Integrity Model based Intrusion Detection System: A Practical Approach

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
Directoriate of IT & SS, University of Kashmir, Srinagar

ABSTRACT

Information is considered to be an asset for any organizations. Malicious attacks/threats can compromise the security and trust of a system, which shall be controlled by introducing Intrusion Detection System. In order to offer maximum security for the confidential data and the corresponding data integrity, a novel Integrity model based Intrusion Detection system is proposed. Hence, the optimum Integrity is increased by increasing the intrinsic attributes of Information System like accuracy, consistency and reliability. The proposed research paper tries to propose a model for improving the optimum information Integrity by quantifying the intrinsic integrity attributes so that the data may not get compromised.

Keywords

DBMS; Malicious attacks; Threats; Intrusion Detection System; Data Integrity

1. INTRODUCTION

Information security is a wide term which means protecting the information and the allied information system from illegal access, disclosure, use, modification, disruption, scrutiny, recording or damage. Security of information ensures the guarantee that information threats and the corresponding controls are in proper stability (Anderson, J. M. (2003)).Security of the information resources must include safeguards and controls and to counterbalance possible attacks/threats as well as controls to guarantee the timeliness, availability, integrity, confidentiality, etc [23]. The terms like computer security, information security, and information guarantee are the most common terms that are used in the said context. These fields are related to one another and tend to share the usual objectives of shielding the three triads of the information i.e. confidentiality(C), integrity(I) and availability(A).

The information may take any form like electronic, print, or other forms and the allied security is concerned with the above three triads of information i.e. CIA . The term Confidentiality is used to prevent the information from the exposure to unauthorized individuals. Integrity means that the data cannot be modified unnoticeably. Any type of Information System (IS) that serves the requisite purpose and the type of information that the user requests must be accessible when user is in need. The IS that stores and processes the data/information and the corresponding controls to check and safeguard the system and the channels used should be altogether operationally accurate.

In figure-1 below, the outer oval represents the information and the other small circles present inside the main large circle represent the traits of the information quality [24]. The inner central circle represents integrity and signifies its importance. Integrity, which is considered as one of the elementary property of the security of the information, is a huge research area. We refer to the various Information Security tutorials and the allied textbooks that examine the mixed flavor of integrity.

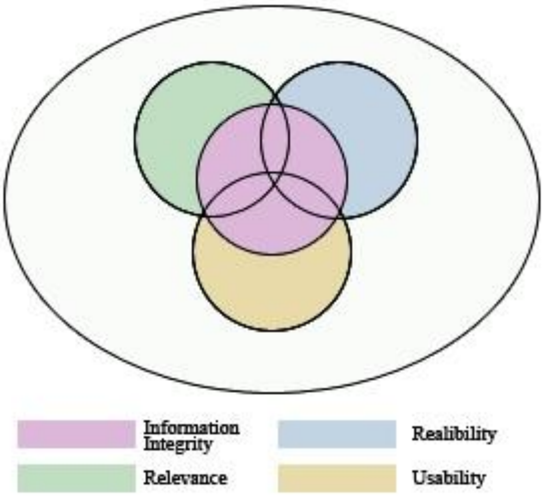

Fig 1: Influence of Information Integrity

Information-flow integrity has its history way back by the integrity model of Biba's (D. E. Bell and L. J. LaPadula), which complements Bell and LaPadula's model (L. J. LaPadula and D. E. Bell) for mandatory access control. The IS if compromised by any type of attack/vulnerability leads to the threat that effects the properties of the information and the corresponding IS. In IS, a threat can be artificial or it can be natural that has the likelihood to cause damage. In the framework of information and the corresponding security mechanism, the blow of the vulnerability/ threat is a compromise of availability(A), integrity(I), and confidentiality(C) (K.D. Loch, H.H. Carr and M.E. Warkentin).

The integrity as a parameter of security did not receive much attention within the researchers worldwide. Out of the three triads of the information, confidentiality has been analysed and examined by way of its two important properties (Khan, Q.R,Butt,M, Zaman, M, Asger (2013)). Information security in any organization has become one of the most important concerns of any information systems. Thus, the information system(IS) that serves the organization needs must ensure that their assets are properly protected from any security lapse. To develop a secure information system, the first step is to identify threats. Once potential threats are known, the nest step shall be establishing controls finally, the third step is to examine / discover any breach of security. According to various researchers efforts of preventing the information system from the threats include deploying state of art access controls, intrusion detection system (IDS), and the allied security mechanisms. An intrusion is a malicious agent that enters into the information system and compromises the system in terms of Confidentiality, Integrity, and Availability. Intrusion when break out into the system would cause loss of integrity, Confidentiality etc., and results in unauthorized alterations of users system files/users information. In order to protect the information and the corresponding system from these threats being triggered by the intrusions, various IDS have been proposed by the researchers using data mining. Most of the IDS does not focus on the information integrity, it is due to this reason that we target on this vital issue.

