IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES
ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 4, April 2022

A Critical Analysis on the Use of Big Data Analytics for Cybersecurity

Vineet Saxena, Assistant Professor,
College of Computing Sciences and Information Technology, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email Id- tmmit_cool@yahoo.co.in

ABSTRACT: ***With thousands of connected devices, the the Internet of Things era has increased the surface area that hackers might exploit, necessitating the need for swift and precise attack detection. Cyberattack sorts and incidence have exponentially increased as a result of the Internet's fast expansion. There are several well-known cybersecurity systems in place to thwart these assaults. The production of Big Data across computer systems, meanwhile, is quickly making these conventional techniques obsolete. To address this issue, corporate research is currently concentrating on Security Analytics, or the use of Big Data Analytics methods for cybersecurity. Analytics may help network administrators, especially, with the surveillance and monitoring of live system streams and the real-time identification of malicious and abnormal (outlier) trends. All conventional security measures are intended to be covered and improved by such behaviour.***

KEYWORDS: ***Business, Big Data, Big Data Analytics, Cybersecurity, Fraud.***

1. INTRODUCTION

An increasingly exposed environment makes cyber protection a difficult process. Data collection volumes are constantly growing in the Big Data and Internet of Things age, occasionally swallowing as much as a petabyte of security events every day, and ingestion rates are only expected to rise exponentially over time. A wide surface of access points to protect against cyber assaults has been generated by the connecting of billions of devices through networks and clouds. A strong, data-driven, real-time cyber security defensive plan is increasingly necessary as the volume, sophistication, and variety of cybercrime increase[1].

Firewalls, intrusion response systems, and outdated threat detection methods are insufficient to protect against contemporary cybersecurity threats. More than ever, corporate executives are placing a high importance on swift and precise threat detection, necessitating the use of big data analytics into cybersecurity. Big data analytics makes it possible to quickly handle enormous amounts of high-velocity business data from several sources. It is critical to find abnormalities and attack patterns as fast as possible, to reduce system vulnerabilities, and to increase overall resilience. This requires efficient processing of these huge, heterogeneous information[2].

Cybercriminal intrusions can have disastrous consequences. Big data security breaches may lead to severe fines, significant financial losses, irreparable harm to a brand's reputation, the complete demise of a company, and even time in jail. Cyber defence analysts may collect and better analyse huge data with the use of big data analytics dashboards and machine learning. Data analysis will identify possible cyber risks and provide corporate executives a better understanding of how to anticipate and defend against assaults[3].

1.1. Big Data

This is how Gartner defines big data - “Big data is high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for

ISSN PRINT 2319 1775 Online 2320 7876
Research paper © 2012 IJFANS. All Rights Reserved, **UGC CARE Listed (Group -I) Journal Volume 11, Iss 4, April 2022**

enhanced insight and decision making." There are plenty of definitions out there for big data but Gartner's definition made best sense to me. One notable omission in this definition is visualization. The reason I feel visualization is important is that the collection of data always outpaces our ability to derive value from it. This is due to limited availability of actionable insights. However, with the aid of visual analytics, the structures and patterns in the data can be analyzed and actionable insights can be derived at a rapid pace. The majority of methods used today for big data analytics have been around for a while, including machine learning, behavioural analysis, predictive analysis, statistics, and others. Traditionally, these methods were used to structured data collections with sizes between a few MB and a few GB. Today, they are capable of handling larger amounts of data, including both organised and unstructured data, up to petabytes[4].

Enhanced detection is the key component of this strategy, and big data analytics are used to achieve this. The detection process must be able to recognise shifting use patterns, carry out complicated analysis quickly and almost in real time, and carry out complex correlations across a range of data sources, including server and application logs, network events, and user actions. Big data security analytics are necessary for this, which also calls for advanced analytics that go beyond straightforward rule-based methods. Organizations may increase their cyber resilience by combining security and analytics as it stands now.

1.2. Big Data for Cybersecurity

The main goal of integrating big data into cybersecurity is to enhance possible cyber threats with a more sophisticated method to detection. Any system's detection process has to be quick in order to catch both significant and subtle changes. Rapid, in-the-moment execution of the sophisticated analysis is required. Only a Big Data based solution architecture can handle the sophisticated analytical techniques needed to assess both the history and present data from various data sources[5]–[7] (Figure 1)**.**

