IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Special Issue-14, May 2019 E-ISSN: 2347-2693

Analysis of Security Threats using Machine Learning and Cloud Computing Technology

Prajwal Kulkarni[1*], Sneha Pattar[2], Gopal Krishna Shyam[3]

[1,2]CSE, School of Computing and It Reva University, Bangalore, India
[3]School of Computing and II, Reva University, Bangalore, India

[*]*Corresponding Author: praju.9741@gmail.com Tel.: +7204774630*

DOI: https://doi.org/10.26438/ijcse/v7si14.3235 | Available online at: www.ijcseonline.org

***Abstract*—** Theatrical Events of fear like Terrorism based operations have be sighted everywhere throughout the world. This surveillance system analyses and speculates the possible suspects depending upon their conducts, records them into Watch-List, classifies them and stores their images in the Government cloud. Whenever the suspects in the Watch-List land at any Local camera resembling movement cams, Metro stations and Airports which are served by the government cloud, it recognizes them using facial recognition software.
Instantly the framework alarms the experts and significant information is sent to the Military Intelligence. Based on the rundowns and photos gathered by the Military surveillance systems, they coordinate with the machine which utilizes facial acknowledgment programming to perceive the suspects in nearby reconnaissance cameras which are served by the administration cloud. The most problems faced is issues of privacy, there is a strict law for invading of public privacy just on suspicion without any proof. Hence its not possible for putting a surveillance on any individual. This machine resolves as it provides physical proofs of why that individual is being surveillance, moreover even common crimes within the city could be stopped by the local authority as facial recognition spots this individual in any camera. The application of this machine is limitless as terabytes of data is available in the local cloud just the accumulating this data and processing through proper channel is necessary

***Keywords*—**Terrorism, machine learning, Local Cloud, Government Cloud

I. INTRODUCTION

The need of a new means to combat terrorist threats is growing every day because danger is developing each day on account of proceeds with assaults inside the regular citizen regions. Most terrorists are not known, they are not part of any country. They live in shadows, their targets are unknown, their identities are similar as citizens that is why it's very hard to differentiate them from the civilians.

This is where surveillance systems are introduced, but living in such intense population it's nearly impossible to watch out for each individual. Therefore, Military intelligence brought in intelligent systems with information extraction technology. Surveillance systems however depend on the data of Military Intelligence server. And image created on their schematics. Data mining and automated data analysis are used to create their identities. It is suggested that these techniques be explored as the potential use in the terrorism domain. The most important aspect we have to consider is that only data available in their cloud is not enough to make the list of possible threats.

Most of the intelligent systems matched only the criteria which only Military intelligence have collected and do not use Machine learning and Artificial Intelligence to foresee results for the more prominent dangers. Learning each move of the terrorist exercises will give information for the following target and Counter Terrorism can stop the assault before it occurs.

Therefore, there is need of Intelligent Surveillance Systems within the City and Surveillance cameras watching every major public place 24/7. There is also need of data gathering separately and processing it to create a "watchlist", but with this machine there is no need to accumulate as data is already available in their department example, Financial Regulatory bodies will have data of Fraud money laundering Local police will be having data of criminals within their locality, Cyber security Division will have information about individuals visiting the suspicious IP and so forth. Collection of all these data and making a facial identity of this individual and dump in the watch-list. Significant work here is done, all its left is to coordinate these people in any open camera and local authorities will be alerted. some of the techniques used to make this machine work.

II. RELATED WORK

Other countries National Security build an Intelligent Surveillance which was working on biases of Link Analysis. It involves detecting association between entities. Many association-rules based techniques exist, possessing varying degrees of 'intelligence'. Link analysis in the diagram causes one to outwardly distinguish unusual examples and practices. Research on connection investigation has been around since the Internet web search tool was conceived.

Intelligent systems cross verified any Person located on any camera to the possible threat which they had in their database and furthermore this system would continue surveillance on them on basis of doubts of local authorities or information gained from the Information Extraction Algorithms from their System, there were few issues about the privacy and it was difficult to filter from the whole lot of population [2].

III. METHODOLOGY

1.Link analysis
Link analysis concept is introduced which uses relations or certain patterns to locate the terrorists. Not only this technique is used in the Military intelligence cloud but also The Local cloud which can detect certain pattern.

2. Artificial Intelligence
Introducing AI in the Intelligent Systems along with the Link Analysis will help this machine to predict and identify the possible suspects. This machine extracts information of the behavior of an Individual, the unusual behavior of any Civilian is recorded and matched with the behavior training data-set that is stored in the Machine, if the new data-set is matched then this will result in creating of identity and this identity will be sent to Counter Terrorism Cell.

3. Area surveillance
The helpfulness of CCTV is seriously endangered by human checking. People are extremely poor at screens and also have trouble of staying alarm for extensive stretches of time. Therefore this system has encoded facial recognition software to CCTV cameras. Facial Recognition software in the local cameras which automatically recognize the possible threat suspects and flags them, their identity is created by the facial recognition software and these id's will be sent to local Authorities this will make them easy to track them.

4. Personal Identity
Adhar Card in India and Social security number in other various countries is one of the method to create identities in this machine, as there face to their finger print is recorded in the data base any Individual put in Watch-List the Machine matches their faces with the Govt Personal Identification cards such as Adhar card in India and Social Security numbers in various country becomes easy to create identities, but it does not completely gives an optimal solution as the person within the country is not the terrorist, however it's easy to filter the people in Watch-List based on their Personal Identities so that if any person's records are not found in the government issued Id's it's possible that this individual is a possible threat.

5. Social Media
[6]The era of social network has been easy to track people link analysis allows you to connect the dots while creating the identities.[6] Whenever any person is dropped into Watch-List or Terrorist-Watch List, its mandatory to create their identities, based on facial recognition the Machine targets faces if there is a face matching available in the social network.
The machine uses data mining techniques and link analysis to find any pattern of their face, not only that the interest of an individual and tracking their footprint via social media is very easy and it also provides brief details about their community circle and what kind of people they in contact with. However, making identities based on social media is not possible considering there are millions of users and there could be possibilities of gathering information on fake profiles and end up building false identities, therefore creating identities of suspected people out of social media is a small thread program in this in this machine

6. Money laundering
Financial organizations and regulatory bodies oversee the financial [1]crimes and frauds. Financial bodies in India are SEBI, RBI, IRDA, PFRDA, Forward Market the financial bodies are independent in India based on banking, insurance, stock market etc.
Terrorists need huge money and this large amount is not overlooked by any financial bodies in India
the problem here is not all the information is shared
how do terrorist get funding the major question lies still unanswered they are well funded by few methods like

1. Charities: - donations are one of the largest sources of funding to the terrorists any wealthy person launder's money in the name of religion or unofficially being part of terrorism activity .

Saudi Arabia is the major source of terrorist funding through charity.

The money laundered is huge and keeping track or identifying such donations and collecting the data of the donator and the receiver is not easily possible. But the financial regulatory bodies have preferences and can locate such money.

2. Illegal activities:- Many terrorist organizations have been funded through illegal activities like Drugs, human trafficking, etc. surviving in the group and providing training requires gigantic cash and drug traffickers launder money in exchange to weapons etc.
3. Front companies: - Numerous Terrorist associations use real organizations favoring their activities. These companies' profits are used as front for money laundering. Business in livestock trading fish leather aimed to support terrorist also, business involved in construction's render huge profits to terrorist organization.
4. Fund Transfer: - These assets are moved in "plain sight". On the off chance that the exchange is occurring through banking, it is done through shell organizations

Another traditional way terrorist use to transfer money is through Hawalas. These are the most trusted commendable agencies famous in Asia, who are spread all through the world is their most utilized approach to exchange cash. Just with a handshake and listening to a specific password theses agencies are able to exchange money

6.1 Problems in detecting these frauds

The major problem is lack of technology which can detect such fraud money, as there is huge population growing and different religion, cast ,color all mixed together

The real issue is absence of technology which can distinguish such fraud money as there is huge population growing and diverse religion, cast, shading all combined in countries like India, it's very difficult for Financial regulatory organizations to detect such illegal money and more difficult to know if this money is used for terrorist organization.

Another major problem is Terrorist are aware of how these Financial regulatory function they have first-hand knowledge of these regulatory bodies monitoring the illegal money therefore terrorist began to rely on cash leaving less paper trail.

The data is gathered by financial regulatory bodies but not processed or efficiently analyzed as to know for the purpose of these illegal cash which are rendered mostly it is difficult when the money is donated

to overcome this situation this surveillance system uses link analysis technique to detect such money

the money rendered information is available in the Regulatory bodies and the information is fed into this machine, this data is matched with the created Id's of Watchlist and the Terrorist Watchlist.

6. Filtering Civilians from Watch-List and Terrorist-Watch List

Machine filters the Civilians from Watch-List and Terrorist-Watch List, basically to any individual to end up in Watch-List continues surveillance can be done, keeping a track on these Individuals and learning more about them is the first step, then creating their identities and cross verifying them with the Government Issued Identities, if there is no record found about them will directly send their created Identity's like their face, possible names their alias whatever the machine gets data about them from the Link Analysis to the Military Intelligence, here there data is verified with the Terrorist-Watch List data.

If no records are found the Local authorities are warned and are asked to continue the surveillance of this individual. Sometimes there may be possible that Person in Watch-List gets flagged as Terrorist as some pattern will match in the Terrorist-Watch List database created by the Military Intelligence, this could be big win as a terrorist is identified and Counter Terrorism can get directly involved and make an operation to bring him down before he possesses threat to the society

IV. RESULTS AND DISCUSSION

1. Watch List

For this classification the information is acquired by the nearby local surveillance systems, like CCTVs, Metro camera or information gathering objects inside the territory to identify the behavior of the regular citizens and if there is any person's behavior matches the Watch List Training set, immediately that individual is listed in Watch List and could be brought in for questioning by the authorities.

4.1 Training set for WA (Watch list Algorithm)

1. People caught on tapes while taking pictures of security infrastructure
2. Messages to the subspecies Websites
3. Gaining information about locations
4. Purchasing Chemicals in large quantities
5. Producing Different identities
6. Identity not found in any server

2. Terrorist –Watch List

To filter the ordinary civilians from the possible suspects behavior learning algorithms is introduced

This algorithm is fed with training set of possible terrorist behavior, not just that even people aiding and abiding who are put into directly Terrorist-Watch List

But the data is obtained by the Military Intelligence Server

5.1 Training set of TWA(Terrorist-Watch list Algorithm

1. Material support
2. Tracing credit card frauds
3. Tracing Ips of website searches which involve Speech of violence, discrimination's etc
4. Communication activities
5. Aiding and abiding the terrorist suspect
6. Weapons purchase

The following diagram represents ghow the machine categorise people into Watchlist and Terorrist Watchlist Thus separates civilians falling into wrong hands

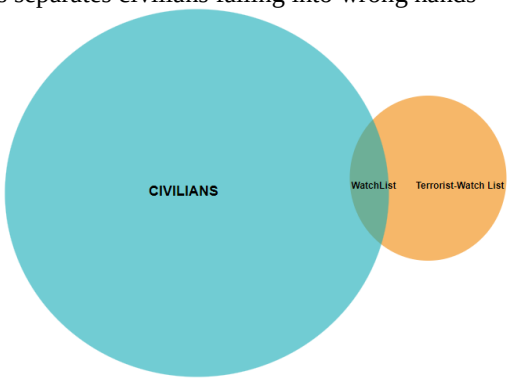

figure 1 :Venn Diagram

The following diagram represents working procedure of the machine and its data flow

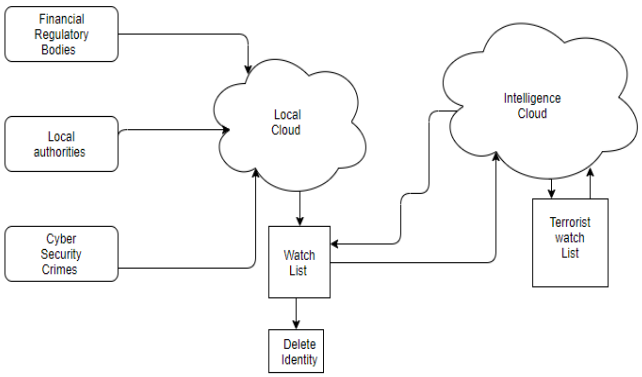

figure 2: System framework

V. Conclusion and Future Scope

This machine has the ability to track any subspecies terrorists or even a common criminal not just track them also identify them if they are caught in any camera anywhere in the country. Also, its easy to filter from normal citizens and the suspected one.

The application of this machine is limitless and the facial recognition helps majorly. An individual in Watchlist lands to any local camera then immediately all the surveillance team of that region are alerted and this information is updated again in the watch list, these way authorities could track all the movements of this individual. This machine could stop a catastrophe before it even happens, but it also has a major security issues, this machine in wrong hands could create nationwide chaos.

Therefore the machine is completely in control of Military Intelligence Authorities, all other divisions provide information and receive processed data if only necessary. Another problem is Law forbids to surveillance on any individual or citizens of the country there need to be proper proofs and lots of time to gather the proper evidence requires time. But this machine has capacity to gather relevant information.

References

[1] Andrey I. Kapitanov, Ilona I. Kapitanova,Vladimir M. Troyanovskiy, Vladimir F. Shangin, Nikolay O. Krylikov National Research University of Electronic Technology Zelenograd, Moscow, Russia Approach to Automatic Identification of Terrorist and Radical Content in Social Networks Messages, 2018
[2] Norshuhani Zamin: A Comprehensive Survey on Security in Cloud Computing, 2009 Computation World:
[3] Vassilis Plachouras Thomson Reuters, Corporate Research and Development 1 Mark Square, London, EC2A 4EG, United Kingdom Email: vassilis.plachouras@thomsonreuters.com Information Extraction of Regulatory Enforcement Actions: From Anti-Money Laundering Compliance to Countering Terrorism Finance, 2015
[4] Jochen L. Leidner Thomson Reuters, Corporate Research and Development 1 Mark Square, London, EC2A 4EG, United Kingdom Email: jochen.leidner@thomsonreuters.com Information Extraction of Regulatory Enforcement Actions: From Anti-Money Laundering Compliance to Countering Terrorism Finance, 2015
[5]https://www.cfr.org/backgrounder/tracking-down-terrorist-financing, 2019
[6] B.Thuraisingham.: and Counter-Terrorism. CRS Press / Chapman Hall, Web Data Mining and Applications in Business, 2015
[7]https://www.cfr.org/backgrounder/tracking-down-terrorist-financing, 2019

