Journal of Advances and Scholarly Researches in Allied Education
Vol. XV, Issue No. 5, July-2018, ISSN 2230-7540

Analysis on Investigative Data Mining in the Counter-Terrorism, Technology and Transparency

Sanjay Dwivedi[1]* Dr. Prabhat Pandey[2]

[1] Research Scholar

[2] OSD Additional, Directorate of Higher Education Rewa Division

Abstract – Data mining and data investigation is distinguishing, assembling, and handling the data that was broke down. To do this requires first recognizing what the investigation was expected to find and the kind of data that will be valuable. This isn't generally a straightforward errand. For data mining, analysts have created methods for "dynamic realizing" that can discover data that would be valuable to gather. The data mining process itself was regularly help with distinguishing sorts of data that are not valuable. One regular fantasy about data mining and computerized data investigation was that they expect data to dwell in one expansive database.

Keywords: Data Mining, Counter-Terrorism

----------X----------

1. INTRODUCTION

Data mining is the way toward posturing inquiries and removing helpful examples or patterns frequently already obscure from a lot of data utilizing different procedures, for example, those from design acknowledgment and machine learning. There have been a few advancements in data mining and the innovation is being utilized for a wide assortment of uses from showcasing and back to pharmaceutical and biotechnology to sight and sound and diversion. As of late there has been much enthusiasm on investigating the utilization of data digging for counter-fear mongering applications. For instance, data mining can be utilized to recognize bizarre examples, fear monger exercises and deceitful conduct. While these utilizations of data mining can profit people and spare lives, there is likewise a pessimistic side to this innovation, since it could be a danger to the security of people. This is on account of data mining devices are accessible on the web or generally and even nave clients can apply these devices to separate data from the data put away in different databases and documents and thusly damage the security of the people. To do powerful data mining and concentrate valuable data for counter-psychological warfare and national security, we have to assemble a wide range of data about people.

The quick development of accessible data in all areas of society requires new computational strategies. Other than customary factual strategies and standard database approaches, ebb and flow look into known as Investigative Data Mining (IDM) utilizes current techniques that begin from inquire about in Algorithms and Artificial Intelligence. The principle objective is the mission for intriguing and justifiable examples. This pursuit dependably been and will dependably be basic undertaking in law implementation, particularly for criminal examination, and more particular for the battle against fear based oppression. IDM is characterized as: "The method which models to data to anticipate conduct evaluates chance, decide affiliations and help in killing the fear based oppressor arrange"

In the region of law implementation the requirement for IDM is clear in perspective of gigantic heap of data that is (and can be made) accessible these days.

Test is mining data continuously. The test is to have the capacity to make deductions about missing hubs and connections in the chart. Likewise the chart could be substantial. The inquiry is how might one diminish the diagram to a more sensible size? At long last finding the data to test the thoughts is as yet a noteworthy test. How might we get unclassified data? Is it conceivable to scour and clean the arranged data and create sensible data at the unclassified level? How might we discover substantial dataal indexes comprising of sight and sound data write? Is it conceivable to build up a

proving ground where one can apply the different data mining devices to decide their productivity? Web digging is a test for identifying strange examples. In a way web mining envelops data mining as one has to mine every one of the data on the web and in addition mine the structure and use designs. By mining the utilization designs one could get examples, for example, there are a surprising number of visits to a government site from Paris around 3am early in the day. Data on the web incorporates organized and additionally unstructured data. In this way the devices created for data digging apply for web mining too. What's more, we require apparatuses to mine the structure of the web and additionally the utilization designs. Protection is a noteworthy test as for data digging for counter-fear based oppression. The test is to remove valuable data from data mining however in the meantime look after protection. A few endeavors are in progress for security protecting data mining. The thought here is to utilize different systems, for example, randomization, main stories, and multi-party approach requirement for protection saving data mining. While there is some advance, the adequacy of these procedures should be resolved. The above are a portion of the difficulties for data digging for counter-fear based oppression talked about at the workshop. That is, while data mining could turn into a helpful instrument for counter-psychological oppression, there are numerous difficulties that should be tended to. They incorporate mining mixed media data, diagram mining, building models continuously, learning guided data mining to dispose of false positives and false negatives, web mining, and protection touchy data mining. Research is advancing the correct way. Be that as it may, there is still much to be finished.