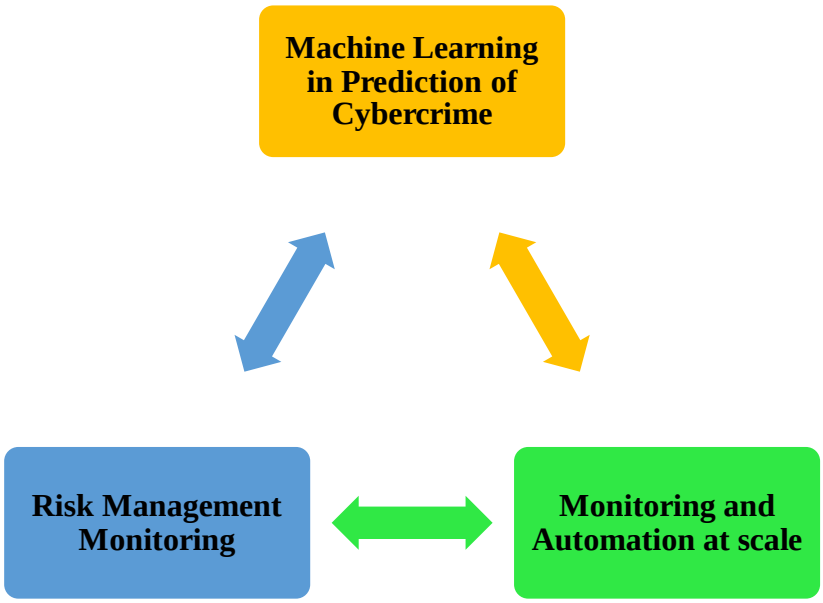

Figure 1: Illustrating the applications of Big Data Analytics in Cybersecurity.

1.2.1. Machine Learning in Prediction of Cybercrime

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 4, April 2022

The past and present data may be analysed to examine and forecast danger trends using data from security measures and machine learning algorithms. Before any assaults are carried out, this strategy can assist in identifying the attackers' contact points. It can also assist with quick reactions to data breaches. These algorithms can autonomously correlate the data to identify patterns of vulnerabilities. Examples of common use cases include anomaly detection, malware identification, and look-alike predictions[8].

1.2.2. Monitoring and Automation at scale

A significant portion of cyberattacks are the result of employee illiteracy in any particular firm. Employees are frequently uninformed of cyber risks and ill-prepared to respond in various situations, making them attractive targets for attackers. Big data analytics may assist in keeping an eye on a broad range of system and user actions to prevent dangers. Many data breaches may be avoided using this strategy. Security professionals may automate these procedures to reduce data breaches and hasten the recovery time in the event of an attack. Businesses may utilise information from a variety of monitoring technologies, including Nagios, Splunk, OSSEC, and others[9], [10].

1.2.3. Risk Management Monitoring

Real-time risk monitoring and detection are challenging tasks, but big data analytics may ease this burden by massively automating the process. Real-time analytics may be added to intrusion detection systems (IDS) for a more thorough method of identifying any malicious activity occurring in the system. Before an attacker may enter the system without authorization, these systems prevent the dangers. For instance, we may aggregate additional information from proxy logs, good/safe domains, and system health monitoring.

2. DISCUSSION

Professionals that can handle and utilise such a considerable amount of important data are in high demand as a result of the exponential rise of data volume over the past few years. Unfortunately, very few data professionals today are aware of the value of big data analytics, how to conduct a successful analysis of big data, and how to use the results to generate knowledge that can be put to use. Network security organisations struggle with a severe shortage of qualified big data scientists, which is problematic for businesses that require in-house data management. Right now, there is just more demand for big data security analytics than there are skilled experts who can use it successfully.

Big data handling goes beyond simply classifying and archiving it. The ability to derive valuable insights that enable your company to safeguard its intellectual property and seek development prospects is the most crucial aspect of big data security analytics. The sheer amount of data that has to be processed, along with the inability to modify it in ways that reveal trends and network abnormalities, is overwhelming for many firms. Your company can continue to spend money on poor network security measures, leaving you vulnerable to assaults or data theft. This might therefore have a negative impact on your bottom line.

Analytics reports, when correctly handled, may help you decide which network security initiatives to end and where to put more money. Big data security is challenging in today's technology environment as hackers become more skilled. Big data sets are at a greater risk of being compromised since this problem becomes much more difficult as the volume grows. This

ISSN PRINT 2319 1775 Online 2320 7876
Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 4, April 2022

is especially true for businesses in sectors like healthcare and finance since several sorts of fraud may be carried out using the data, such:

- Identity fraud
- Check fraud
- Credit card theft
- Medical fraud

Companies with huge data sets require more cybersecurity protection than businesses with smaller data sets. Because of this, it's crucial to make sure that nobody but authorized users has access to your company network. Big data is frequently stored together, so if a hacker manages to break in, they may easily access all the data (Figure 2).

