ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Special Issue 7, October 2015

A Compact Structure in Big Data Analytics to Substantiate the Threats in Computer-Security

Dr. Anthony Vincent. B, Rajesh H

Assistant Professor, Department of Computer Science, Kristu Jayanti College, K.Narayanapura, Kothanur (PO), Bangalore, India

Assistant Professor, Department of Computer Science, Kristu Jayanti College, K.Narayanapura, Kothanur (PO), Bangalore, India

ABSTRACT: Big Data assures to open new possibilities in all aspects of business and analytics, there is an obvious downside. The more we digitize information and the more information we gather, the more doors we potentially open for hackers and intruders. Big Data has rendered older security models largely outmoded. The all-in-one security product approach that served the industry well in last decade seems hopelessly derisory today.

The Big companies have experienced high-profile data breaches were spending billion dollars on security. So private and public sectors were thinking they had to pitch money at the problem posed by Big Data as well as the serious implications of a breach. The breaches helped create more awareness of the challenge being faced in the enterprise. These companies are beginning to realize the problem posed by Big Data as well as the serious implications of a breach. It is not only threatens a company's brand and stock value, but it can also impacts private and government sectors.

We need to use software to do the heavy lifting to combat securities and cyber-terrorists. Our objective of this to establish a compact structure in Big Data analytics in Computer-Security domain to substantiate the threats. This can be done through formulating and assessing the threats through the security tools in which focusing on the following areas: accelerate incident detection, improve staff efficiency, reduce false positives, automate manual processes, and surpass point tools.

KEYWORDS: Big data, Investigation, Computer-Security, analysis, threats, detection, efficiency

I. INTRODUCTION TO CONFRONTING OF BIG DATA

As the amount of huge data being collected continues to grow, many supplementary companies are building big data warehouses to store, aggregate and extract meaning from their data. Acquiring big data comes with its own exceptional challenges beyond being a high-value target. Many of the warehouses collect data at huge volumes and large transmission of velocity from various data sources, and they all likely to generate its own data transmission workflows. These connections to multiple warehouses can increase the attack apparently for an opponent.

Four categories of information that constitute big data:

1. System-generated data. It covers RFID data, geo data from mobile phones, and data from observing devices such as utility meters.
2. Computer systems log data, such as clickstreams from websites.
3. Text information from various social media sites such as Linked In, Twitter, Facebook and Google Plus.
4. Multimedia information from Flickr, YouTube.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Special Issue 7, October 2015

The following are the differences when comparing with the existing database systems

- The data gathered, consolidated and evaluated for big data analysis
- The infrastructure used to keep storing big data
- The technologies used to analyze structured and unstructured big data

The variety, velocity and volume of big data intensify security management challenges that are assessed and reported in traditional security management. Big data warehouses will likely include information dumped by various springs across the sectors. This variety of data makes secure access management as an experiment. Each data source will likely have its own access constraints and security procedures, making it difficult to balance suitable security for all data sources with the need to have a comprehensive and extract significance of the data.

II. BIG DATA: A VALUABLE ASSET

There are four extensive ways in which using big data can create value.

1. Big data can be usable at much higher frequency and I can unlock significant value by making information transparent.
2. Big data exposes variability and boost performance. As organizations create and store more transactional data in digital form, they can collect more accurate and detailed performance information on everything from product inventories to pale days,
3. To make better management decisions and to use data for basic low-frequency forecasting to high-frequency forecasting to adjust their business levers just in time. Sophisticated analytics can extensively improve decision-making process.
4. Big data can also be used to improve the development of the next generation of products and services. [2]

Internet of Things (IoT) vs Big data:

The Internet of Things (IoT) is on its way to becoming the next high-tech rebellion technology to the modern era in term of security. IoT and big data basically are two wings of the bird. Handling and extracting value from IoT data is the major experiment that will enable the private and public sectors faced in today's generation. Both private and public should set up a proper analytics platform/infrastructure to investigate the IoT data to be used in near future or in the present world.

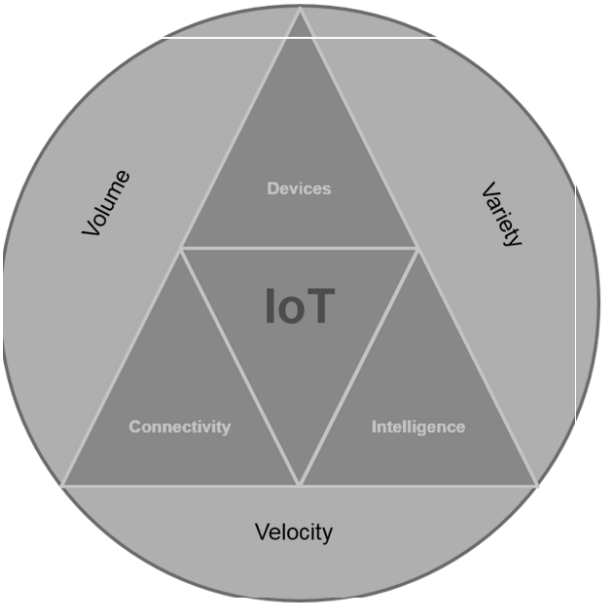

Figure 1: Dimensions of IoT to Big data

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Special Issue 7, October 2015

