Macrothink Institute™

Network Protocols and Algorithms
ISSN 1943-3581
2016, Vol. 8, No. 4

Internet Traffic Surveillance & Network Monitoring in India: Case Study of NETRA

Rajan Gupta

Dept. of Computer Science, Faculty of Mathematical Sciences, University of Delhi

1st Floor, North Campus, Delhi – 110007, India

E-mail: rgupta@cs.du.ac.in, guptarajan2000@gmail.com

Sunil Kumar Muttoo

Dept. of Computer Science, Faculty of Mathematical Sciences, University of Delhi

1st Floor, North Campus, Delhi – 110007, India

Received: October 20, 2016 Accepted: December 30, 2016 Published: December 31, 2016

DOI: 10.5296/npa.v8i4.10179 URL: http://dx.doi.org/10.5296/npa.v8i4.10179

Abstract

Internet traffic surveillance is gaining importance in today's digital world. Lots of international agencies are putting in efforts to monitor the network around their countries to see suspicious activities and illegal or illegitimate transmission of messages. India, being a center of attraction for terrorist activities, is also working towards development of such surveillance systems. NETRA or Network Traffic Analysis is one such effort being taken by the Indian Government to filter suspicious keywords from messages in the network. But is it good enough to be used at highest level for security analysis or does the system design needs to be improved as compared to other similar systems around the world; this question is answered through this study. The comparison of NETRA is done against Dish Fire, Prism and Echelon. The design of the NETRA scheme and implementation level analysis of the system shows few weaknesses like limited memory options, limited channels for monitoring, pre-set filters, ignoring big data demands, security concerns, social values breach and ignoring ethical issues. These can be covered through alternate options which can improve the existing system. Inclusion of self-similarity models, Self-Configuring Network Monitoring and smart monitoring through early intrusion detections can be embedded in the architecture of existing surveillance system to give it more depth and make it more robust.

Keywords: Cyber Attacks, NETRA, Network Monitoring, Network Traffic Analysis, Surveillance System, Spy System

1. Introduction

The extensive usage and penetration of technology, specifically internet, is one of the most crucial and pivotal factors that have possibly led to an increase in the criminal activities. Terrorist activities have also started to gain wide range and spectrum of supporters due to the easy availability and access of internet and differed platforms of social media. Terrorist groups have been reported to use internet for a wide range of activities such as recruitment, funding, training and instigation for committing heinous acts of violence and destruction, and the gathering and dissemination of information for terrorist purposes [1].

The terrorist propaganda deals with various text and multimedia communications that are aimed at delivering theories and ideologies to promote along with the real world practical instructions on how to carry out plans, explanations and/or promotion of terrorist activities. Internet is the easiest and the most widespread means in which, such theoretical and practical messages can be transmitted to a large audience and community within a quick succession of time. This further strengthens the fact that a proper surveillance is essential and mandatory in order to be in a position to combat such terrorist acts. Lots of traffic monitoring and surveillance applications have been started due to this.

Globally, the trend of attacking the critical information infrastructure which by the terrorist groups has emerged which includes the use of launching complex software codes and viruses into the systems along with a Distributed Denial of Services which are being used to paralyze the computer systems of the countries. These attacks are such that can be launched from any place in the world using a botnet network system, an evidence f of which was presented in the form of the 2007 Estonian network attack which is considered the largest DDOS attack yet. With over 33 nations working for creating cyber warfare systems, along with the alleged ISIS threat of an prospective cyber-attack against the US government. This is a major cause of concern for the governments worldwide [2].

The Jihadist group of terrorists has fast adapted themselves to use the social media and the internet as their tools for making an impact over the world leaders in power and the regular civilians. Although the proportion of such anti national groups is far much less than the entire user base of the social media networks, the ISIS (or ISIL) leads the other terrorist groups in their connection with the social media. The current activities of the ISIS depict a keen knowledge of the functioning and the social media system which is revealed through their recent social media which are strategically designed to be deceptive and misleading. Until the fall of 2014, the social media networks like twitter adopted a relatively tolerant approach toward the permissible content on the social media, which changed after the ISIS circulated video evidence of the beheading of an American Journalist James Foley on the social media. As per the estimates made by the Brooking about the twitter activities of the ISIS terrorist group, over 45000 twitter accounts were being operated by the ISIS followers at the end of 2014 [3].

