Security and Privacy –A Big Concern in Big Data A Case Study on Tracking and Monitoring System

Tilwani Mashook[1] Patel Malay[2] Pooja Mehta[3]
[1,2]U.G.Student [3]Professor
[1,2,3]Department of Computer Engineering
[1,2,3]Sal Institute Of Technology& Engineering Research

Abstract— With the ever-increasing usage of Employee Tracking and Monitoring System data for fleet management is increasing enormously there is a need for proactive Tracking and Monitoring. In addition, the new wave of digitizing Fleet records has seen a paradigm shift in the corporate industry. As a result, the corporate industry is witnessing an increase in sheer volume of data in terms of complexity, diversity and timeliness. As corporate experts look for every possible way to properly manage and track Employee while improving Monitoring process, Tracking and management, big data emerges as a plausible solution with the promise to transform the corporate industry. This paradigm shift from reactive to proactive employee data can result in an overall decrease in risk costs and mismanagement of tasks by employee which would eventually lead to Company's growth. While the Corporate industry harnesses the power of big data, security and privacy issues are at the focal point as emerging threats and vulnerabilities continue to grow. In this paper, we present the state-of-the-art security and privacy issues in big data as applied to Employee Tracking and Corporate Fleet Management.

Key words: Big Data, Fleet Management, Global Positioning System Issues, Privacy Issues of Data, Location Intelligence, Monitoring, Tracking,etc

I. INTRODUCTION

Employee Tracking is an emerging technology in existing research and have the potential to transform the way of human life in the working hours.(i.e., make life more Accurate and Analyzed). A GPS (Global Positioning System) is the smallest unit of a mobile phone that has unique features, such as, it supports large scale deployment, mobility, reliability, etc. GPS is not limited to science and engineering, but they are also included in other popular applications such as the military, human monitoring, infrastructure monitoring, government security policy, Object Monitoring. The main goals of Employee Tracking Systems are to monitor the employees or the field laborers and help them analyze themselves also to let the organizations to analyze their performance.The raw data obtained from the servers is processed online or offline for detailed analysis at the remote server according to the application requirements.

II. WHERE'S THE PROBLEM?

The development of a Tracking application offers many novel challenges, such as, reliable data transmission, support and fast event detection, timely delivery of data, power management and proper visualization of data. Further however, deploying new technologies in tracking and monitoring applications without considering security often makes patient privacy vulnerable For instance, the employee's locational vital signals are very sensitive because they keep on changing frequently when the employee is travelling. Further, GPS covers a broad range of tracking and monitoring applications Task data monitoring, and activity monitoring incorporates, location tracking for field employees, etc. Consequently, tracking and monitoring share individual data with Admin, Managers, and HR in the corporates. Indeed tracking and Monitoring applications can offer many advantages to Employee monitoring, but the data of an individual are highly vulnerable, so security and privacy become some of the big concerns for tracking and monitoring applications, especially when it comes to adopting wireless technology or Global Positioning System.[7]

III. MAJOR CHALLENGES WHEN IT COMES TO SECURITY

Almost all data security issues are caused by the lack of effective measures provided by antivirus software and firewalls. These systems were developed to protect the limited scope of information stored on the hard disk, but Big Data goes beyond hard disks and isolated systems. And as tracking and monitoring applications will be continuously receiving data at a huge speed data will be touching skies.[4] [20]

A. Nine Big Data Security Challenges for tracking and monitoring applications:

- Most distributed systems' computations have only a single level of protection, which is not recommended.
- Non-relational databases (NoSQL) are actively evolving, making it difficult for security solutions to keep up with demand.
- Automated data transfer requires additional security measures, which are often not available.
- When a system receives a large amount of information, it should be validated to remain trustworthy and accurate; this practice doesn't always occur, however.
- Unethical IT specialists practicing information mining can gather personal data without asking users for permission or notifying them. [1]

- Access control encryption and connections security can become dated and inaccessible to the IT specialists who rely on it.
- Some organizations cannot – or do not – institute access controls to divide the level of confidentiality within the company.
- Recommended detailed audits are not routinely performed on Big Data due to the huge amount of information involved.
- Due to the size of Big Data, its origins are not consistently monitored and tracked.[13][16]

