International Journal of Computer and Communication Technology

Volume 5 | Issue 4 Article 9

October 2014

Privacy Preserved Centralized Model for Counter Terrorism

ABHISHEK SACHAN
Computer Science Maulana Azad National Institute of Technology, Bhopal, India,
abhisheksachan.manit@gmail.com

DEVSHRI ROY
Computer Science Maulana Azad National Institute of Technology, Bhopal, India, droy.iit@gmail.com

Recommended Citation
SACHAN, ABHISHEK and ROY, DEVSHRI (2014) "Privacy Preserved Centralized Model for Counter Terrorism," *International Journal of Computer and Communication Technology*: Vol. 5 : Iss. 4 , Article 9.
DOI: 10.47893/IJCCT.2014.1256
Available at: https://www.interscience.in/ijcct/vol5/iss4/9

Privacy Preserved Centralized Model for Counter Terrorism

[1]ABHISHEK SACHAN & [2]DEVSHRI ROY

[1&2] Computer Science Maulana Azad National Institute of Technology, Bhopal, India
E-Mail : abhisheksachan.manit@gmail.com[1], droy.iit@gmail.com[2]

Abstract -Privacy preservation is an important aspect in field of counter terrorism. In the present scenario terrorist attacks are biggest problem for the mankind and whole world is under constant threat from these well-planned, sophisticated and coordinated terrorist operations. Now every country is focusing for counter terrorism. Government agencies are collecting the data from various sources and using that data to connect the dots to detect the terrorist group's activities and prevent the peoples from terrorist attacks. There are some chances that information may be misused by agencies. Different countries are having government agencies which are dealing with the counter terrorism but they are not sharing the data with each other because they don't want to disclose sensitive data. Alone a country can't fight against the terrorism. In this paper we are proposing a model so that these agencies can share the information without violation of the privacy.

Keywords - *privacy preservation; counter terrorism, data mining; surveillance.*

I. INTRODUCTION

Today, terrorist attacks are biggest problem for the mankind and whole world. Terrorists are those individuals who plan, participate in, and execute acts of terrorism. According to Brian Jenkins of the Rand Corporation terrorism is "the calculated use of violence such as fear, intimidation or coercion, or the threat of such violence to attain goals that are political, religious, or ideological in nature. Terrorism involves a criminal act that is often symbolic in nature and intended to influence an audience beyond the immediate victims."[1].

Counter-terrorism is the practices, tactics, strategies, and techniques that governments, militaries and police uses to prevent or in response to terrorist threats, both real and imputed. Counterterrorist operatives are engaged in the battle against terrorism. They may be agents of a state or country, including intelligence agents, investigators, and military personnel; or they may be law enforcement officers working at state or local levels. Some time private security and corporate security personnel may also be engaged in counterterrorism operations [1].

The term privacy is used frequently in ordinary language, until now there is no single definition of privacy [10]. The concept of privacy has broad historical roots in sociological and anthropological discussions about how extensively it is valued and preserved in various cultures [11]. Historical use of the term is not uniform, and there remains some confusion over the meaning, value and scope of the concept of privacy [13]. Privacy refers to the right of users to conceal their personal information and have some degree of control over the use of any personal information disclosed to others [12].

Security and privacy are related to each other we have to develop the system with privacy-protection technologies to protect civil liberties. Coordinated policies can help bind the two to their intended use [18]. Privacy-preserving is an important concern in the application of data mining techniques to datasets. Datasets contain personal, sensitive, or confidential information. Data distortion is a technique to preserve privacy in security-related data mining applications, such as in data mining-based terrorist analysis systems [2].

Today, data is one of the most important corporate assets of companies, governments, and research institutions [3] and is used for various private and public interest. The use of data mining technologies in counter terrorism and homeland security has been flourishing since the U.S. Government encouraged the use of information technologies [4]. Government access and use of personal information in commercial databases raise concerns about the protection of privacy and due process [5].

Data can be collected at a centralized location or collected at different locations, but integrated at a centralized location (data warehousing). Alternatively, data can be collected and stored at distributed locations. Different data storage patterns may have different privacy concerns. If the data

storage is centralized, the major privacy concern is to shield the exact values of the attributes from the data analysts. Thus, data distortion is a technique that is usually considered in such a situation [6, 7]. On the other hand, in a distributed database situation, the major privacy concern is to maintain the independence of the distributed data ownership and to prevent the exchange of exact values of the attributes between different parties of the distributed database ownership. This concern is related to the issue of data mining in a distributed environment [2, 8, 9].

It is necessary that data mining technologies designed for counterterrorism and security purpose have sufficient privacy awareness to protect the privacy of innocent people. Unfortunately, most existing data mining technologies are not very efficient in terms of privacy protections, as they were originally developed mainly for commercial applications, in which different organizations collect and own their databases, and mine their databases for specific commercial purposes. In the cases of security and counterterrorism, data mining may mean a totally different thing. Government may potentially have access to any databases and may extract any information from these databases. This potentially unlimited access to data and information raises the fear of possible abuse [2].

