Threat Mitigation Strategy in Information System using Intrusion Detection System: A General Classification Reviews

Qamar Rayees Khan
Department of Computer Sciences, BGSB University, Rajouri (J&K)

Muheet Ahmed Butt
Department of Computer Sciences, University of Kashmir, Srinagar

Mohammad Asger
Department of Computer Sciences, BGSB University, Rajouri (J&K)

Majid Zaman
Directorate of IT & SS, University of Kashmir, Srinagar

ABSTRACT
The information security as a term starts its impact when the computers dominated the market. As the computer system becomes more and more affordable security problems and solutions were phrased. Before the mid 1980 till date, the Information Security concerns of any organizations has also increases many fold. Majority of the organizations either big or small are facing an increasing number of threats every day in the form of viruses and attacks etc, that compromise the Integrity of the Information System. Since then many different mechanisms were opted by organizations like intrusion detection to protect their organizations from these kinds of threats/ attacks. In this paper we try to highlight the impact of Threat on the information system and corresponding mitigating strategy like IDS. This paper will mainly focus on classification of Intrusion Detection Systems.

Keywords
Information Security, Threats, Viruses, attacks, Intrusion detection system.

1. INTRODUCTION
Information which is considered as an asset to any organizations does not have the value if it gets compromised by any means. Information/data is stored, processed and transmitted in the system that constitutes information system (IS). The information system is comprised of hardware, software and the human-ware. The nature and the type of the data/information varies form organization to organization. Confidentiality, Integrity, Availability are the three main attributes of the information security. Confidentiality means restricting the unauthorized users from entering into the system, Integrity means protecting the data from any kind of modification, alteration and the Availability means the data should be offered when requested to serve the purpose [1][19]. The components of the information system should be protected from the threats caused by intrusions by applying various security measures. Threat is anything natural or artificial activity that might cause harm to the system and that might infringe the confidentiality, integrity, or availability of any system resources. People using the computer and the allied resources commonly misuse hardware, software, data and other resources [2] that lead to a specific risk. The Risk happens when IS resources are susceptible to threats. The Risk Management in any organization tries to mitigate Threats or tries to minimize their impact. Risk is the combination of both vulnerability and threats. Security professional often depict Risk by using this equation:

Risk (**R**) = Threat (**T**) × Vulnerability (**V**)

In order to reduce the impact of the loss associated with a particular IS Threat, various security countermeasures are adopted [3]. For the clear understanding of the IS Threats, researchers used criminology perception [4] to assemble security approaches into various categories as given in table.1 as under [5]:

Table.1 Security Approaches

S No.	Secuirty Approach	Type
1	Hardware	IT Related
2	Software	IT Related
3	Data Information	IT Related
4	Network	IT Related
5	Physical	Non-IT Related
6	Personnel	Non-IT Related
7	Administrattion (Regulations/Policies)	Non-IT Related

A Threat Model was developed with the intention that the Threats can occur within or outside the organisations. The perpetrators in this model will be either human or anything else and the activities may be deliberate or unintentional and the result is the compromise of security goals (CIA) [6].