2. INTRUSION DETECTION USING DATA MINING

Intrusion detection (ID) as the term includes classification and recognition of malicious activities/threats that leads to the loss of integrity(I), confidentially(C) and availability(A) of the data assets. A conventional ID technique like signature based ID was exclusively used to identify the attacks that are known. In this technique, event is being matched with the signature to identify invasion as they dig out the characteristics from the various review streams and match the same with the signatures hit by the intrusion as made available by the specialists. The attack signatures are maintained in the database. The database is to be updated manually so that any latest form of intrusions is revealed. The bottleneck of this technique is that it is unable to identify any new intrusion.

Many rule-based IDS show capabilities that highly depend on the rules recognised by security specialist. To solve the above restrictions, a number of IDSs based data mining techniques are implemented.

Data Mining (DM) is simply a pattern discovery[18][19][20][21][22]. In order to find a normal or abnormalities in huge data sets, various softwares like Weka, matlab, etc are applied. In order to contribute in Intrusion detection, data mining must serve the following:

- Eliminate the normal action from abnormal data so that the expert emphasis on actual attacks.
- Next is to recognise the fake alarm entity as well as abnormal signature.
- Discover abnormal action that exposes an actual hit.

In order to achieve the above tasks, various data mining techniques are used like Data summarization,Visualization,,Clustering [Manganaris et al., 2000],Association rule discovery,[Clifton and Gengo, 2000; Barbara et al., 2001],Classification [Lee and Stolfo, 1998]. Data mining is used as a tool for detecting intrusions. DM based intrusion detection techniques (IDT) generally falls under various categories:

2.1 Misuse Detection (MD)

This technique is based on patterns and signatures of already known attacks. A constantly updated database signatures of known attacks is used to match the pattern. In this technique, each occurrence is categorized as either ‘normal’ or ‘abnormal/intrusions’ and the requisite categorized data is used to train the algorithm. This technique automatically retrains ID models on various input data. The merit of using MD technique is achieving high level of accuracy in detecting known attacks. The setback of this technique is the incapability of detecting new attacks that are not yet observed.

2.2 Anomaly Detection (AD)

Anomaly Detection (AD) technique detects the deviations from the normal behaviour. It constructs models of ordinary actions and automatically identifies the deviations and labels the same as threat. The limitation of this technique is that of its false alarm rate (RFA). The behaviour of the various unnoticed Information system may be treated as suspect/anomalies and classify it as potential threat.

Many techniques have been put forward by the various researchers for the design of IDSs. For example, Bridges and R.B. Vaughn (M. Moorthy and Dr. S. Sathiyabama(2005)) put forward IDS that join both the misuse and the anomaly IDS. Also the various Clustering techniques can be of much useful for detecting intrusions from the network data (KapilWankhade and SadiaPatka(2010). These Data mining systems are able to generalize new and unknown attacks that leads to the compromise (M. Moorthy, Dr. S. Sathiyabama) (2012)).

3. RELATED WORK

Several ID systems/techniques were suggested by the researchers for Intrusion Detection and a few of them are listed below:

Table1. Contribution & Literature survey

Authors/Researchers	Contribution/s
Weiming Hu et al. (Weiming Hu, Jun Gao, Yanguo Wang, Ou Wu, and Stephen Maybank(2014))	Have put forward two online Adaboost-based ID algorithms
Carol J Fung et al.(Carol J Fung and Jie Zhang)(2012)	Put forward a distributed Host-based IDS (HIDS)
QuanyanZhuet al.(Quanyan Zhu, Carol Fung, RaoufBoutaba, Tamer Basar(2012))	Have outlineed an IDN system, called GUIDEX
Min Wei and Keecheon Kim(Min Wei and Keecheon Kim(2012))	Have put forward an IDS for WIA-PA networks
Francisco Maciá-Pérez, J. Mora-Gimeno(2011)	Suggested an IDS (NIDS) implanted in a smart sensor stimulated device
Zhenwei Yu et al. (Zhenwei Yu, Jeffrey J. P. Tsai, and Thomas Weigert(2007))	Put forward an automatic tunning IDS (ATIDS)

