International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Email:editorijoer@gmail.com http://www.ijoer.in

Vol.4., Issue.1., 2016
(Jan-Feb)

REVIEW ARTICLE

ISSN: 2321-7758

BIG DATA ANALYTICS FOR SECURITY AND PRIVACY OF POLICE ONUSES (SPPO)

ROMIKA YADAV[1], VINTI PARMAR[2], MAMTA SHARMA[3]

[1]Research Scholar, Indira Gandhi University, Meerpur, Rewari, India
[2]Research Scholar, Indira Gandhi University, Meerpur, Rewari, India
[3]Jamia Hamdard University, New Delhi, India

ABSTRACT

Security and privacy becomes continuously stiffer for the every aspects of the data communication. Today's software provides many security services to make things confidential. Introducing Big data Analytics provides significant opportunities for security and privacy of data. Even though the principles of policing remain a constant, the world in which the police operate has undergone dramatic shifts. Keeping the peace, protecting life and property and enforcing the law are responsibilities that are now challenged by rising citizen expectations, the changing nature and growing sophistication of crime and a need to address often severe budgetary constraints. With a growth in the wireless applications on the networks need for reliable Security and Privacy for Police Onuses (SPPO) provides secure mechanism of data aggregation and reliable data communication over the large network. The purpose is to analyze the state of the art big data research for information security to determine the research direction.

Keyword-Security, Privacy, Big Data Analytics, Hadoop, Police Onuses

I. INTRODUCTION

Security and privacy becomes constantly stiffer for the all aspects of the data communication. Privacy issues involving sensing, identification, storage, processing, sharing, and use of this information in technical, social, and legal contexts. Privacy of personal location information is becoming an increasingly important issue. Security – i.e., the confidentiality, integrity, and authenticity of information – is often a necessary ingredient to privacy, as it facilitates the control of information flows (i.e., who gets to know what when?) and helps to ensure the correctness of data. Recent technological advances in wireless location tracking (such as that found in cell phones and radio frequency identification (RFID) chips, among others) present unprecedented opportunities for monitoring individuals' movements. While such technology can support useful location-based services (LBS), which tailor their functionality to a user's current location, privacy concerns might seriously hamper user acceptance.

II. RELATED WORK

Big Data Analytics consist of large data set that is Big Data used to discover patterns by the process to collect organize and analyze the data sets. Large Enterprises generates data in 10 to 100 billion events per day. Existing techniques do not work with

large scales of data. Problems worse when enterprises move to cloud architecture and Location Based Service systems has been analyzed. The analysis confirmed the heterogeneity of the research problems associated with Location Based Services as well as the array of solutions to address these problems [12]. Computational location privacy algorithms treat location data as geometric information, not as general data [13].Studies show that people are generally not concerned about location privacy, although they are sensitive to how their location data could be used, and their sensitivity may raise with their awareness of privacy leaks. Offering users to control who can read what tags is difficult due to the high number of items and the lack of user interface [14].

III. PROBLEM DEFINITION

Large Enterprises generates data in 10 to 100 billion events per day. Existing techniques do not work with large scales of data [1]. Retaining large quantities of data was not economically feasible. Most event logs recorded and other computer activities were deleted at fixed period of time i.e. 60 days [1]. SIEM tool were not designed to analyze and managed unstructured data; however they were bound with predefined schemas [1]. Data Correctness or provenance of data, whether this data trustworthy or not. To overcome above challenge needs authentication of data to use in the tools. Require visual analytics of data that provide visual interface. Need development in HCI [1]. Bharat Bhargava et al. [7] discuss problems of traditional security mechanisms are tailored to securing small-scale data; they can't meet the needs of big data. Moreover, the inherent vulnerabilities of a cloud-based environment require significant focus on both privacy and security together with risk management procedures [7]. The existing techniques suffer from several major problems including lack of secrecy and privacy, which makes the network vulnerable to adversaries and attacks [9]. Redundancy exists in data, resulting in data and network overload. Traditional operations are performed for data aggregation. Hence, the security factor is not that high [9].

IV. PROPOSED WORK

This Big data applications become part of security management software and provide complete data, Less noisy data, query data in heterogeneous and finally Hadoop is used to cluster the data to bring new opportunities of data [1]. The WINE Platform [2] and BotCloud [3] allow the use of MapReduce to efficiently process data for security analysis. Traditional SIEM takes 20 minute to search a month's load of data; however Hadoop system running queries with Hive it gets result in approximately in one minute [4]. Big data tools also suited for Advanced Persistence Threats (APT) detection and forensics. To detect these attacks collecting external and internal shared intelligence data [5,6].