B. Some of the latest challenges observed in the Big Data by the Tracking and Monitoring Application's Organization:

1) User Data Privacy

You would be surprised to know how the amount of data collected about each person in particular can be processed and analyzed to provide a surprisingly complete picture. Consequently, establishments that own the information are legally responsible for the security of their data. Attempts to make anonymous certain data are useless in protecting people's privacy, because there is so much data available, that you can use some of it as a link for identification purposes.[6] User information is in transit all the time, being accessed by the inside users, outside contractors, and business partners sharing it for research.[19]

2) Granular Access

One of the greatest challenges when implementing a big data security system is respecting privacy concerns while still permitting the usage and analysis to continue. While a privacy breach has ethical and legal implications, a large amount of data is useless without being able to use it. This is one of the reasons only 0.5% of data is being used and analyzed at the moment. Granular access control acts on every piece of data individually, ensuring a high level of both security and usability. However, some major problems with efficient implementation of granular access control are keeping track of privacy requirements and policies in a cluster-computing setting; keeping track of user access and the proper employment of security requirements.[11][17]

3) Monitoring in Real-time

Real-time monitoring is designed to alert the company at the very first sign of an attack; however, the amount of feedback from SIEM (security information and event management) system, whose aim is to provide the big-picture feedback of the data, is enormous. Companies that have the resources to closely monitor this feedback and separate the real attacks from the false ones are rare. Fortunately, there are providers that can offer an alternative through a remote support software, for both small businesses and larger enterprises. [7][8]

4) Granular Audits

The major goal of monitoring in real-time is to give the company the heads-up at the first sign of trouble. Since this does not always happen because of the challenges of identifying the real risks among the huge number of false alarms, it is crucial to have regular, granular audits to recognize breaches after the fact. Audit information can help to identify exactly what happened, so that future breaches can be identified and avoided. An effective inspection depends on numerous factors – controlled and timely access to information, the integrity of the information, etc. [7][17]

The majority of solutions and platforms are still struggling to handle the vast volume, variety and velocity of big data. So far, security has been a tack-on feature to the managing tools; however, it is now evident that the value of big data lies in both the company's ability to leverage it for better products and its ability to protect it from outside attacks.

5) Preserve the Privacy in Data Mining and Analytics:

Big data can enable "invasions of privacy, invasive marketing, decreased civil liberties, and increased state and corporate control". The amount of information collected on each individual can be processed to provide a surprisingly complete picture. As a result, organizations that own data are legally responsible for the security and the usage policies they apply to their data. Attempts to anonymous specific data are not successful in protecting privacy because there is so much available that some data can be used as a correlation for identification purposes.Users' data are also constantly in transit, being accessed by inside users and outside contractors, government agencies, and business partners sharing data for research.[9]

6) Encrypted Data-Centric Security.

There are two distinct approaches to applying security controls to control data visibility: first, controlling access to the system, and secondly, applying encryption to the data itself. The first method, which is easier and less costly to implement, is also less effective, as it provides what it calls a larger "attack surface". If the system is breached, then the attacker has access to all the data. Deploying encryption on all data on a granular basis helps ensure that even if there is a system breach, the data itself remains protected.[18]

7) Data Provenance and Verification

Big data is collected from a wide variety of sources, and in enterprise settings that can mean millions of end-user machines. In this environment, the question of how trustworthy the data might be is of paramount importance. As the volume grows, so does the complexity of the provenance. Provenance information is contained in the metadata attached to each data object and provides information about the object's creation. In big data applications, the provenance metadata includes the provenance for the big data infrastructure itself, which is like having meta-metadata. As development in this area progresses, provenance metadata will become more complex due to large provenance graphs generated from provenance-enabled big data applications. Analytics for graphs of this size and complexity are very resource-intensive in terms of computational overhead. The major threats to data integrity in big data applications are malfunctioning infrastructure, and attacks on infrastructure from inside or outside the organization. The provenance metadata itself must be protected as well so that audits and other detection methods can be effective in verifying data sources.[15]

8) Integrity and Reactive Security:

Endpoint Input Validation and Filtering, Because of the breadth of data sources, including endpoint collection devices, a major challenge facing big data schemes is whether the data is valid from the point of input. Given the size of the data pool, how can we validate the sources? How can we be sure that a source of input data is not malicious, or simply incorrect? In addition, how can we filter out malicious or unreliable data? Both data collection devices and programs are susceptible to attack. An infiltrator may spoof multiple IDs and feed fake data to the collection system (ID clone attack, or Sybil attack). [10]