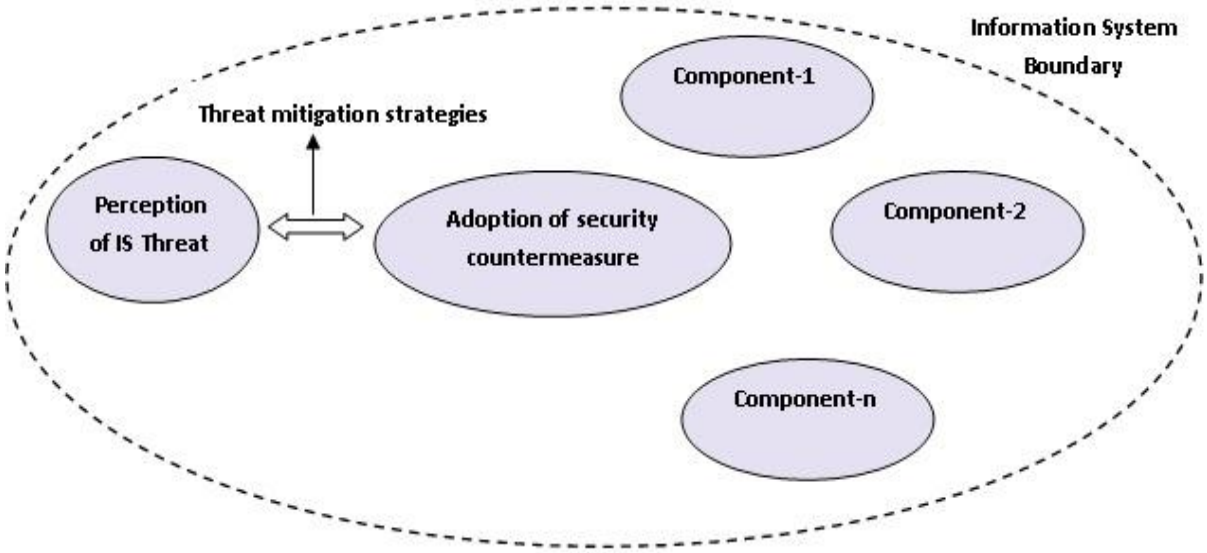

Fig 1: Information System & IS Threat Management

As depicted in the fig-1 above, the implementation of the requisite security countermeasure includes all the IT related efforts like Hardware, Software, Data, Network and Non-IT efforts like physical, personnel[11][12][13][14][15]. A successful IS security adopted by any organization should safeguard the IS and the allied resources against illegal use or alteration of information, that may be in storage or in processing or in transit, and against the DoS to illegal users [7][17][18]. The deterrent efforts in mitigation the IT Threats include installation of advanced security software like Firewall, Intrusion Detection System, Surveillance mechanism and the creation of exception documents [8].

2. INTRUSION DETECTION SYSTEM (IDS)

Intrusion is a malicious agent that may cause damage/threat to the Information System resources. Intrusions when break into the system compromises the Confidentiality, Integrity and Availability of the IS resources. The cause and effect of an intrusion on the IS resources may vary depending on the type of the intrusion. In order to mitigate the extent of damage caused by the intrusions, several Intrusion Detection Systems (IDS) have been developed from time to time. Intrusion detection (ID) is a process/procedure of detecting an intrusion. The IDS has its history in 1990 when it became available in the market [9]. The working of IDS is simply like an burglar alarm as it alarms when it detects something unusual i.e. intrusion. The nature of the alarm may be visual/audible or silent depend on the working environment. A typical IDS performs the following tasks as in Figure-2.

Pre-processing is the first phase of the IDS where data is organised in a specific pattern for classification. This phase collects the activity from the IDs. Next is the analysis phase wherein the data record is matched with the Knowledge base. The data record after analysis shall be either as an intrusion or normal data. Next is the response phase wherein we get an alert after analysing that data is either as an intrusion or normal data. The response of the attack shall be automatically or manually configured. Last but not least is the refinement phase wherein fine tunings is done. It updates based on the previously identified intrusions [10].

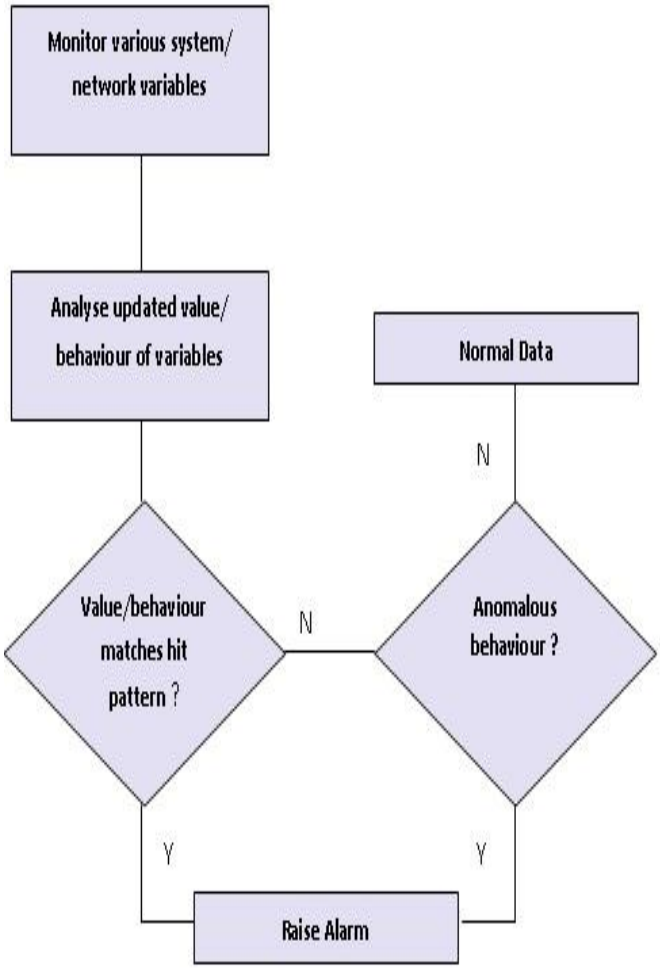

Fig 2: Working of a typical IDS

3. CLASSIFICATION OF IDS

For the clear understanding, comparing and contrasting the various IDS, Classification of IDS play a major role [10]. We try to classify the IDS by way of two patterns:

3.1 Pattern-1

In this pattern, the classification is based on the place where ID systems can be placed. It is further classified into three subclasses.

