TABLE OF CONTENTS

A STUDY OF BIGDATA ANALYTICS AND CYBER SECURITY AS EMERGING TRENDS IN CYBER ERA

Gajanan S. Kumbhar
Research Scholar (Ph.D. Computer Science),
Tilak Maharashtra Vidyapeeth, Pune, Maharashtra, India.
gskumbhar2@gmail.com

Dr. Ajit S. Ghodke
Associate Professor, Department of Computer Science,
Tilak Maharashtra Vidyapeeth, Pune, Maharashtra, India.
ghodke.a@gmail.com

ABSTRACT

In recent, Bigdata analytics is in active use at different fields which has attracted the interest of security communities. Fraud detection is one of the visible uses for big data analytics. New big data technologies like Hadoop ecosystem, stream mining is enabling the analysis of large scale, mixed datasets at unmatched measures and speeds. Technologies are transforming security analytics by giving facility like storage, maintenance and analysis of security information. The application of Bigdata analytics to security problems has a significant potential. In computing context, the term security stands for cyber security. Cyber criminals are never going to stop attacking and when it comes to a Bigdata, the Bigdata technologies has to take more security safeguards with use of cyber security tools and techniques. Bigdata analytics will be leveraged for network and user with real time predictive data analytics also.

KEYWORDS: *Big Data Analytics, Cyber Security, Hadoop, Predictive Data Analytics, Security Safeguards.*

I.   INTRODUCTION

Big data has become an important topic in science, health, engineering, medicine, finance, business and finally society itself. More than 2.5 quintillion bytes of data are created every day [3]. Today all the big organizations are adopting the Big Data technology to improve their business [6].

The Bigdata analytics is the process of collecting, organizing and analyzing a large volume of data to discover useful information. It helps to understand the information contained in data & important for future decision. Bigdata analytics is performed using specialized applications & tools which enable an organization to process a large volume of data.

One of the key points is that big data is not necessarily a still data. It is always in motion which gives rises to man difficulties in analyzing this moving data [6].

In recent, Bigdata analytics is in active use at different fields which has attracted the interest of security communities. Fraud detection is one of the visible uses for big data analytics. Now days Cyber security threats are rising because of sophisticated attack methods used by cyber criminals. The

growing role of malicious insiders in several recent large scale security breaches clearly indicates that traditional approaches to information security can no longer keep up [1].

Applying big data analytics in cyber security is critical. By exploiting data from the networks and computers, analysts can discover useful network information from data. Decision makers can make more informative decisions by using this analysis, including what actions need to be performed, and improvement recommendations to policies, guidelines, procedures, tools, and other aspects of the network processes [5].

The business companies have to alter their cyber security concepts in current scenario. Cyber criminals are never going to stop attacking, and with such a big target to protect, it is cautious for any enterprise utilizing big data technologies to be unbeaten as possible in securing its data [4]. A new generation of security analytics solutions has emerged in recent years, which are able to collect, store and analyze huge amounts of security data across the whole enterprise in real time [5].

You can't discuss the future of cyber security without considering emerging trends in technology and threat landscapes. As organizations develop and adopt technologies related to big data, cognitive computing and the Internet of Things (IoT), cyber threats are growing in both volume and complexity [8].

II. IMPORTANCE OF THE STUDY

1. To Study how we can wrap security breaches in association with Bigdata analytics.

2. To study security tools for organizations data like Hadoop, Mapreduce and NoSQL can be valuable.

III. RESEARCH METHODOLOGY

1. This paper is based on secondary data & review of relevant literature; points are discussed on the same.

2. This study gives a review of how Bigdata analytics and cyber security are allied with each other.

IV. FINDINGS/ DISCUSSION

1. One of big data's biggest advantages is its ability to analyze massive numbers of potential security events and connect between them to create a prioritized list of threats. As cyber criminals are rapidly evolving their hacking techniques, and are attacking quickly, making timely security and fraud analytics more critical than ever, big data analytics enables enterprises to combine and correlate external and internal information to see a bigger picture of threats against their enterprises [2].

2. Big data tools present a terrible protection when used correctly. While businesses are using big data to boost their outcome and cyber criminals hiding within big data to make it work to their advantage [2].

3. Applying big data analytics in cyber security is critical. By exploiting data from the networks and computers, analysts can discover useful network information from data. Decision makers can make more informative decisions by using this analysis, including what actions need to be performed, and improvement recommendations to policies, guidelines, procedures, tools, and other aspects of the network processes [5].

4. Having a large amount of historical data at hand also significantly simplifies initial calibration to the normal patterns

of activity of a given network, which is then used to identify anomalies. Existing solutions are already capable of automated calibration with very little input required from administrators [1].