2. REVIEW OF LITERATURES

National Counter Terrorism Center of India (2013): Data mining is moderately new innovation in the nation however it has been being used in the greater part of the propel nation, Data mining is a promising device in the battle against psychological warfare, It as of now plays various imperative parts in counter fear mongering including finding known suspects, distinguishing and following suspicious budgetary and different exchanges, and encouraging record verifications.

DeRosa (2004): brought up that robotized data examination strategies can be helpful apparatuses for counterterrorism in various ways. One starting advantage of the data investigation process is to aid the imperative undertaking of precise distinguishing proof.

Column, P.R. (2004): There are currently a few noteworthy databases on fear monger episodes put away at scholastic organizations like the University of Maryland (START) and at government offices like the US Homeland Security Agency. Occasion data on fear based oppressor prisoner episodes are given by 'Universal psychological warfare: properties of psychological militant occasions', which was initially amassed by Mickolus (1982) and later refreshed. This database records transnational psychological militant episodes and in this manner overlooks supposed 'residential fear based oppression'.

B. Thuraisingham (2003): positions data mining as a key element in the battle against fear mongering and wrongdoing Data mining is developing as one of the key highlights of numerous country security activities. Specialist said data mining can be utilized to recognize surprising examples, fear based oppressor exercises and deceitful conduct. Data mining has been expanding supporting the law implementation offices in the battle against fear based oppression. This lead the United States of American's legislature in the wake of 9/11 to build up the Total data Awareness later renamed the fear monger Data Awareness, however both program has since been suspended noted Seifert.

B. Thuraisingham(2003): said that data mining created as another train for a few reasons. Helping data mining in countering fear based oppression is anyway because of the expansion in speed of PCs preparing power, the declining expense of innovation too.

C. Clifton, M. Kantarcioglu, and J. Vaidya(2002): Game theoretic methodologies have been utilized to dodge the issue of data quality. The way that legislatures and psychological oppressors (groups) strategize has been considered, for example, to clarify why fanatic gatherings regularly increment fear based oppressor movement after an administration has made concessions to direct groups. These outcomes have yielded imperative experiences about psychological oppression in India and different nations; however they are not by and large inspired by ordinary data investigation.

F. Bolz (2001): Another approach is to construct models of systems of psychological militant and fear based oppressor associations. In spite of the tradition that fears based oppressors ought not to be dealt with as unitary performers, the investigation of psychological militant associations as systems is less created. Informal organization examiners have found that undercover associations have a tendency to be cell and conveyed as opposed to various leveled, and the administration has bolstered research to show these as standard systems through the National Research Council.

R. Agrawal and R. Srikant(2000): The International Policy Institute for Counter-Terrorism in Herzlia, Israel, gives an dataal index of psychological militant assaults in Israel. The US Department of Homeland Security underpins the National Memorial Institute for the Prevention of psychological warfare learning base, which gives on line a posting of fear mongering episodes with data on the psychological oppressors and an

accentuation on legitimate data. Another on-line posting is the worldwide fear mongering database (GTD) which incorporates data on worldwide psychological oppressor occasions beginning from1970. Scientists have utilized these fundamentally to create synopsis measurements and essential unthinkable examinations. Standard measurable demonstrating has yielded a few bits of knowledge into the determinants and timing of psychological oppressors' episodes.

3. COUNTER TERRORISM

Pattern based examination may likewise have potential counterterrorism employments. Pattern based questions take a prescient model or pattern of conduct and look for that pattern in dataal indexes. In the event that models can be culminated, design based quests could give signs to "sleeper" cells made up of individuals who have never occupied with movement that would interface them to known psychological oppressors. The potential advantages for counterterrorism are huge. However, when the legislature can break down private data a lot more adequately, that data could turn out to be more alluring, and the administration's capacity to influence the lives of people can increment. There is noteworthy open unease about whether securities for protection are sufficient to address the negative results of expanded government utilization of private data. These worries are uplifted on the grounds that there is so small comprehension of how the legislature may utilize these data investigation instruments. Nor is there commonly much open civil argument or talk before these devices are received. This absence of straightforwardness not exclusively can settle on the administration's choices less educated, yet it expands open dread and misjudging about employments of these strategies. Maybe the most critical worry with data mining and computerized data examination is that the legislature may fail to understand the situation, and blameless individuals will be slandered and troubled.