Telephone companies are sharing the telephone records of millions of peoples with the security agency. Security agency can use this information to create a database of detailed information for every telephone call made within the country. Intelligence agency then mined this database to uncover hidden terrorist networks [14].

People expect from their government to protect them from enemy attacks along with their civil liberties and privacy. Personal privacy is only violated if the violated party suffers some tangible loss, such as unwarranted arrest or detention. Privacy-protection technology is a key part of the solution not only to protect privacy but also to encourage the intelligence, law enforcement, and counterterrorism communities to share data without fear of compromising sources and methods [18].

Advanced information technologies offer key assets in confronting a secretive, asymmetric, and networked enemy. The policies must ensure that these powerful technologies are used responsibly and that privacy and civil liberties remain protected. People expect from their government to protect them from terrorist attacks, but fear the privacy implications of the government's use of powerful technology controlled by regulation and oversight. Some people believe the dual objectives of greater security and greater privacy present competing needs and require a trade-off; others disagree [15, 18, 19, 21].

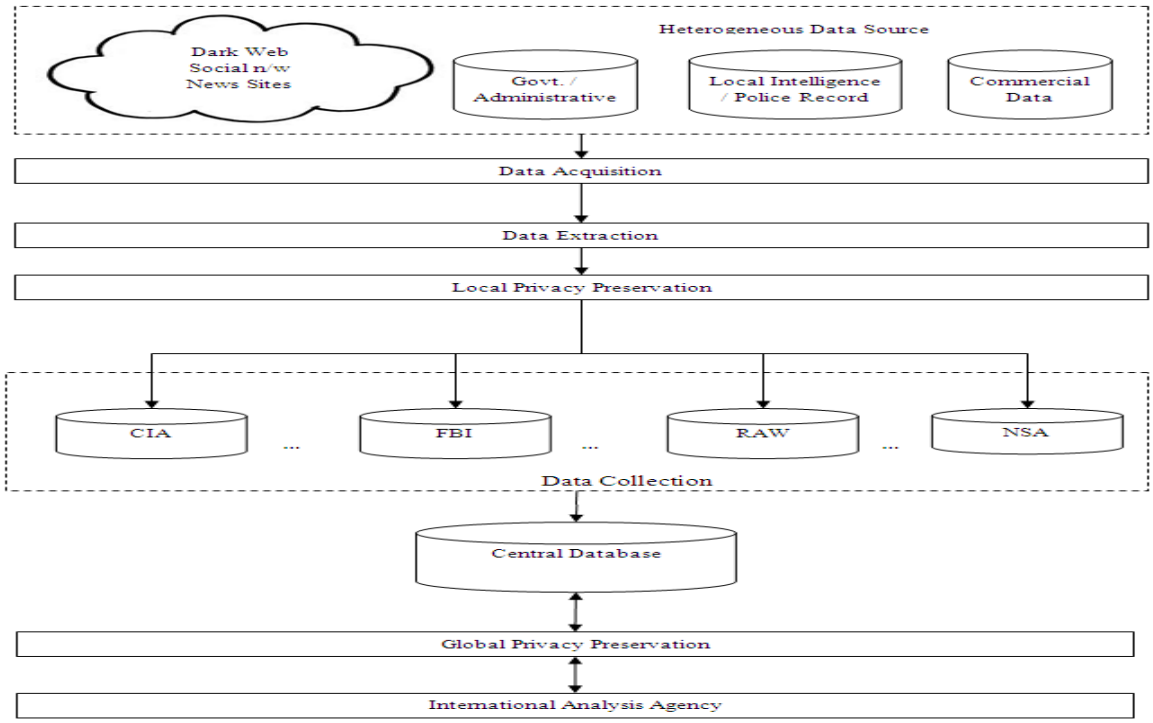

Figure 1. Privacy Preserved Centralized Model for Counter Terrorism

II. MODEL ARCHITECTURE

Privacy Preserved Centralized Model is proposed for Counter Terrorism. When we are discussing about counter terrorism one problem is coming that how can we allow our government agencies to perform surveillance over us. People believe that their privacy may be violated. Another problem is that different countries are having security agencies which are dealing with the counter terrorism but they are not sharing the data with another country because they don't want to disclose their sensitive data.

In this model we have tried to protect the privacy of individual along with the privacy of country's data so that data could be shared without violating privacy. Local privacy preservation module is use to preserve the privacy of the people's during surveillance & data collection. Government security agencies are increasingly moving towards data mining with the hope that advanced statistical techniques will connect the dots and uncover important patterns in large databases. Data surveillance technology is able to predict and prevent terrorist attacks, detect disease outbreaks, and allow for detailed social science research—all without the corresponding risks to personal privacy because machines, not people, perform the surveillance [14].

In this model central data mining concept is use, to solve the second problem of sharing the data between countries. Central database is the database in which data available all over the world is stored. International analysis agency is third party. No country can directly access this data. Agency will perform mining over this central data and return the desired data to the requested country. Even agency can't violet the privacy because it is restricted with the global privacy policies.

