I, Su W, Sankarasubramaniam Y, Cayirci E. Wireless Sensor Internet/network s: A Survey. Computer Internet/network s. 2002;38(4):393-422.
23. Martinez K, Hart J, Ong R. Environmental Sensor Internet/network s. IEEE Computer. 2004;37(8):50-56.
24. Abouhogail R. Security Assessment for Key Management in Mobile Ad Hoc Internet/network s. International Journal of Security and Its Applications. 2014;8(1):169-182. DOI: 10.14257/ijsia.2014.8.1.16.
25. Ngai E, Liu J, Lyu M. On the Intruder Protection for Sinkhole Attack in Wireless Sensor Internet/network s. IEEE International Conference on Internet/network s; c2006.
26. Martins D, Guyennet H. Wireless Sensor Internet/network Attacks and Security Mechanisms: A Short Survey. 13th International Conference on Internet/network-Based Information Systems; c2010.
27. Jain M. Wireless Sensor Internet/network s: Security Issues and Challenges. International Journal of Computer and Information Technology. 2011;2(1):62-67.
28. Sethi N, Sharma D. A Novel Method of Image Encryption Using Logistic Mapping. International Journal of Computer Science Engineering, 2012 Nov, 1(2).