This is the issue of "false positives"— when a procedure mistakenly reports that it has discovered what it is searching for. With these devices, a false constructive could imply that as a result of awful data or defective hunt models a man is erroneously distinguished as having a fear based oppressor association. In any case, regardless of whether comes about are exact, governments components are at present lacking for controlling the utilization of these outcomes. On the off chance that they are not controlled, private data can be utilized shamefully, there are no unmistakable rules now for who sees private data, for what reasons, to what extent it is held, and to whom it is scattered.

A related concern is "mission crawl"— the propensity to grow the utilization of a questionable strategy past the first purposes. Utilization of questionable apparatuses might be regarded adequate given the potential damage of cataclysmic fear mongering; however there will then be an incredible compulsion to extend their utilization to address other law implementation or societal concerns running from the genuine to the trifling.

One critical road for tending to a significant number of these difficulties to protection and freedoms, at any rate to some extent, is innovation. Some security ensuring innovation is as of now accessible and substantially more is being investigated. Specialists are taking a gander at techniques to culminate look models and purify data to lessen false positives: "anonym zing" innovation intended to veil or specifically uncover recognizing data so the administration can direct inquiries and offer data without knowing the names and characters of Americans; review innovation to "watch the watchers" by recording movement in databases and systems to give powerful oversight; and lead handling or permissioning innovation that guarantees that data can be recovered just in a way that is reliable with protection shields and different standards. In spite of the fact that this innovation can address a portion of the dangers with utilization of datamining and mechanized data examination procedures, it won't be sufficient all alone. Arrangement activity is expected to guarantee that controls and securities go with utilization of these intense devices. The approach issues that require consideration include: •

Research on data mining and robotized data investigation: Data-mining and computerized data examination instruments have awesome potential for counterterrorism, however to understand that potential completely, more research is required. The legislature should bolster this exploration. An administration arrangement for this exploration should consider the setting in which these apparatuses may in the end be conveyed. This implies inquire about on security ensuring innovation and even some investigation of protection arrangement issues ought to be incorporated. •

Lucidity about utilization of data mining and mechanized data examination: One of the central explanations behind open worry about these apparatuses is that there seems, by all accounts, to be no steady strategy controlling choices about when and how to utilize them. Approaches for data mining and mechanized data examination methods should set forward guidelines and a procedure for basic leadership on the kind of data investigation system to utilize—subject based or pattern based, for instance—and the data that will be gotten to. They should command investigation into data precision and the level of blunders that the

examination is relied upon to create, and they ought to expect government to set up an instrument for amending mistakes before activities start. •

Utilization of list items: There ought to likewise be a steady approach on what move can be made in view of query items. At the point when computerized data examination comes about are utilized just to encourage investigation and examination, and not as the sole reason for confinement or some other government activity, there are less conceivable negative outcomes for people. Along these lines, direction is vital on the conditions, assuming any, under which results can be utilized as the reason for activity. •

Controls on the utilization of distinguishing data: Currently no reasonable direction exists for government substances and workers about how to deal with private data, and this absence of course can prompt oversights and conflicting utilization of data. Maybe the most essential advance to address protection worries with the utilization of data mining and mechanized data examination is for the official branch to actualize clear rules for government workers on how they may get to, utilize, hold, and spread private data.

4. COUNTER-TERRORISM, TECHNOLOGY AND TRANSPARENCY

In the battle against psychological oppression innovation is a great instrument. Be that as it may, as the European Group of Personalities in the field of Security expressed "innovation itself can't ensure security, however security without the help of innovation is unimaginable" (European Communities, 2004, p.12).