4. PROPOSED MODEL

In order to offer maximum security for the confidential data and the corresponding information system, a novel Integrity model based Intrusion Detection system is proposed as depicted in Figure-7 below. Hence, the optimum Integrity is increased by the increase of its intrinsic traits of accuracy, consistency and reliability. The proposed model tries to implement the methods to improve the optimum Integrity in Information System by quantifying intrinsic integrity traits of accuracy, consistency and reliability so that the data may not get compromised. The steps are as follows:

a) Primarily, a dataset is given as the input for this ID model.

b) Next is clustering, which improve the quality of the datasets by reducing the quantity in a cluster.

c) Next phase is Mining and is performed on the clustered datasets as in step b, the results so produced from the dataset is followed by the optimization in mining process.

d) After obtaining the desired optimized mined results, the next phase Classification is to be carried out by using the requisite classifier. Classification of Intrusion or Non-Intrusion is carried out in this phase.

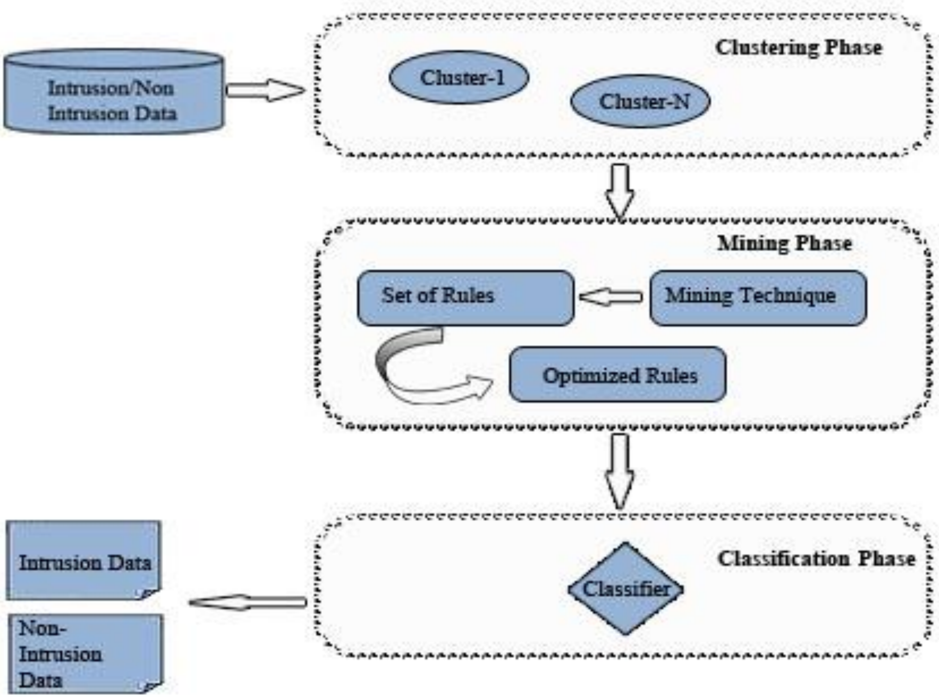

Fig. 2: Proposed Intrusion Detection Model

e) Our proposed ID Model is supposed to be implemented using Matlab with the requisite techniques which effectively identify the Intrusion data from the datasets.

f) The results so generated from the above experiment and the corresponding performance assessment results are analysed.

g) An assessment metrics is created and is used to assess the efficiency of proposed ID model for its effective detection mechanism of Intrusion data in the dataset.

h) The performance of the proposed model is analyzed by nine metric parameters as: Rate of Detection (DR), Rate of False Alarm (FAR), Sensitivity, Accuracy, Consistency Error, Reliability, Rate of False Positive (FPR) and Rate of False Negative (FNR).

i) Finally, our proposed work shall be compared with other existing ID Systems/techniques for better results so that the integrity of the information & the allied information system may not get compromised.

5. CONCLUSION

This paper gives an overview of the Information Integrity and the threats that may cause harm to the information system. Various existing Intrusion detection techniques have also been analysed. To provide an optimum security to the IS from threats/intrusions, a practical approach of a novel model of Intrusion Detection is proposed. The proposed model tries to improve the optimum Integrity in Information System by quantifying intrinsic integrity attributes of accuracy, consistency and reliability so that the data may not get compromised. We hope that our model will be helpful for the future researchers to make the research over Intrusion Detection by taking into account the integrity of the information and the corresponding information system.