There are various privacy preservation techniques and technologies that can be applied over local and global privacy preservation modules. Privacy Appliance, Transformation Spaces, Immutable Audit, Selective Revelation, Self-Reporting Data, Anonymization and Inference Control are some privacy protection technologies [18]. Privacy preservation data mining techniques are k-anonymity, l-diverse, taxonomy tree, randomization, perturbation, condensation and cryptographic etc. that can be used based on the requirement [16, 17, 20, 22, 23].

III. CONCLUSION

We can say that by using this model security agencies can perform surveillance and data collection for counter terrorism without the violation of individual's privacy. This model helps to share data between agencies/countries without disclosure of country specific sensitive information. This model is uses both centralized and distributed data mining concept. Now the performance of the model is dependent on privacy preservation technique. If we will use strong/secure techniques in the model for privacy preservation then model will be strong/secure else weak.

REFERENCES

[1] Frank Bolz, Jr., Kenneth J. Dudonis, David P. Schulz, "The Counterterrorism Handbook Tactics, Procedures, and Techniques", In CRC Press, 2002.

[2] Shuting Xu, Jun Zhang, Dianwei Han, JieWang, "Singular value decomposition based data distortion strategy for privacy protection", In Knowledge and Information Systems, March 2006.

[3] Estvill-Castro V, Brankovic L, Dowe DL, Privacy in data mining. Australian Computer Society, NSW Branch, Australia. Available at w.acs.org.au/nsw/articles/ 1999082.html, 1999.

[4] Taipale KA, "Data mining and domestic security: connecting the dots to make sense of data", In Columbia Sci Tech Law Rev 5, 2003, pp. 1–83.

[5] Dempsey JX, Rosenzweig P, "Technologies that can protect privacy as information is shared to combat terrorism", Legal Memorandum #11, The Heritage Foundation. Available at www. heritage.org/ Research/ HomelandDefense/ lm11.cfm, 2004

[6] Agrawal D, Aggarwal CC, "The design and quantification of privacy preserving data mining algorithms", In Proceedings of the 20th ACM SIGACT-SIGMOD-SIGART symposium on principles of database systems, Santa Barbara, California, USA, 2001.

[7] Liew CK, Choi UJ, Liew CJ, "A data distortion by probability distribution", In ACM Transaction Database System,1985, pp. 95–411.

[8] Agrawal R, Evfimievski A, Srikant R, "Information sharing across private databases", In Proceedings of the 2003 ACM SIGMOD international conference on management of data, San Diego, CA, 2003, pp. 86–97.

[9] Gilburd B, Schuster A, Wolff R, "K-TTP: a new privacy model for large-scale distributed environments", In Proceedings of the 10th ACM SIGKDD international conference on knowledge discovery and data mining, Seattle, WA, USA, 2004.

[10] J.DeCew, privacy, The Stanford Encyclopedia of Philosophy, Editor:Edward N.Zalta, Summer 2002.

[11] A. F. Westin, The Right to Privacy, Atheneum 1967.

[12] S. Cockcroft and P. Clutterbuck, "Attitudes towards information privacy", In Proceedings of the 12th Australasian Conference on Information Systems, Australia, 2001.

[13] Justin Zhan, "Privacy Preserving Collaborative Data Mining", In IEEE, 2007.

[14] Simson L. Garfinkel, Michael D. Smith, "Data Surveillance" , In IEEE SECURITY & PRIVACY,2006,pp.15-17.

[15] R. Popp and J. Yen, eds., "Emergent Information Technologies and Enabling Policies for Counter-Terrorism", In Wiley & Sons/IEEE Press, 2006.

[16] PinkasB., "Cryptographic Techniques for Privacy-PreservingDataMining" In ACM SIGKDD Explorations, 4(2), 2002.

[17] S. Laur, H. Lipmaa, and T. Mielik¨ainen, "Cryptographically private support vector machines", In Twelfth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2006, pp. 618–624.

[18] Robert Popp, John Poindexter, "Countering Terrorism through Information and Privacy Protection Technologies", IEEE SECURITY & PRIVACY, 2006, pp.18-27.

[19] Report to Congress Regarding the Terrorism Information Awareness Program, DARPA, May 2003; [response to Consolidated Appropriations Resolution, Pub. L. no.108-7, div. M, sec. 111(b), 2003].

[20] Charu C. Aggarwal and Philip S. Yu, "A condensation approach to privacy preserving data mining", In EDBT, 2004, pp. 183–199.

[21] J. Poindexter, "Overview of the Information Awareness Office," In DARPATech 2002, DARPA,2002, www.fas.org/irp/agency/dod/poindexter.html.

[22] Machanavajjhala A., Gehrke J., Kifer D., and Venkitasubramaniam M, "l-Diversity: Privacy Beyond k-Anonymity", In ICDE, 2006.

[23] E.Poovammal ,Dr. M. Ponnavaikko, "An Improved Method for Privacy Preserving Data Mining", In IEEE International Advance Computing Conference Patiala, India, 2009.