In the Indian context, the 2016 ORF report on the Indian National Security Architecture identified that the year 2015 witnessed cyber-attacks on 72 per cent of the Indian firms with attempts made for corporate espionage [4]. India was the topmost targeted nation by the

cyber-criminal through the 7 social media in the year 2014. The Computer Emergency Response Team (CERT) on 8th January 2015 reported as many as 8311 incidences of security breaches which increased from the previous recoded figure of 5987 in November, 2014, while the reported incidences of disfiguring of the websites increased from 1256 to 2224 in the same period. The CERT in 2015 ranked India as the third most vulnerable nation in Asia susceptible to the most of the continents ransom-ware cyber-attacks. A figure replicated in the Kaspersky Security firm's 2016's third quarterly report which reveals that India faces one third of the ransom-ware incidents in APAC region [5].

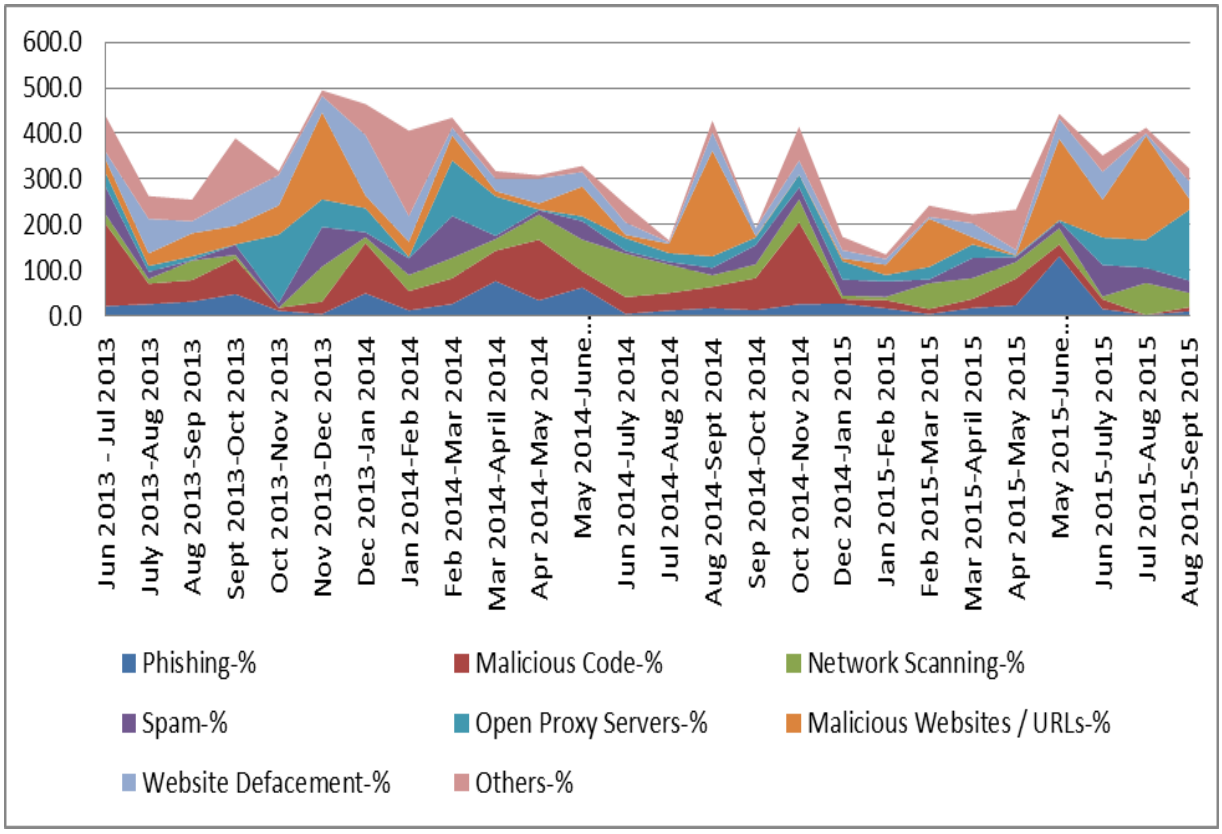

Figure 1.Natural Log of Number of Activities conducted by CERT-IN in past few years (Data Source: http://www.cert-in.org.in/)

Fig. 1 shows the security attacks being encountered through the network monitoring on quarterly basis by CERT-IN (Indian Government Web Monitoring Team). Malicious websites and malicious codes are the most encountered anomalies within the internet traffic surveillance in India in past few years. Fig. 2 shows the activities undertaken by CERT-IN in the past few years. Bot infected systems were tracked highest number of times in last few years followed by handling of security incidents. All these activities undertaken by CERT-IN can be supported by a good surveillance system.

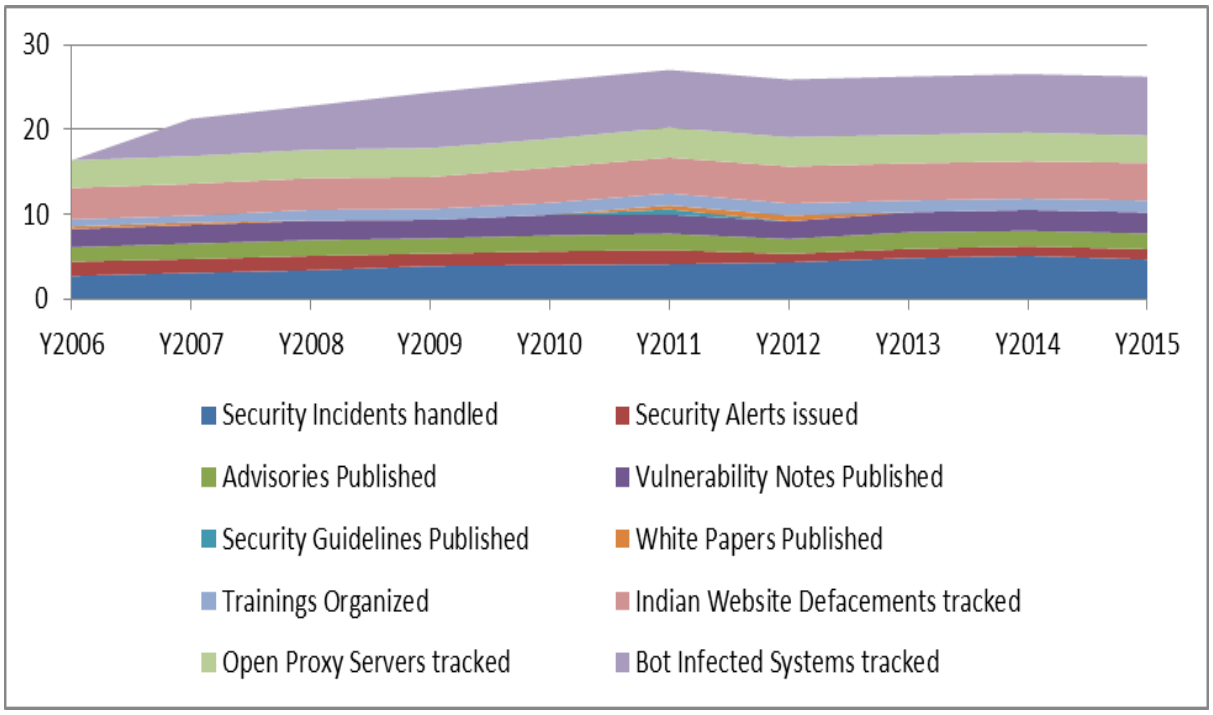

Figure 2. Natural Log of Number of Activities conducted by CERT-IN in past few years (Data Source: http://www.cert-in.org.in/)