And it should be should remembered that not all IoT data is significant. An IoT might not be generated continuously in an accessible way, and sectors using IoT must handle the huge volume of stream data and perform actions on that big data. The schedules can be event association, metric calculation, statistics groundwork, and analytics. In a typical big data scenario, the data might not be always stream data, and the actions are different. Building an analytics resolution to manage the scale of IoT data should be done must be modified accordingly in order the secure the data.

IoT data will require software engineers to make some indispensable necessary changes to their field of security landscape. As the IoT develops, an unmanaged number of IoT approaches will be connected to the network. These approaches will be of different shapes and sizes and positioned outside the network, skilled of communicating with commercial applications. Therefore, each device should have a non-reputable credentials for authentication purposes. The types of devices that make up the IoT and the data they generate will vary in time-to-time and the raw data, various data types, and communication code of behavior – and this carries inherent data security risks. This assorted IoT world is new to security professionals, and that helps of knowledge feeds and will increases security jeopardies in IoT. Ant this might attack and could threaten more than just the data and the resource used in IoT and it also may perhaps damage the connecting devices in all the sectors. [1]

III. A PROCEDURAL OUTLINE TO DEAL WITH BIG DATA

Step 1: Segregate big data. A big data environment may include a dataset with proprietary research information, a dataset requiring regulatory compliance, and a separate dataset with personally identifiable information (PII).
Step 2: Correlate big data. A researcher might want to correlate their research with a dataset including PII data,
Step 3: Restrict data sets to ensure adequate security
Step 4: Protect big data by balancing analysis and on a use-case basis.

Analytics Platform: Our proposal approach
Phase1: Receive data

Receive measures from IoT-connected devices. The devices can be connected to the network using Wi-Fi, Bluetooth, or any wireless technology, but must be able to send messages to an agent using specific protocol. Mostly used protocol is Message Queue Telemetry Transport (MQTT) and Mosquitto is a popular open-source MQTT agent.

Phase 2: Store data

Once the data is received, the next concern is the technology platform to store the IoT data. Use Hadoop framework or Hive to store big data. But for IoT data, use the latest tools like Apache CouchDB , Apache Storm and Apache Kafka.

Phase 3: Secure data

A multifaceted security system and appropriate network integration will help in preventing attacks and keep them from spreading to other areas of the network. A properly configured IoT system should follow better network access control policies to check which IoT devices are allowed to connect. Software-defined networking (SDN) technologies, in combination with network identity and access policies, should be used to create dynamic network segmentation. [1]

Phase 4: Apply analytics to the data

A proper analytics platform should be based on three parameters: performance, correct size infrastructure, and future growth. For performance, a plain-metal server, a single tenant physical server dedicated to a single customer, is the perfect choice. For infrastructure and future growth, hybrid is the right option. Hybrid deployments, which consist of cloud, managed hosting, collocation, and dedicated hosting, combine the best features from multiple platforms into a single optimal environment. Managed Service Providers (MSPs) are also playing role on their platforms to handle IoT data. MSP vendors works on the infrastructure, performance, and tools side to protect the entire IoT domain.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Special Issue 7, October 2015

Figure 2: Security measures

IV. CONCLUSION

The use of big data analytics will have a significant foundation of competition and development for individual organizations. From the point of competitiveness and the potential detention of values, all companies must to take big data analytics extremely. In most developed industries, well known competitors and new comers alike will influence data driven strategies to innovate, compete, and capture value from deep and up-to-dated information. Few issues need to be addressed to capture the complete potential of big data. Policies in subject with privacy, security, intellectual property, and liability will need to be explored in a big data world. Rather than Organizations putting the right talent and technology, the structure workflows and incentives to optimize the use of big data should have been configured.

All private and public sectors should be ready to adapt technologies to map with IoT data. Network, disk, and compute power all will be compressed and should be planned to inculcate of this new type of data technology. The growth of the IoT proclaims a new age of technology, and organizations that wish to participate in modern era will have to change the approach they do things to lodge new data types and data sources. This technique will be the beginning to the modern era. As the IoT grows and all sectors will also grow with IoT proportionally.

REFERENCES

[1] http://data-informed.com/the-impact-of-internet-of-things-on-big-data/
[2] http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier