Journal of Engineering Design and Analysis
Volume 3, Issue 1 - 2020, Pg. No. 35-38
Peer Reviewed Journal

Review Article

The Review of Big Data Security Analytics for Protecting Cloud-based Virtualized Infrastructures

Hilal Ahmad[1], Sukhdeep Singh[2]

[1]M.Tech Scholar, [2]Assistant Professor, Department of Computer Science Engineering, IET, Bhaddal Technical Campus, Ropar, Punjab, India.

INFO

Corresponding Author:
Hilal Ahmad, Department of Computer Science Engineering, IET, Bhaddal Technical Campus, Ropar, Punjab, India.
E-mail Id:
khanhilal777@gmail.com
Orcid ID:
https://orcid.org/0000-0003-2815-0820

How to cite this article:
Ahmad H, Singh S. The Review of Big Data Security Analytics for Protecting Cloud-based Virtualized Infrastructures. *J Engr Desg Anal* 2020*;* 3(1): 35-38.

Date of Submission: 2020-03-10
Date of Acceptance: 2020-04-25

ABSTRACT

Cloud computing is a popular model designed to deliver information technology services and security is one of the key concerns and is therefore designed to combat detected attacks in critical infrastructures. A virtualized framework has become an important target for cyber attackers to initiate advance attacks. The virtualized framework contains virtual machines that rely on the multi-instance theme of the current hardware defined by the software. The paper deals with security majors for virtualized infrastructures and a comprehensive review of big data security analytics for the protection of virtualized infrastructures in the cloud environment.

Keywords: Intrusion Detection Systems (IDS), Security Data and Event Management (SIEM), Hadoop Distributed File System (HDFS), VM, Internet of Things (IoT)

Introduction

Security analytics applies analytics on the various records that are acquired at various points within the network to find attack existence. By grasping the huge variety of records created by totally different security systems (e.g., Intrusion Detection Systems (IDS), Security Data and Event Management (SIEM), etc.), pertain huge information analytics are going to be apt to note attacks that aren't set via signature or rule-based recognition ways. whereas security analytics eliminates necessitate for signature info by applying event association to find already undiscovered attacks, this is often typically not performed in a period of time and current execution is just about not adjustable. This digitalisation of the marketing world is swing corporations at hazards of cyber-attacks on top of ever antecedent. Huge information analysis has the potential to supply security versus these attacks. Since the construction of a company security circumference has nearly departed in recent years due to the increasing promotion of cloud and mobile services, data security has tailored a smart pattern switch from regular perimeter security tools relating to detective work and observation distractive activities within company networks. Growing advanced attack techniques employed by cyber criminals and therefore the growing task of distractive insiders in varied current large-scale security rupture clearly specify that ancient perspective to data security will now not sustain.

Analytics is an essential part of the resistance to cyber sturdiness. With growing advanced associated constant attacks and therefore the straightforward incontrovertible fact that each administration should secure itself against all classes of attacks whereas an assailant solely wants one victorious try, the company should revise its cyber security plan. They need to manoeuvre on the far side pure interruptions towards the PDR pattern: stop-find-Respond. At the key of this proposal stands improved observation which is wherever huge information analytics comes into play. Recognition should be able to distinguish dynamic use influence to implement compound review quickly, near real-time; to execute complicated correlations over a range of information origin vary from application logs and server to network events and user activities. This would like each leading analytics on the far side straightforward rule-based perspective and therefore the capability to run analysis on the huge quota of gift and historical information-big data security analytics. Mingle the current condition of analytics with security helps the administration upgrade its cyber flexibility. Because of the security industry's feedback to those disputes, a brand new origination of security analytics solutions has appeared in current years, that are able to gather, save and examine monumental amounts of security information over the full venture in real-time. Upgraded by further subject information and external warning intelligence, this information is then examining victimisation totally different correlation algorithms to note deviation and thus acknowledge doable vicious activities. In contrast to classic SIEM solutions, the aforementioned tools utilize in close to real-time and make a tiny low quantity of security attentive align by intensity consistent with a threat model. These alerts are improved with further argumentative details and are able to deeply clarify a security analyst's job and authorize fast awareness and reduction of cyber-attacks.

Literature Review

Niloufer and Saritha (2018) the research paper entitled "Implementation of big data protection analytics in virtualized infrastructures" describes Extensive knowledge and contributed computing are two necessary problems with the happening years, authorize showing possessions to be equipped as data Technology management with extravagant accomplishment and activity. This paper proposes innovative falsifiable data primarily based wholly on security investigation techniques to manage with distinctive motivated attacks in a virtualized infrastructure.