This statement shows how from one viewpoint data and interchanges innovation (ICT), biotechnology, neuroscience and nanotechnology add to the improvement of vital counter-fear based oppressor systems and then again that we ought to be practical about their effect. There are no simple, speedy answers for manage the risk of psychological oppression. Osama receptacle Laden, for pattern, was found based on human insight. Simply after his conceivable area in Abbottabad in Pakistan was followed, did innovation including satellite reconnaissance, Forward Looking Infrared Devices (FLIR) and biometric Secure Electronic Enrolment Kits (SEEKs) assume a part in recognizing movement in the compound and in distinguishing the Al Qaeda pioneer? Expanding mechanical advancements and in addition contemporary security concerns, for pattern, universal psychological warfare appear to legitimize the utilization of creative devices. All things considered, fear mongers draw on current innovation, particularly the web (Fenwick, 2011; European Council 2009).

Digital assaults on basic foundation, for pattern, vitality or correspondence systems, state PC systems and so forth., prompt new complex national security dangers. In this manner, by utilizing mechanical security devices the state is basically changing in accordance with contemporary societal improvements. Be that as it may, what recognizes the state from others, for pattern, private elements is their restraining infrastructure on the utilization of power and its insurance of the govern of law. Moreover, security advancements are potential ground-breaking methods for social control by the state and there are predicted and unanticipated social results to their utilization (Bruggeman, 2011).

On the off chance that there are, for pattern, no appropriate balanced governance in connection to new mechanical counter-fear based oppression instruments, there is a hazard that, to cite Mathiesen (1997), a procedure of 'panoptic' reconnaissance creates, where the few – for this situation the state – ceaselessly keep under perception the many – the general population – (Cohen, 1995; Foucault, 1979). This encourages the making of a purported 'reconnaissance society' , where the accumulation of individual data influences everyone, potential psychological militants and additionally common individuals who risk being – preventively – named a danger to national security or open request.

5. PATTERN-BASED DATA ANALYSIS: POTENTIAL FOR COUNTERTERRORISM

Pattern based data investigation likewise has potential for counterterrorism in the more drawn out term, if look into on employments of those procedures proceeds. As will be examined in more detail in the following area, data mining research must discover approaches to recognize valuable patterns that can anticipate a to a great degree uncommon action—fear based oppressor arranging and attacks.18 It should likewise distinguish how to isolate the "flag" of pattern from the "clamor" of guiltless movement in the data. One conceivable favorable position of pattern based inquiries—in the event that they can be idealized—would be that they could give pieces of data to "sleeper" movement by obscure psychological oppressors who have never occupied with action that would connect them to known fear based oppressors. Not at all like subject-based questions, design based hunts don't require a connection to a known suspicious subject.

Sorts of pattern based pursuits that could demonstrate valuable incorporate scans for specific blends of lower-level movement that together are prescient of psychological oppressor action. For instance, a pattern of a "sleeper" fear based oppressor may be a man in the nation on an understudy visa who buys a bomb-production book and 50 medium-sized heaps of compost. Or on the other hand, if the worry is that fear based

oppressors will utilize vast trucks for assaults, robotized data investigation may be led routinely to distinguish individuals who have leased extensive trucks, utilized lodgings or drop boxes as addresses, and fall inside specific age goes or have different characteristics that are a piece of a known psychological oppressor design. Huge patterns in email movement may be found that could uncover fear monger action and psychological oppressor "instigators."

Pattern based inquiries may likewise be exceptionally valuable accordingly and outcome administration. For instance, scans of healing facility data for reports of specific mixes of manifestations, or of different databases for patterns of conduct, for pattern, pharmaceutical buys or work non-appearance may give an early flag of a fear monger assault utilizing an organic weapon.

6. THE PROCESS

Despite the fact that there are evident potential advantages of data mining and mechanized data examination systems, it is critical to have a comprehension of the procedure utilized as a part of those practices and the dangers of mistake and interruptions on protection. This area gives an essential portrayal of how these methods function.

► Gathering and Processing the Data

The initial step for data mining and data examination is distinguishing, assembling, and handling the data that will be investigated. To do this requires first recognizing what the examination is expected to find and the sort of data that will be helpful. This isn't generally a straightforward assignment. For data mining, analysts have created methods for "dynamic realizing" that can discover data that would be valuable to gather. The data mining process itself will regularly help with distinguishing sorts of data that are not valuable.

One basic legend about data mining and mechanized data investigation is that they expect data to dwell in one huge database.

Normally, data for data mining have been consolidated into a solitary database, called an data distribution center or data shop, for mining. There are preferences to this approach—it takes into account more productive hunting and down simpler institutionalization and purifying of the data—however it isn't important.

