RESEARCH ARTICLE OPEN ACCESS

Data Mining approach for IDS in Cloud Environment-Challenges and Opportunities

Gopala B[1], M Hanumanthappa[2]

1 Department of Computer Science and Applications, Bangalore University,Bangalore. India.
2 Department of Computer Science and Applications, Bangalore University,Bangalore. India.

Abstract:

Smart devices are becoming most important communication tool for people across the world. However it also becoming target for security threats and attack. A cloud based IDS can be used to overcome the issues of resource constraints, misbehavior or anomalous activity in smart devices effectively. Cloud computing has become a great enable of cross platform applications for smart devices. It provides the data to be stored in remote servers and delivered over a network. An intrusion Detection system is a common security tool used to increase the level of security in cloud computing using data mining approaches. Data mining based Intrusion Detection system demonstrated high accuracy and good generalization of intrusions in changing environment. Cloud computing provides flexible and pay-per use based services to users. This paper provides a survey on improving Intrusion Detection system for the cloud environment.

Keywords— **Intrusion Detection, cloud computing, Data mining,Data slicing.**

I. INTRODUCTION

An intrusion detection system is a device or an application software that checks network or system activities for harmful activities or rule violations and sends reports to the administrator. The aim of intrusion detection is to identify security deviations in information systems. Intrusion detection is a reactive approach to security as it checks information systems and raises alarms when security violations are recognized. Examples of security violations include the abuse of privileges or the use of attacks to exploit software or protocol vulnerabilities. Traditionally, intrusion detection techniques are classified into misuse detection and anomaly detection categories. Misuse detection works by searching for the patterns of known attacks. Anomaly detection uses a model of normal user or system performance and indicates significant deviations from this replica as potentially malicious.

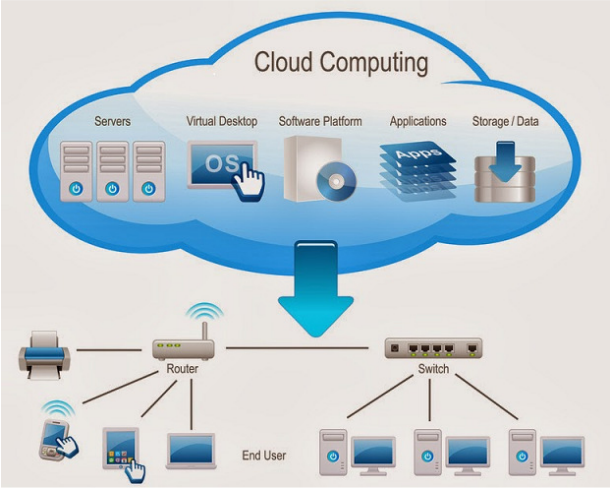
Data Mining is a Knowledge Discovery in Databases(KDD), refers to the nontrivial extraction of implicit, previously unknown and potentially useful information from data in databases. Data mining finds valuable information hidden in large databases. Data mining is the process of analyzing data and the use of software techniques for finding patterns and consistencies in sets of data. The computer is responsible for finding the patterns by identifying the underlying rules and features in the data.

Cloud computing is network based computing, in which shared resources, data and information are provided to computers on-demand. It is a model for enabling ever-present, on-demand access to a shared pool of configurable computing elements. Cloud computing and storage solutions provide users and enterprises with various competences to store and process their data in third-party data canters.

2. APPLICATIONS OF DATA MINING AND CLOUD COMPUTING IN INTRUSION DETECTION SYSTEM

In this modern world Intruders cleverly use the modified versions of command and thereby erasing their footprints in audit and log files. Successful IDS intellectually differentiate both intrusive and nonintrusive records. Most of the existing systems have security breaches that make them easily attackable. The substantial research on intrusion detection technology which is still considered as immature and not a perfect tool against intrusion. The IDS based data mining can efficiently identify user data and predicts the results that can be utilized in the future. Data mining in databases has gained a great deal of attention in IT industry and in the society. Data mining has been involved to analyze the useful information from large volumes of noisy, fuzzy and dynamic data. The IDS can use Data mining techniques for analysing captured packet and classifying according to their severity measures. The administrator receives the alarms to handle the situation in advance based on the state of the data. Cloud based IDS (CIDS) has a scalable and elastic architecture. There is no single point of failure architecture distributes the processing load at different cloud locations and separates the user tasks from the cloud by executing them in a multiple nodes. To increase attack indemnity, CIDS synthesizes knowledge techniques and behaviour based ones. It collects events and audits from nodes so that the detector and correlated components can analyze them. Furthermore, to take into account the huge amount of data in a cloud that prevents administrators from observing any action, a further CIDS component parses and encapsulates a highly intensive number of alerts from a NIDS component in a physical or virtual switch inside the cloud virtual network. The IDS detectors installed in the cloud system provides alert messages to the administrators. CIDS located inside the cloud middleware which provides a similar environment for accessing all nodes. The middleware sets the access control protocols and supports a service-oriented environment. Since the middleware can be installed inside different grid and cloud systems, CIDS can be applied to several Grid and cloud systems.