6. REFERENCES

[1] Anderson, J. M. (2003). “Why We Need a New Definition of Information Security,” Computers & Security (22)4, p. 308-313.

[2] Carol J Fung, Jie Zhang.(1973). "Effective Acquaintance Management based on Bayesian Learning for Distributed Intrusion Detection Networks", In Proceeding of IEEE Transactions on Network and

Service Management, Vol. 9, No. 3,pp. 320-332, September 2012.

[3] D. E. Bell and L. J. LaPadula(1973). Secure computer systems: Mathematical foundations. Technical Report MTR-2547, Vol. 1, MITRE Corp., Bedford, MA, 1973.

[4] Francisco Maciá-Pérez, J. Mora-Gimeno,(2011). "Network Intrusion Detection System Embeddedon a Smart Sensor", In Proceeding of IEEE Transactions on Industrial Electronics, Vol. 58, No. 3,p. 722-732, Mar 2011.

[5] FenyeBao, Ing-Ray Chen, MoonJeong Chang, and Jin-Hee Cho,(2012). "Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection", In Proceeding of IEEE Transactions on Network and Service Management, Vol. 9, No. 2, p. 169-183, June 2012.

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

[7] KapilWankhade, SadiaPatka,(2010). "An Efficient Approach for Intrusion Detection Using Data Mining Methods", in International Conference on Information Retrival& Knowledge Management, p.. 200-103, Mar 2010.

[8] Khan, Q.R, Butt,M, Zaman, M, Asger, M,(2013). "A Novel Approach Based Information Integrity Modeling", Inter. Jour. of Engineering Science and Innovative Technology (IJESIT) , Volume 2, Issue 1, January 2013 ,p. 210-215.

[9] J. LaPadula and D. E. Bell., (1996).Secure computer systems: A mathematical model. Technical Report MTR-2547, Vol. 2, MITRE Corp., Bedford, MA, 1973. Reprinted in J. of Computer Security, vol. 4, no. 2–3, p. 239–263, 1996.

[10] Moorthy, Dr. S. Sathiyabama ,(2012). "A Study of Intrusion Detection using Data Mining", In Proceeding of IEEE-International Conference on Advances In Engineering, Science and Management (ICAESM -2012), p. 8-15, March 2012.

[11] Min Wei and Keecheon Kim, (2012)."Intrusion Detection Scheme Using Traffic Prediction forWireless Industrial Networks", in Journal of Communications and Networks, Vol. 14, No. 3, p. 310-318, June 2012.

[12] Quanyan Zhu, Carol Fung, RaoufBoutaba, Tamer Basar,(2012). "GUIDEX: A Game- Theoretic Incentive-Based Mechanism for Intrusion Detection Networks",in IEEE Journal on Selected Areas In Communications, Vol. 30, No. 11, p. 2220-2230, Dec 2012.

[13] Weiming Hu, Jun Gao, Yanguo Wang, Ou Wu, and Stephen Maybank,(2014). "Online Adaboost-Based Parameterized Methods for Dynamic Distributed Network Intrusion Detection", In Proceeding of IEEE Transactions on Cybernetics, Vol. 44, No. 1, p. 66-82, Jan 2014.

[14] Zhenwei Yu, Jeffrey J. P. Tsai, and Thomas Weigert,(2007). "An Automatically Tuning Intrusion Detection System", in IEEE Transactions on Systems, Man, and Cybernetics - Part B: Cybernetics, Vol. 37, No. 2, p. 373-384, April 2007.

[15] Barbara, D., N. Wu, and S. Jajodia [2001]. "Detecting Novel Network Intrusions Using Bayes Estimators", Proceedings Of the First SIAM Int. Conference on Data Mining, (SDM 2001),Chicago, IL.

[16] Manganaris, S., M. Christensen, D. Zerkle, and K. Hermiz [2000]. "A data mining analysis Of RTID alarms", Computer Networks, 34, p. 571-577.

[17] Clifton, C., and G. Gengo [2000]. "Developing Custom Intrusion Detection Filters Using Data Mining", 2000 Military Communications International, Los Angeles, California, October 22-25.

[18] Lee, W., and S. Stolfo [1998]. "Data Mining Approaches for Intrusion Detection", in Proceedings of the 7th USENIX Security Symposium, San Antonio, TX.

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

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

[21] 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.

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

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

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

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

[26] Khan, Qamar Rayees, et al. "Review of Intrusion and Anomaly Detection Techniques." International Journal of Modern Engineering Research (IJMER), Volume 4.