5. Bigdata is presenting challenges to cyber security. For an example, the Internet of Things (IoT) will reportedly soon generate a staggering 400 zettabytes (ZB) of data a year. Self-driving cars are predicted to mix out 4000 GB of data per hour of driving. Big data analytics, as an emerging analytical technology, gives the capability to collect, store, process, and visualize these vast amounts of data.

6. One of the biggest concerns in our present age revolves around the security and protection of sensitive information. In our current era of Big Data, our organizations are collecting, analyzing, and making decisions based on analysis of massive amounts of data sets from various sources, and security in this process is becoming increasingly more important [5].

7. Cyber-attacks are becoming increasingly sophisticated, from drive-by downloads to watering hole attacks to the most common attack vector – spear phishing. Malware is now polymorphic, changing its thumbprint as many as thousands of times per minute to evade corporate defenses. Advanced persistent threats (APTs) are now constantly targeting specific organizations, often starting with spear phishing emails which compromise systems to gain network access and eventually deploying additional tools to fulfill attack objectives [7].

8. Securing Big Data:

A. **Hadoop:** Hadoop is the industry standard for handling big data because it's very scalable. You do not have to

worry about the spiteful issues associated with big data spanning across multiple disks and multiple machines .It takes care the resilience, fault tolerance, and scalability issues [3].
This technology plays an important role in making Big data a trending topic in today's scenario [6].

B. **Map Reduce:** Map Reduce (Map Reduce has their own vision of Hbase), in memory databases and analysis frameworks like Spark and Shark, as well as graph databases like unlimited Graph and Titan. Map Reduce highlights parallelism in data retrieval. Jobs are parceled out or 'mapped' to a number of subsidiary nodes, with result handed backup (reduced) in the ultimate of the original tasks [3].

C. **NoSQL:** It's a platform such as Cassandra , Mongo DB, and others .It's techniques that directly address some of limitations of traditional relational data store when analysis of a body of data is the priority .They can be highly distributed systems ,developed in many cases to deliver better performance in data management and retrieval at Internet scale .They are well suited for the analysis of an entire body of recorded data to discover patterns, trends, and anomalies which makes them compelling candidates for handling large and diverse bodies of security-relevant data[3].

V. SUGGESTIONS

1. Businesses should identify and encrypt their data, integrating big data analytics into a solid infrastructure to offer strong security solution [2].

2. In current digital era we have to understand the importance of security as we process and analyze massive amounts of data [4].

VI. CONCLUSION

Big Data Analytics in Cyber security examines security challenges surrounding big data and provides actionable insights that can be used to improve the current practices of network operators and administrators [5]. Bigdata analytics can predict cyber-attacks in real-time, by using tools and combat the cyber-attacks immediately.

REFERENCES

[1] A Survey over 330 participants from more than 50 countries "How big data technology can help to increase Cyber Attack resilience by better detection of attacks, enabling real-time response", **BARC** (Business Application Research Center), Kuppinger Cole, Available at: <https://bi-survey.com/big-data-security-analytics> [Accessed 20 February 2018].

[2] Big Data: A Double-Edged Sword in Cyber security, Sohini Bagchi, Available at: <http://www.cxotoday.com/story/big-data-a-double-edged-sword-in-cybersecurity>, [Accessed 20 February 2018].

[3] Big Data In computer Cyber Security Systems, Amani Mobarak AlMadahkah, IJCSNS International Journal of Computer Science and Network Security, VOL.16 No.4, April 2016.

[4] Big Data Analytics for Security, Alvaro A.Cardenas[1], Pratyusa K. Manadhata[2], Sreeranga P. Rajan[3], Available at: < https://www.infoq.com/articles/bigdata-analytics-for-security>[Accessed 20 February 2018]

[5] Big Data Analytics in Cyber security, Onur Savas[1], Julia Deng[2], Available at: < https://www.crcpress.com/Big-Data-Analytics-in-Cybersecurity/Savas-Deng/p/book/9781498772129>[Accessed 20 February 2018].

[6] BIG DATA "AN INDISPENSABLE NEED OF IT INDUSTRY", Shahnawaz Sarwar[1], Aiman Zubair[2], Cyber Security International Journal of Technology & Management Vol. 7 Issue 2, April 2014- September 2014, 523-530..

[7] Cyber Security Enhanced with Powerful Big Data Analytics, Rich Nowalk, Available at:https://www.opextechnologies.com/cyber-security-enhanced-with-powerful-big-data-analytics [Accessed 20 February 2018].

[8] The Future of Cyber security, Domenico Raguseo , Available at: <https://securityintelligence.com/the-future-of-cybersecurity>[Accessed 20 February 2018].