- Host Based IDS.
- Network Based IDS.
- Hybrid Based IDS

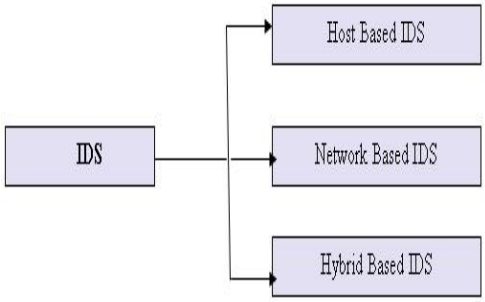

Fig 3: Classification based on Deployment

3.2 Pattern-1I

In this pattern, the classification is based on analysis of the technique that is used. It is further classified into three subclasses.

- Mis-use Based IDS
- Signature Based IDS
- Anomaly Based IDS.

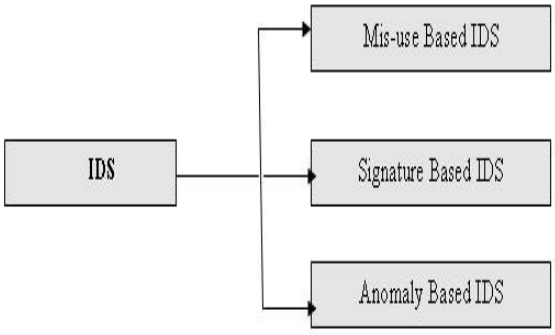

Fig 4: Classification based on Analysis of Technique

The Signature Based IDS is itself classified into various categories:

- Expert system IDS
- Signature Analysis IDS
- Petri Nets IDS
- State Transition IDS

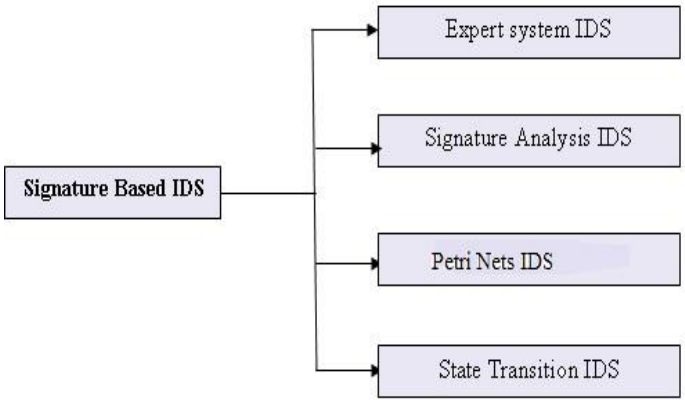

Fig 5: Signature Based IDS Classification

The various types of sub categories which come under Anomaly IDS are as:

- Statistical Based
- Expert system
- Neural Networks
- Computer immunology
- User Intention Identification System.
- Data Mining

In this classification various techniques are being used/implemented to combat with the intrusions and their allied impact. Techniques like statistical based, neural network algorithms [16], immunology and the data mining techniques etc, are used.

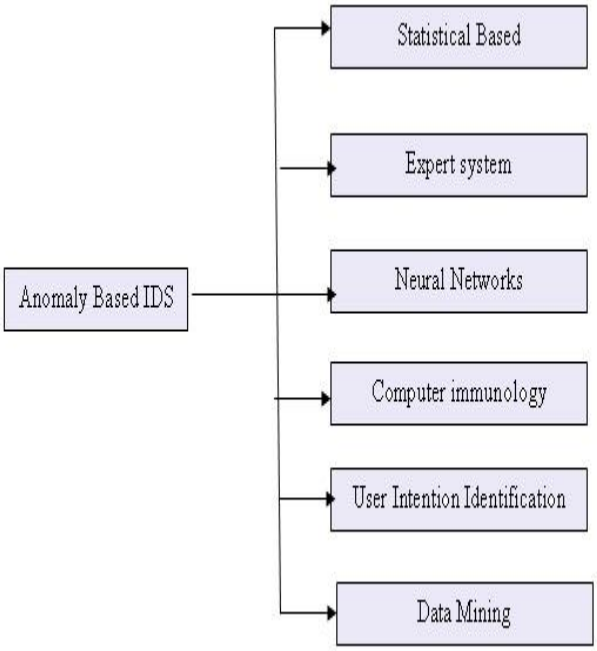

Fig 6: Anomaly Based IDS Classification

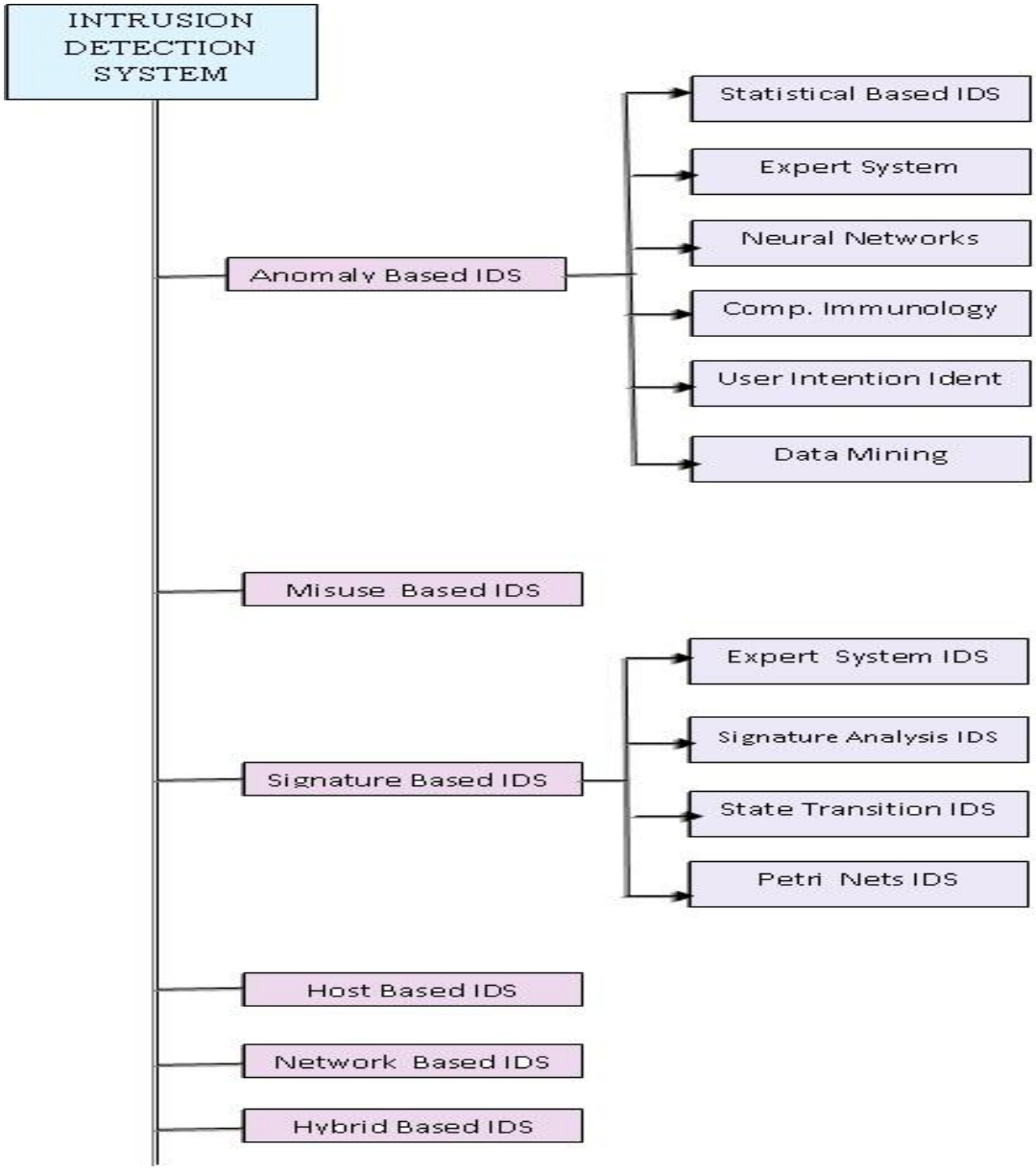

Fig-7: A Big Picture of IDS Classification

4. IDS USING DATA MINING

In figure-6,7above, Data mining (DM) is a pattern discovery and play a significant role in IDS. The following data mining methods are often used to get the information about intrusions by examining the system/network data [11].

4.1 Classification

It is a learning technique that is supervised. This type of IDS based on Classification categorizes all the system/network traffic into either normal or abnormal. This technique is predominantly used for anomaly detection. The steps in classification process are as under:

a) It accepts the dataset as input.

b) Maps the data items into specified groups or classes.

c) Classifier predicts a class which a new item belongs.

4.2 Association Rule

This technique is used to search an item set which is repeatedly occurring from a huge dataset. The steps in mining of association rule are as under:

a) Frequent Item set Generation: It generates all such collection of items whose support value is greater than the particular threshold.

b) Association Rule Generation: on the basis of frequent item sets generated as in (a) above, it generates the perquisite rules of the form "if then".

4.3 Clustering

It is a learning technique that is unsupervised. It discovers patterns in unlabelled data. This technique labels the data and assigns the same into clusters. A particular cluster consists of members that share the common properties. Members that belong to a different cluster are different from each other. This technique can be useful for categorizing network data and correspondingly detecting intrusions. Clustering

technique can be used on Anomaly detection as well as on Misuse detection.

5. CONCLUSION

Intrusions pose a great threat to the Information System assets. Various Information Technology threat mitigation strategies are in place to countermeasure the perceived threats. Out of the various countermeasures, Intrusion Detection finds its place to protect the IS from the allied threats and attacks that compromise the integrity of the data/information. Intrusion detection is still a fledging field of research. This field is still in infancy mode. In this paper, we tried to highlight various categories of intrusion detection so that we will get a better idea about each and every class of intrusion detection. In future research work, we will try to highlight prime design characteristics (via guidelines) for selecting a particular type of Intrusion detection System (IDS) according to your organization need.

6. RERERENCES

[1] Michael E. Whitman, Herbert J. Mattord.(2012), Principles of Information Security, CENGAGE Learning, fourth edition.

[2] D.W. Straub, W.D. Nance.(1990), Discovering and disciplining computer abuse in organization: a field study, MIS Quarterly ,pp. 45–55.

[3] T.R. Peltier.(2001), Information Security Risk Analysis, Auerbach,New York.

[4] D. Icove, K. Seger, W. Vonstorch, Computer Crime. (1999), A Crimefighter's Handbook, O'Reilly & Associates, Inc.

[5] Quey-Jen Yeh a,*, Arthur Jung-Ting Chang. (2007), Threats and countermeasures for information system security: A cross-industry study, Elsevier, Information & Management 44, pp- 480–491.

[6] K.D. Loch, H.H. Carr, M.E. Warkentin. (1992), Threats to information systems: today's reality, yesterday's understanding, MIS Quarterly 16 (2), pp. 173–186.

[7] CNSS, National Information Assurance (IA) Glossary (CNSS Instruction No. 4009), Committee on National Security Systems, revised in June 2006, http://www.cnss.gov/instructions.html, (cited July 5, 2006).

[8] A. Kankanhalli, H.H. Teo, B.C.Y. Tan, K.K. Wei. (2003), An integrative study of information systems security effectiveness, International Journal of Information Management, pp. 139–154.

[9] Bernard Menezes (2011) , Network Security and Cryptography, CENGAGE Learning.

[10] Beigh, B. M., & Peer, M. A. (2012). Intrusion Detection and Prevention System: Classification and Quick, ARPN Journal of Science and Technology, VOL. 2, NO. 7, ISSN 2225-7217.

[11] Mitchell D'silva, Deepali Vora.(2013), Comparative Study of Data Mining Techniques to Enhance Intrusion Detection, Inter. Jour. of Engineering Research and Applications (IJERA), Vol. 3, Issue 1 , pp.1267-1275 , ISSN: 2248-9622.

[12] Butt, Muheet Ahmed, and Majid Zaman. "Assessment Model based Data Warehouse: A Qualitative Approach." International Journal of Computer Applications 62.10 (2013).

[13] Butt, Muheet Ahmed, and Majid Zaman. "Assessment Model based Data Warehouse: A Qualitative Approach." International Journal of Computer Applications 62.10 (2013).

[14] Zaman, Majid, and Muheet Ahmed Butt. "Enterprise Data Backup & Recovery: A Generic Approach." International Organization of Scientific Research Journal of Engineering (IOSRJEN) (2013): 2278-4721.

[15] MaqboolRao, Nouman, et al. "Distributed Data Warehouse Architecture: An Efficient Priority Allocation Mechanism for Query Formulation."

[16] Butt, Muheet Ahmed. "COGNITIVE RADIO NETWORK: SECURITY ENHANCEMENTS." Journal of Global Research in Computer Science 4.2 (2013): 36-41.

[17] Butt, M. A., and M. Zaman. "Data Quality Tools for Data Warehousing: Enterprise Case Study." IOSR Journal of Engineering 3.1 (2013): 75-76.

[18] Khan, Sajad Mohammad, Muheet Ahmed Butt, and Majid Zaman Baba. "Information Communication Technology: Practices for Academia."