There are large numbers of different data sets which are currently maintained by the world net data warehouse. One of them is router configuration which includes information related to security, access list, topology, and the likes. A 'triple A' system covering authentication along with authorization and accounting systems makes up as the components of the registration records. Similarly, the data under call record comprises of summary related to customer's dial-up session on per-session basis. Email server logs' include SMTP and POP3 transaction summaries. Router statistics is obtained by SNMP polling. It includes link/router utilization, access and gateway routers [6].

Apart from them, numerous packet scopes exist for IP packet headers' collection and they are designed for high performance systems. They act as passive link access in which the modification of the device driver was done for all the 'read' commands but not 'write' commands for the network interface which was under monitoring. This monitoring can be T3 which was, for a case, terminated at router modeled 7505 by Cisco and is designed for the forwarding of the packets towards monitor for the capture. Now, these captured packets are utilized for the collection of header which contains vital information. Similarly, data apart from textual form like multimedia data is monitored by passing the traffic through various protocols like RTSP, SIP and other protocols related to session-control for set-up and packet filters tear down for capturing multimedia sessions [6].

NETRA (Network TRaffic Analysis) is a networked software system developed by Centre for Artificial Intelligence and Robotics (CAIR), a departmental laboratory under Defense Research and Development Organization (DRDO) in response to the ever increasing terrorist and criminal threats received via the internet and other means of data communication [7]. NETRA, a Hindi word meaning "Eyes" is the Government of India's Internet Monitoring

System and is designed to detect, analyze and intercept the internet traffic using pre-defined filters (basic system shown in Fig. 3). The conceptualization of NETRA is a result of the Indian Security Agencies' need to design and implement a software system that could monitor & simultaneously report the usage and flow of Internet Traffic and associated activities on real time basis.

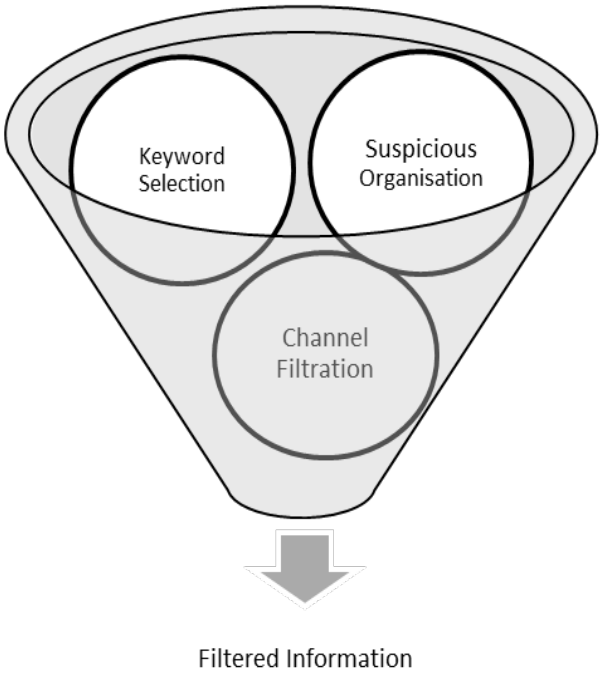

Figure 3. The NETRA System's basic working process

This paper analyzes the architecture and scheme of NETRA and discusses various issues related to it. Based on the concerned areas, recommendations are made for the betterment of the whole system. This study is a conceptual study towards development of a new surveillance and monitoring system at smaller scale to evaluate only a particular type of social media platform for any suspicious terror activity or hate message promotion through usage of various keywords. It will be helpful for the Government to monitor the Social Media Traffic and which will have the capability to be extended up to the level of Mobile Surveillance system for various communication applications. The aim of this paper is to review an existing system which has been designed in Indian conditions for monitoring and surveillance, so that the shortcomings can be utilized for existing system's improvement and new system's features selection.

The paper has been divided into six sections. First section introduced the need and background of networking monitoring and analysis. Second system will describe the existing system i.e. NETRA's features and its historical development. The third section will elaborate the issues and challenges faced by NETRA in its current form with implemented features based on existing theories and concepts. Fourth section will introduce the features of other renowned monitoring and surveillance systems like Prism, Dish Fire and Echelon from different countries and will highlight the similarities and differences with NETRA system. Based on challenges and issues along with other existing systems, recommendations will be

made in the fifth section. Finally sixth section will conclude the current study with future scope of work being mentioned at the end.

2. Literature Review

There have been different security concepts studied by various researchers in past, however this section reviews studies majorly from areas like Internet Traffic Surveillance, Network Monitoring, Intelligent Spy Systems and Central Monitoring System. In 2005, Zander et al [8] proposed the usage of Machine Learning techniques for traffic monitoring as it was considered to be dynamic classification of anomalies in the network. The flow statistics were used for the unsupervised learning like the size of packets, duration of the packet transfer and related stuff. The authors argued that network monitoring cannot be based only on the packet header for anomaly detection but should also be based on other characteristics like their flow and other network features. So, India spy system using other characteristics like body text through words can be a good combination. Prior to machine learning, Zander et al [9] presented only statistical analysis on the flow of the data through network in collaboration with Cisco Systems.

Before the work was carried out on the packet fields other than header of the data, Boyed et al [10] presented the analysis of surveillance on the video traffic in the network. They presented their analysis based on the Network Tomography which is useful in finding out the source-destination network traffic with the help of the link statistics. The authors worked majorly on the movement of the object from one region to the other. This work may not be an immediate value addition to the keywords tracking by the Indian Network Monitoring System but will definitely provide the robust technique for video surveillances. But such videos and internet calls (non-text based data transmission) will require more surveillance in the upcoming data monitoring schemes within the Indian tracking system. Wang et al [11] described in their technique that digital watermarking could be a potential solution for the VoIP calls so that anonymity can be tracked and suspects can be monitored regularly for their conversations.

Network monitoring has been studied through different channels in past by various researchers. Gavalas et al [12] used the role of mobile agents for monitoring the network. Filtering was applied for the data packets using mobile agents and an improvement over the overheads of the traffic was observed. Anagnostakis et al [13] started with the packet level network monitoring which was programmable in nature. The logic was developed on the fact that majority of the routers have an in-built monitoring capability with the likes of SNMP, NetFlow, and RMON. The authors developed various functionalities within their system like IP Traceback, detection of worms, network traffic analysis, and charging based on ECN. Specifically in the traffic analysis, the packet train was identified which was based on similarity of adjacent packets. No specific packet text was analyzed. Liotta et al [14] discovered role of mobile agents for active Network Monitoring within a distributed system. Agents work as the network monitors not confined to a particular node which helps them in sensing better location and are useful in even optimizing them. Chen et al [15] worked on the

overlay network monitoring through algebraic approach. Their scheme was useful in the case of scalability of the nodes, achievement of efficiency even when the topology of the network changed, and error handling within the various topologies. Ho et al [16] used Network Coding for the monitoring of the network in a multicasting mode. The information stored in network was used for detection of loss and errors in the network. Leners et al [17] presented a FALCON framework for network monitoring in which the error or malicious activities were tracked for the network in a distributed system. However, the end points and their data packets were not the prime focus. Logics of the proposed system were implemented on various machines and the overall system's reports were integrated.

There have been various tools also prepared in the past for network monitoring like MOTE VIEW [18] and NG-MON [19] which are useful for network monitoring activities. However, there have been very less studies presented on the Surveillance systems in India and specifically with the characteristics of a Spy Systems. Therefore, this study would be useful in analyzing the current monitoring/surveillance or spy system in India i.e. NETRA and make comparison against other prominent such systems used worldwide in the past. Moreover, the technical research studies in the past will be helpful in suggesting architectural changes in the system so that it becomes more robust and effective in handling various types of intrusions through keywords mapping and network characteristics.