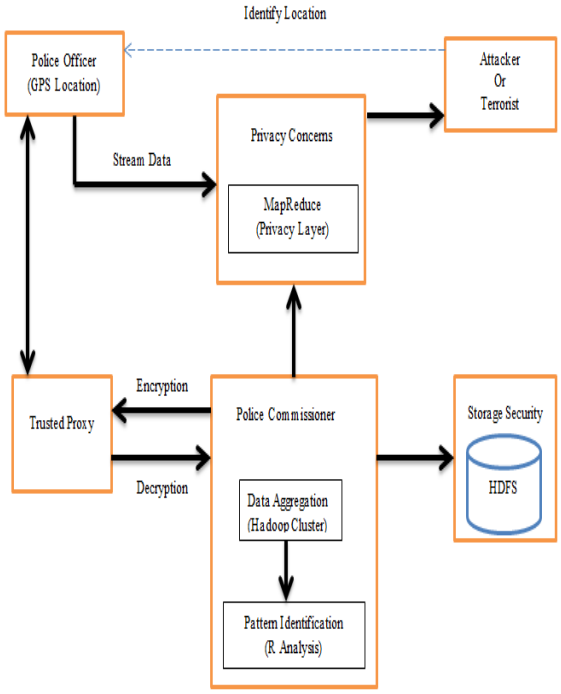

Figure 1: Framework of Security and Privacy of Police Onuses (SPPO) on Hadoop Technology

V. CONCLUSION AND FUTURE WORK

In Problem domain has been analyzed and outline of the solution has been developed. Various privacy techniques have been studied to provide security and efficiency. The integration of location privacy through MapReduce, data aggregation through Hadoop clusters and pattern identification through R Studio in the wireless network for Security and

Privacy of Police Onuses. Future works includes automation of this integrated mechanism. Based on the analysis of police onuses applications and their proposed architecture i.e. SPPO.

REFERENCES.

[1]. Cardenas, Manadhata and P. Rajan, "Big Data Analytics for Security", IEEE Computer and Reliability Societies, pp. 74-76, Nov/Dec. 2013.

[2]. T. Dumitras and D. Shou, "Toward a Standard Benchmark for Computer Security Research: The Worldwide Intelligence Network Environment (WINE),"Proc. EuroSys BADGERS Workshop, ACM, 2011, pp. 89–96.

[3]. J. François et al., "BotCloud: Detecting Botnets Using MapReduce,"Proc. Workshop Information Forensics and Security, IEEE, 2011, pp. 1–6.

[4]. E. Chickowski, "A Case Study in Security Big Data Analysis," Dark Reading, 9 Mar. 2012.

[5]. P. Giura and W. Wang, "Using Large Scale Distributed Computing to Unveil Advanced Persistent Threats," Science J., vol. 1, no. 3, 2012, pp. 93–105.

[6]. T.-F. Yen et al., "Beehive: Large-Scale Log Analysis for Detecting Suspicious Activity in Enterprise Networks," to be published in Proc. Ann. Computer Security Applications Conference (ACSAC 13), ACM, Dec. 2013.

[7]. Bharat Bhargava et al., "Introduction: Securing Big Data Applications in the Cloud", IEEE CLOUD COMPUTING PUBLISHED BY THE IEEE COMPUTER SOCIETY, 2014.

[8]. George F. Hurlburt and Jeffrey Voas, "Big Data Networked Worlds", Published by the IEEE Computer Society, 2014.

[9]. Sumalatha Ramachandran et al., "DATA AGGREGATION AND PRIVACY FOR POLICE PATROLS", International Journal of Ad hoc, Sensor & Ubiquitous Computing, 2011.

[10]. Dinesh B. Raut and PragatiPatil, "Research on Emergency Call and Location Tracking System with Enhanced Functionality for Android", International Journal of Advance Research in Computer Science and Management Studies, 2015.

[11]. Nayot Poolsappasit and Indrakshi Ray, "Towards Achieving Personalized Privacy for Location-Based Services", TRANSACTIONS ON DATA PRIVACY, 2009.

[12]. Chen-Wei Tan et al., "A Glimpse into the Research Space of Location Based Services", JOURNAL OF ADVANCES IN INFORMATION TECHNOLOGY, 2012.

[13]. John Krumm, "A survey of computational location privacy" Persvasive Ubiquitous Computing, Springer, 2009, pp. 391–399.

[14]. Marc Langheinrich, "Privacy in Ubiquitous Computing", John Krumm (ed.): Ubiquitous Computing, Chapman & Hall / CRC Press, Sep. 2009.