IV. HOW TO ENSURE SECURITY AND PRIVACY:

During the transition phase, the EHR vendor must work closely with the healthcare provider for a smooth and secure transition. The company should provide some type of comprehensive user guide for the users in the provider's practice for implementing some of the software's or applications in the device of the human who is supposed to be tracked or monitored. [3]There are six ways in which tracked and monitored record or data security and privacy can be ensured and they are as follow:

1) Enhance administrative controls
– Update policies and procedures
– Guide employees through the stringent privacy and security training process
– Run background checks on all employees
2) Monitor the devices and system access
– Have exigencies in place for data recovery or restoration
– Provide identification and verification requirements to all system users
– Access the list of authorized users
– Supply passwords and personal identification numbers (PINs)
– Provide automatic software shutdown routines
– Leave data backup and recovery to the professionals
– Businesses should leave data backup and recovery to the professionals
3) Identify Workstation Usage
– Set privacy filters at each workstation
– Distinguish the different capabilities of different workstations
4) Audit and monitor system users
– Identify any weakness in the system
– Detect any security breach or attempt at a breach
– Regularly audit all authorized users
– Issue specified punishments to employees not following compliance guidelines
5) Employ device and media controls
– Construct a security plan for data disposal
– Remove data from reusable hardware
– Track all reprocessed hardware
– Back up all data from all hardware. [8][18]
6) Apply data encryption
– Disguise all data inside tracked data and monitored data through cryptography.[5]
– Reliable electronic records companies apply these enhanced security and privacy protocols. Perhaps the most important security protocol is data encryption, which causes data to become unreadable to outside sources.
– Electronic records specialists also provide remote storage and data backup systems. While this may not necessarily present as strong of a defense against hackers and data breaches as data encryption, it provides security for healthcare organizations against the potential of software failures or natural disasters that could destroy or damage files.[12]

V. CONCLUSION

As big data transforms tracking and monitoring, security and employee privacy is paramount in driving such technologies. As tracking and monitoring data storage clouds with big data become prominent, hosting companies will be more reluctant to share massive tracked and monitored data with the organization for centralized processing and evaluating the fleet and employees according their working capability. Secure employee tracked and monitored data management is inevitable as the clouds aggregate and link large amounts of data from disparate networks. Additionally, secure and privacy preserving real-time analytics will propel proactive tracking and monitoring. In this paper, we review some of the security and privacy issues in Big Data a need for technological breakthroughs in computational, storage and communication capabilities to meet the growing demand of securing tracked and monitored data of the employees or different users who are being tracked and monitored continuously [2].

REFERENCES

[1] Jose Moura,Carlos Serrao ”Security and Privacy Issues in Big Data”
[2] Harsh Kupwada “Big Data and Privacy Issues in HealthCare” Patil Publication
[3] https://www.researchgate.net

[4] http://www.datacenterknowledge.com/
[5] http://www.ironmountain.com/Knowledge-Center/Reference-Library/View-by-Document-Type/General-Articles/E/Electronic-Health-Records-Security-and-Privacy-Concerns.aspx
[6] https://blog.appdynamics.com/
[7] M. Gruteser ”Privacy Issues in Location Tracking” IEEE SECURITY AND PRIVACY.
[8] http://cseweb.ucsd.edu/groups/csag/html/teaching/cse225s04/Reading%20List/gsi-security.pdf
[9] https://www.researchgate.net/publication/300413833_A_survey_on_security_and_privacy_issues_in_big_data
[10] http://ijicse.in/wp-content/uploads/2015/12/v2i4-3.pdf
[11] http://theconversation.com/big-data-security-problems-threaten-consumers-privacy-54798
[12] http://searchsecurity.techtarget.com/feature/Managing-big-data-privacy-concerns-Tactics-for-proactive-enterprises
[13] OECD Privacy Principles: http://oecdprivacy.org
[14] https://www.iso.org/files/live/sites/isoorg/files/developing_standards/docs/en/big_data_report-jtc1.pdf
[15] http://www.computerweekly.com/feature/How-to-tackle-big-data-from-a-security-point-of-view
[16] https://www.secureworldexpo.com/industry-news/10-big-data-analytics-privacy-problems
[17] https://www.infosecurity-magazine.com/opinions/big-data-security-privacy/
[18] http://www.informationweek.com/strategic-cio/security-and-risk-strategy/top-data-privacy-issues-to-scare-you-in-2016/a/d-id/1323752
[19] http://files.technologyreview.com/whitepapers/Oracle-Securing-the-Big-Data-Life-Cycle.pdf
[20] http://www.renci.org/wp-content/uploads/2014/02/0213WhitePaper-SMW.pdf