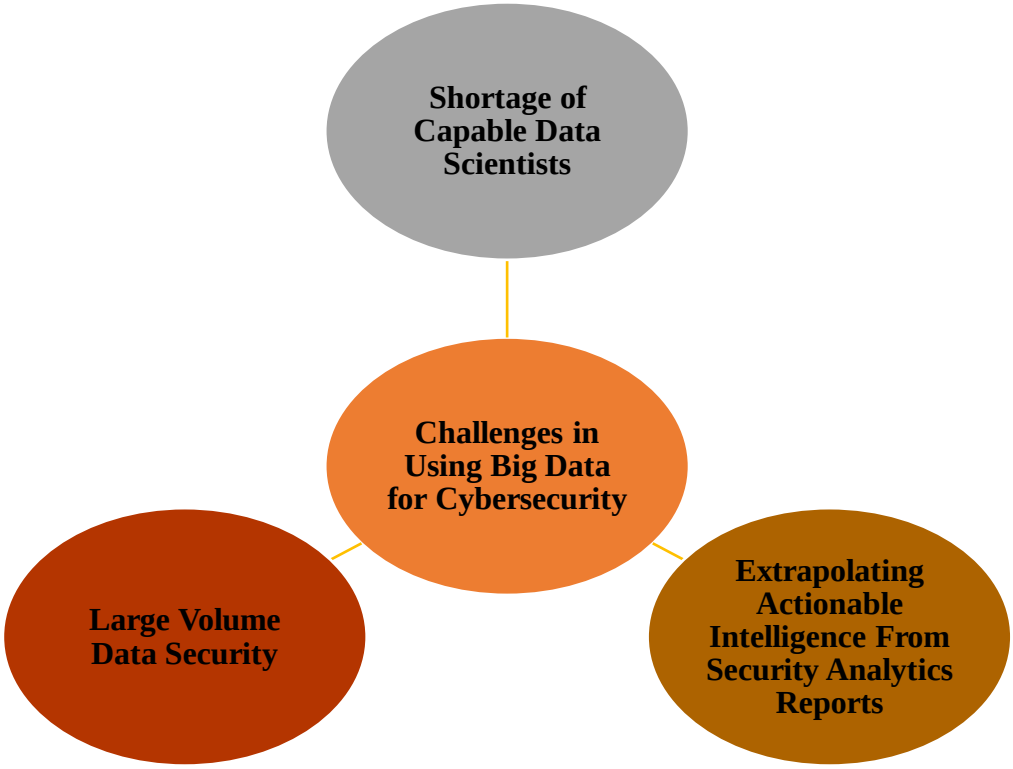

Figure 2: Challenges in Using Big Data for Cybersecurity.

3. CONCLUSION

Real-time actionable information acquisition is the main objective of Big Data analytics for security. In three different ways, big data might significantly affect your present business. It can assist you in: Identify obscure insights Consider customer survey data, for instance, when looking into a high incidence of service cancellations. You could find a trend or core reason that wasn't there previously that you can get rid of to increase retention. Enhance judgments by providing decision makers with better information by taking into account a client's social media profile, for instance, you may acquire a better understanding of that customer and their position in the world. You can then utilise this knowledge to enhance how you respond to support requests or how you order fraud alerts.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper **UGC CARE Listed (Group -I) Journal Volume 11, Iss 4, April 2022**

REFERENCES:

[1] S. Ibrahim, "Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals," *Int. J. Law, Crime Justice*, 2016, doi: 10.1016/j.ijlcj.2016.07.002.

[2] A. Pennington, "Hack attack: TV and cybersecrurity," *Digit. TV Eur.*, 2017.

[3] D. Galinec, D. Moznik, and B. Guberina, "Cybersecurity and cyber defence: national level strategic approach," *Automatika*, 2017, doi: 10.1080/00051144.2017.1407022.

[4] D. J. Lawson, P. Rubin-Delanchy, N. Heard, and N. M. Adams, "Statistical frameworks for detecting tunnelling in cyber defence using big data," 2014. doi: 10.1109/JISIC.2014.47.

[5] R. Bologa, A. R. Lupu, C. Boja, and T. M. Georgescu, "Sustaining employability: A process for introducing cloud computing, big data, social networks, mobile programming and cybersecurity into academic curricula," *Sustain.*, 2017, doi: 10.3390/su9122235.

[6] A. J. Ferrante, "Enhancing Cybersecurity with Big Data Analytics," *Risk Management*. 2017.

[7] T. Mahmood and U. Afzal, "Security analytics: Big data analytics for cybersecurity: A review of trends, techniques and tools," 2013. doi: 10.1109/NCIA.2013.6725337.

[8] W. Dalton, "The silicon hat hacker : using reinforcement learning in hybrid warfare," *Hybrid Threat. Asymmetric Warf. What to do?*, 2017.

[9] M. Bertoncello *et al.*, "Monetizing car data: New service business opportunities to create new customer benefits," *McKinsey&Company*, 2016.

[10] P. G. Martin, "Profiting from the IIOT," *Schneider Electric*, 2016.