Sridhar and Koushik (2017) this research paper entitled "A Study of Big Data Analytics in Clouds with a Security Perspective" describes Big information may be a sensitive subject with sufficient chance for exploration. With the emergence of social media, the info has begun to cross the boundaries of a system, server, and even an information centre. the other manner, Cloud Computing is yet another space within the IT vary wherever numerous resources like the package, framework, storage, etc. are provided as services on-line. This paper focuses upon the present tendency in massive information storage and evaluating, within the clouds, and conjointly determines the protection defects. It conjointly illustrates the approaching risk of this idea wherever the Internet of Things (IoT) attracts the researcher.

Stalin et al (2017) the research paper entitled "Security Analytics for Protecting Virtualized Infrastructures" describes the hindrance of the attack on host packages from a virtual operating system to reinforce the safety aspects in cloud surroundings. The paper presents a security approach supported logistical regression for detective work advanced attacks.

Win et al (2017) the research paper entitled "Big Data Based Security Analytics for Protecting Virtualized Infrastructures in Cloud Computing" describes the cloud-based mostly virtualized infrastructures and has become a prime target for attackers. The paper presents a unique approach of massive knowledge security analytics to spot the advanced attacks in cloud-based mostly virtualized infrastructures.

Yang et al. (2017) the research paper entitled "Big Data and cloud computing: innovation opportunities and challenges" describes This paper surveys the two frontiers Big knowledge and cloud computing – and reviews the benefits and consequences of utilizing cloud computing to grappling huge knowledge within the digital earth and relevant science domains. From the aspects of a general introduction, sources, challenges, technology standing, and analysis opportunities, the subsequent observations are offered: (i) cloud computing and large knowledge change science discoveries and application developments; (ii) cloud computing provides major solutions for large knowledge; (iii) huge Data, spatiotemporal thinking, and varied application domains drive the advancement of cloud computing and relevant technologies with new requirements; (iv) intrinsic spatiotemporal principles of huge knowledge and geospatial sciences give the supply for locating technical and theoretical solutions to optimize cloud computing and process huge knowledge; (v) open handiness of huge Data and processing capability cause social challenges of geospatial significance.

Prashanthi (2016), the research paper entitled "Analysis of security issues in virtualization cloud computing" describes that in today's world it's thought of the topic, because the whole package fabrication is invasive within the development of cloud services at a speedy rate. Cloud computing offers a simple approach to high attainment computing and storage framework via internet services. This paper presents a summary concerning cloud computing, cloud service, typical cloud coming up with concerning virtualization, Virtualization impact on cloud security, and security threats associated with virtualization.

Gholami and Laure (2016) this research paper entitled "Big Data Security and Privacy Issues in the Cloud" describe that a wide scope of security and privacy concerns that have got to be taken into perquisite. Multi-occupancy, loss of management and trust are key objections in cloud computing ambiance. This paper analyses these technologies and an oversized arrangement of each previous and trendy estimate on cloud security and privacy. we have a tendency to classify this analysis as declared to the cloud associating design coherence, resource management, physical resource, and cloud service administration layers, additionally to analysing this institution to exaggerate the Apache Hadoop security jointly of the foremost swollen massive knowledge frameworks.

Wang and Alexander (2015) the research paper entitled "Big Data in Distributed Analytics, Cybersecurity, Cyber Warfare and Digital Forensics" describes that massive knowledge will decrease the handling time of big quantity of knowledge within the assigned computing ambiance victimisation Hadoop. It can also predict potential cyber security rupture, facilitate terminate cyber-attacks. This paper presents massive knowledge applications in spread analytics, standard cyber security, cyber warfare, cyber protection, and digital forensics.

Varsha et al (2015), the research paper entitled "Study of Security Issues in Cloud Computing" describes the need for knowledge security over the network. The paper presents a review of all the problems of rising over a cloud associated with the security of the cloud.

Ahmed and Hossain (2014), the research paper entitled "Cloud Computing and Security Issues in the Cloud" describes the advantages of cloud computing by deploying in wide-ranging domains. The paper presents a review of cloud computing with security problems inherent among the context of cloud and cloud infrastructure.

Proposed System

The paper presents a review of a novel big data-based security analytics (BDSA) approach to protect virtualized infrastructures against advanced attacks. By making use of the network logs as well as the user application logs collected from the guest VMs which are stored in a Hadoop Distributed File System (HDFS), our BDSA approach first extracts attack features through graph-based event correlation, a MapReduce parser-based identification of potential attack paths and then ascertains attack presence through two-step machine learning, namely logistic regression and belief propagation.

Comparative Analysis of Literature Review

Reference	Title	Technique	Research Findings
Niloufer and Saritha	Implementation of big data protection analytics in virtualized infrastructures	Big Data	Proposes innovative falsifiable data primarily based wholly on security investigation technique to manage with distinctive motivated attacks in a virtualized infrastructure
Sridhar and Koushik	A Study of Big Data Analytics in Clouds with a Security Perspective	Big Data Analytics	This paper focuses upon the present tendency in massive information storage and evaluating, within the clouds, and conjointly determines the protection defects
Win et al (2017)	Big Data Based Security Analytics for Protecting Virtualized Infrastructures in Cloud Computing	Virtualized Infrastructures	Presents a unique approach of massive knowledge security analytics to spot the advanced attacks in cloud-based mostly virtualized infrastructures
Yang et al (2017)	Big Data and cloud computing: innovation opportunities and challenges	Big Data and Cloud Computing	This paper surveys the two frontiers-Big knowledge and cloud computing and reviews the benefits and consequences of utilizing cloud computing to grappling huge knowledge within the digital earth and relevant science domains

Prashanthi (2016)	Analysis of security issues in virtualization cloud computing	Cloud Computing	Describes that in today's world it is thought of the topic, because the whole package fabrication is invasive within the development of cloud services at a speedy rate

Conclusion

The paper presents a review of big data security analytics for protecting cloud-based virtualized infrastructures. The proposed work is based on some latest concepts like Hadoop architecture, Logistic Regression, and Belief Propagation.

Refrences

1. Niloufer B, Saritha VJ. Implementation of Big Data Protection Analytics in Virtualized Infrastructures. *International Journal of Technical Innovation in Modern Engineering and Science* (IJTIMES) 2018; 4(9).
2. Sridhar MB, Koushik A. A Study of Big Data Analytics in Clouds with a Security Perspective. *International Journal of Engineering Research & Technology* (IJERT), 2017; 6(1).
3. Stalin JLA, Narayanan MB, Deepak M. Security Analytics for Protecting Virtualized Infrastructures. *Information Systems & eBusiness Network* 2017.
4. Win TY, Tianfield H, Mair Q. Big Data Based Security Analytics for Protecting Virtualized Infrastructures in Cloud Computing. *IEEE* 2017.
5. Yang C, Huang Q, Li Z et al. Big Data and cloud computing: innovation opportunities and challenges. *International Journal of Digital Earth* 2017; 10(1).
6. Prashanthi M. Analysis of Security Issues in Virtualization Cloud Computing. *International Journal of Computer Science and Mobile ComputingIJCSMC* 2016; 5(8).
7. Gholami A, Laure E. Big Data Security And Privacy Issues in The Cloud. *International Journal of Network Security& Its Applications* (IJNSA) 2016; 8(1).
8. Varsha, Wadhwa A, Gupta S. Study of Security Issues in Cloud Computing. *International Journal of Computer Science and Mobile Computing* IJCSMC 2015; 4(6).
9. Wang L, Alexander CA. Big Data in Distributed Analytics, Cybersecurity, Cyber Warfare and Digital Forensics. *Science and Education Publishing* 2015; 1(1).
10. Ahmed M, Hossain MA. Cloud Computing and Security Issues In the Cloud. *International Journal of Network Security & Its Applications* (IJNSA) 2014; 6(1).
11. Inukollu VN, Arsi S, Ravuri SR. Security Issues Associated With Big Data in Cloud Computing. *International Journal of Network Security & Its Applications* (IJNSA) 2014; 6(3).
12. Swathi T, Srikanth K, Reddy SR. Virtualization in Cloud Computing. *International Journal of Computer Science and Mobile Computing* IJCSMC 2014; 3(5).
13. Kazim M, Masood R, Shibli MA et al. Security Aspects of Virtualization in Cloud Computing 2013.
14. Sabahi F. Secure Virtualization for Cloud Environment Using Hypervisor-based Technology. *International Journal of Machine Learning and Computing* 2012; 2(1).
15. Liu W. Research on Cloud Computing Security Problem and Strategy *IEEE* 2012.
16. Sengupta S, Kaulgud V, Sharma VS. Cloud Computing Security - Trends and Research Directions *IEEE* 2011.
17. Neves PC, Schmerl B, Bernardino J et al. Big Data in Cloud Computing: features and issues.