3. Architecture of Cloud computing



Cloud computing architecture includes fat client, thin client, mobile device as front end platforms and servers, storage, a cloud based delivery, and a network as backend platforms. The client platforms are servers, fat clients, thin clients, zero clients, tablets and mobile devices. These client platforms interact with the cloud data storage through an application, through a web browser, or through a virtual session.

In online network data is stored and accessible to multiple clients. Cloud storage is deployed in the public cloud, private cloud, community cloud, or in hybrid cloud. In order to be effective, the cloud storage needs to be agile, flexible, scalable, multi-tenancy, and secure.

4. Challenges in cloud based Intrusion Detection system

In 2015 the authors Hui-Hao Chou et al., worked on "An Adaptive Network Intrusion Detection Approach for the Cloud Environment". Adaptive network-based IDS which is composed by three parts: a preprocessor, an analyser, and a detector. The detector is constructed based on the decision tree algorithm to carry out anomaly detection on

network connection records. The open source software Bro is used to transform the audited data from raw packets into connection records in the pre-processor. The spectral clustering algorithm used to cluster the collected connection records and to label the clustered result. The results for the DARPA 2000data set and the KDD Cup 1999 data set show a significant progress on the detection rate while keeps the false positive rate reasonable low. The DOS attacks and some probing attacks that create a great amount of connections cannot be detected. Besides, the amount of network connection data is usually very large, which makes the spectral clustering algorithm time and space consuming when computing Eigen values and eigenvectors.

In 2015 the authors Hamid Reza and Roya Salek worked on "Toward a policy based Distributed Intrusion Detection System in cloud computing using Data mining Approaches". They analysed on improving Intrusion Detection System efficiency on cloud computing using data mining methods based on CIA model and grouping similar user and security requirements for improving IDS efficiency. The results are simulated using CART and Bayesian network classifier indicates that the proposed approach is able to reduce processing time by 21 percent in average.

In 2015 the authors Anthony Califano et al., worked on "Using Features of Cloud Computing to Defend Smart Grid against DDoS Attacks". They discussed the risks and opportunities that Cloud computing presents to energy suppliers and utility companies, and consider what inherent attributes of Cloud computing may be able to be leveraged to improve Distributed Denial of Service (DDoS) defence for Smart Grid. An extended literature review is performed to determine which DDoS defence techniques can be enhanced by Cloud computing and utilized to defend the SG. The authors proposed that, when risks are properly mitigated, the deployment of Cloud computing can be seen as an overall benefit, where its inherent attributes can be harnessed to make the SG more secure and help mitigate the threat of a crippling DDoS attack.

In 2015 the authors Rupesh R Bobde et al., worked on "An approach for securing data on cloud using Data slicing and Cryptography". The authors proposed a scheme of slicing data into different slices, the data in each slice can be encrypted using different cryptographic algorithms and encryption key for storing in cloud. The objective of the authors is to store data in proper secure and safe manner to prevent from intrusions with reducing cost and time to store encrypted data in the cloud.

In 2014 the authors Chetna Vaid and Harsh K Verma worked on Anomaly based IDS implementation in Cloud Environment using BOAT Algorithm. It tackles the protection of the user's data for enterprises in terms of security with intrusion detection while adopting cloud computing. It identifies a security technique to mitigate security threats in cloud computing. The intrusion detection is processed on the basis of anomaly detection on the generated data from the transactions collected within the cloud network. The data collected will be processed intense data mining using clustering and classified using BOAT algorithm to identify the intruders on the cloud.

In 2014 the authors manoj kumar et al., work on "Unsupervised outlier Detection Technique for Intrusion Detection in cloud computing". They proposed a density based outlier detection for intrusion detection in cloud computing environment. This technique used for accurate attack detection without previous knowledge. They implemented DenOD on IDCC framework. The authors also analysed that the concept can be implemented on real time environment.

In 2013 the authors Jain pratik and Madhu worked on "Data mining based CIDS: cloud Intrusion Detection System for Masquerade Attacks". They presented a CIDS for CIDD data set in detecting more instances of attacks and masquerades in CIDD. They worked on data warehousing, ETL and intrusion database also on database centric IDS, which offers integration of individual components, security and high availability and provides a good GUI for the users to work with network.