Data mining can be led over various databases of shifting sizes; gave that specific low size edges are surpassed to give measurable legitimacy. The same is valid for robotized data investigation. The Treasury Department's Financial Crimes Enforcement Network, for instance, has led data examination to reveal illegal tax avoidance action utilizing an essential interior data distribution center and various optional databases.

Dispersed engineering can have a few points of interest for protection and database security since it enables diverse access and security guidelines to be connected to the distinctive databases and furthermore takes into account disseminated control of database get to, which decreases the open doors for abuse.

The last advance in this first stage is changing the data to make them helpful. This is regularly alluded to as "data accumulation." This progression includes gathering the data, "purifying" them to take out repetitive and other unusable data, and institutionalizing them to make looks more precise. At the point when done well, this procedure has a critical positive effect on the nature of the data mining or data examination item since it lessens data blunders, for pattern, false positives and false negatives. One objective of changing data for data mining is personality determination—deciding if dissimilar character records all speak to one individual or diverse individuals.

7. CONCLUSION

With the rise of advances to counter fear mongering, concerns have emerged in connection to states responsibility. New advancements have expanded the scope of accessible potential outcomes for the state to ensure national security. Numerous individuals are, be that as it may, unconscious of the social (side-) impacts of mechanical counter-psychological warfare measures. These worries are incompletely tended to by concentrating on the governing rules, which infers that open specialists are considered responsible for their laws, directions, strategies and activities and are authorized as needs be. This likewise applies to a state's obligation to manage private substances. In general the 'new' advancements that were talked about here are thought to be valuable apparatuses in the battle against psychological oppression.

REFERENCES

B. Thuraisingham (2003): Web Data Mining Technologies and Their Applications in Business Intelligence and Counter-terrorism. CRC Press

Bruggeman, W. (2011) : The Boundaries and the Future of Technological Control: Technological control has its limits on ethical ground, but also from a social

control point of view', In: E. de Pauw, P. Ponsaers & K. van der Vijver (Eds.), Technological-Led Policing, Cahier Politiestudies 20, 3, (2011), pp. 125-163.

C. Clifton, M. Kantarcioglu, and J. Vaidya (2002): Defining privacy for data mining. Technical report, Purdue University

Choudhury, Tufyal & Helen Fenwick (2011) : The Impact of Counter-terrorism Measures on Muslim Communities, Equality and Human Rights Commission Research Report Series, 72, Manchester, Equality and Human Rights Commission, p. 36

Cohen, S. (1985): Vision of Social Control: Crime, punishment and classification, Cambridge

European Council (2009). 'The Stockholm Programme: an Open and Secure Europe Serving and Protecting Citizens', Official Journal of the European Union (Publication 14449/09) retrieved on 4-6-2010 from http://register.consilium.europa.eu/pdf/en/09/st14/st14449.en09.pdf

European Parliament Committee on Civil Liberties, Justice and Home Affairs (2011), the EU Counter-Terrorism Policy: Main Achievements and Future Challenges, A7-0268/2011 Draft Report of 20 July 2011

F. Bolz (2001): The Counter terrorism Handbook: Tactics, Procedures, and Techniques. CRC Press

Foucault, M. (1979): Discipline and Punish: The birth of the prison, New York: Vintage.

Mary De Rosa (2004): Data Mining and Data Analysis for Counterterrorism, Center for Strategic & International Studies.

Mathiesen, T. (1997): "The Viewer Society: Michel Foucault's 'Panopticon' revisited", Theoretical Criminology, 1, 2, pp. 215- 234.

National Counter Terrorism Centre of India (2013): The Problems and Solutions", Centre of Excellence for Cyber Security Research and Development in India (CECSRDI), 3 February. Retrieved 24 August 2014

Pillar, P.R. (2004): Counterterrorism after al Qaeda. The Washington Quarterly 27(3), pp. 101–113

R. Agrawal and R. Srikant (2000): Privacy-preserving data mining. In Proceedings of the ACM SIGMOD Conference, Dallas, TX

Corresponding Author

Sanjay Dwivedi*

Research Scholar

E-Mail – ipssidhi@gmail.com