In 2013, the authors Yasir Mehmood and Umme Habibe worked on "Intrusion Detection system in cloud computing: challenges and opportunities. They analysed the existing cloud based IDS with respect to type, positioning, detection time, detection techniques, data source and attacks. They analysed various detection mechanisms like signature based, anomaly based and soft computing techniques to achieve the desired level of security in cloud.

In 2013 the authors Luigi Coppolino, Salvatore, Alessia and Romano worked on "Applying Data Mining Techniques to Intrusion Detection in Wireless sensor Networks". They proposed a hybrid distributed IDS for wireless sensor networks. It is composed of a central agent with number of local agents for accurate intrusion detection using data mining techniques. Decision trees are adopted in the detection process of the central agent and analyzed in selected attacks.

5. CONCLUSION

Intrusion Detection System used to increase level of security in cloud computing. Data mining based IDS demonstrated high accuracy in generalizing intrusions in changing network environment. In this paper different challenges and opportunities are discussed to identify intrusions at various levels. Data mining techniques can be successfully applied to classify intrusions in cloud environment.

6. REFERENCES

1. *Hui-Hao Chou and Sheng-De Wang, "An Adaptive Network Intrusion Detection Approach for the Cloud Environment" IEEE 2015, 49th Annual International Carnahan Conference on Security Technology.*
2. *Hamid Reza Ghorbani, Roya SalekShahrezaie "Toward a Policy-based Distributed Intrusion Detection System in Cloud Computing using Data Mining approaches" IEEE, 2nd ICTCK,2015.*
3. *Rupesh R Bobde et al., "An approach for securing data on cloud using Data slicing and Cryptography", IEEE ISCO 2015.*
4. *FaridMolazemTabrizi and KarthikPattabiraman. 2015. Intrusion Detection System for Embedded Systems. In Proceedings of the Doctoral Symposium of the 16th*

International Middleware Conference (Middleware Doct Symposium '15), Ivan Beschastnikh and WouterJoosen (Eds.). ACM, New York, NY, USA, Article 9 , 4 pages.

5. *Kumar M.; Hanumanthappa M., "Cloud based intrusion detection architecture for smart phones," in Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015 International Conference on , vol., no., pp.1-6, 19-20 March 2015.*

6. *Daesung Moon et al., "Intelligent Security Model of Smart Phone Based on Human Behaviour in Mobile Cloud Computing." Springer 2015.*

7. *Manoj kumar et al., "Unsupervised outlier Detection Technique for Intrusion Detection in cloud computing". IEEE ICCT -2014.*

8. *ChetnaVaid and Harsh K Verma, "Anomaly based IDS Implementation in Cloud Environment using BOAT Algorithm" IEEE 2014.*

9. *Mingshen Sun, Min Zheng, John C. S. Lui, and Xuxian Jiang. 2014. Design and implementation of an Android host-based intrusion prevention system. In Proceedings of the 30th Annual Computer Security Applications Conference (ACSAC '14). ACM, New York, NY, USA, 226-235.*

10. *Yasir Mehmood, UmmeHabiba,"Intrusion Detection System in Cloud Computing: Challenges and Opportunities" IEEE 2013,2nd National Conference on Information Assurance.*

11. *Curti, M.; Merlo, A.; Migliardi, M.; Schiappacasse, S., "Towards energy-aware intrusion detection systems on mobile devices," in High Performance Computing and Simulation (HPCS), 2013 International Conference on , vol., no., pp.289-296, 1-5 July 2013*

12. *Vikrant G. Deshmukh et al.,"Intrusion Detection System for Cloud Computing" International Journal of Engineering Research & Technology (IJERT), 2013.*

13. *K. J. Kim and S. J. Ahn"A Collaborative Intrusion Detection System Framework for Cloud Computing." Proceedings of the International Conference on IT Convergence and Security, Springer Science+Business Media 2012.*

14. *Ahmed Patel et al., "Taxonomy and Proposed Architecture of Intrusion Detection and Prevention Systems for Cloud Computing." Springer 2012.*

15. *Macia-Perez, F.; Mora-Gimeno, F.; Marcos- Jorquera, D.; Gil-Martínez-Abarca, J.A.; Ramos-Morillo, H.; Lorenzo-Fonseca, I., "Network Intrusion Detection System Embedded on a Smart Sensor,"inIndustrialElectronics,IEEE Transactions on , vol.58, no.3, pp.722-732, March 2011.*