3. About NETRA System

3.1 Historical Development

As a part of the Government of India's efforts to develop an internet monitoring system, two different agencies, CAIR by DRDO and NTRO were given the responsibility of developing technical systems that would concentrate on scanning through internet data and detecting suspicious words. A private organization – Paladion, took the responsibility of designing the system by helping NTRO, whereas CAIR formed an internal team of 40 members to work on development of NETRA system. Vishwarupal, NTRO's monitoring and surveillance system, faced several problems such as the involvement of some external private company in issues concerning security, and NTRO's ability and competence in operating such a system independently without the help of Paladion. Along with these, other platforms were launched by the Government like the NATGRID which was set up by the Government of India for the monitoring of the terrorist operations through developing a structure for enhancing India's counter terror capabilities [20].

Additionally, the testing of the Vishwarupal by Research and Analysis Wing (RAW) did not end satisfactorily, citing the reason that the system crashed on a frequent basis. On the other hand, NETRA system was designed and operated by a group of Government appointed scientists and no part of its operation involved any external or private agencies leading to security insurance. The testing of NETRA was done by Intelligence Bureau (IB), which was pleased with NETRA's performance and CAIR's continuous investment in its Research & Development wing to cater to changing technologies. Hence, NETRA got preference over

Vishwarupal as the Government of India's official Internet Monitoring System.

3.2 *Features and Implementation areas*

In present context, traffic analysis can analyze the data flow through internet even when the messages being transmitted are encrypted in a manner that is difficult to decrypt. NETRA is modeled to process and filter out the content that is being generated by the "Netizens" (Internet Citizens) these days. It is aimed at encountering and detecting catch words (as shown in Fig. 4) such as 'attack', 'bomb', 'blast', 'kill', 'jehad', 'murder', 'terrorist' among other similar words [21].

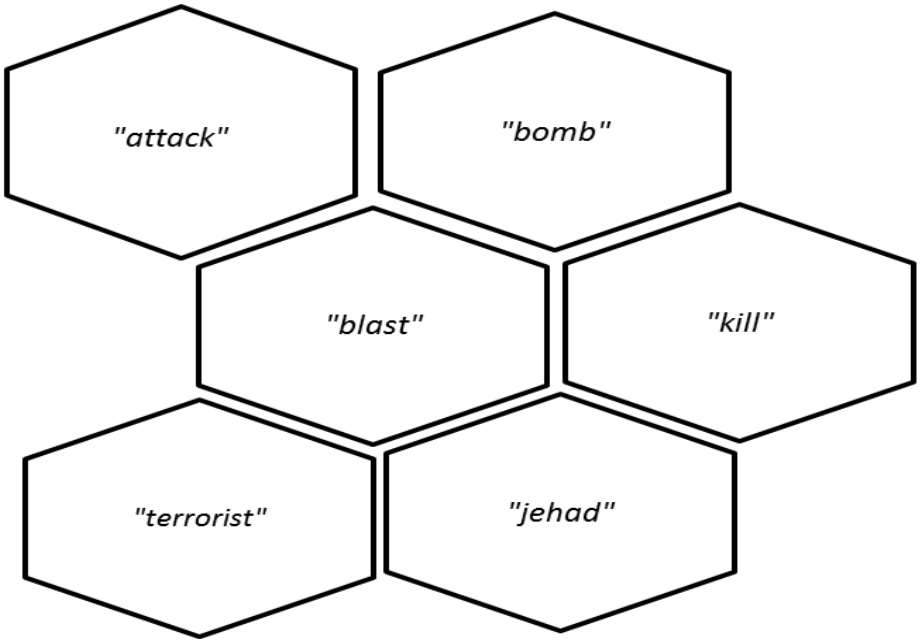

Figure 4. Keywords for surveillance by NETRA

NETRA is designed to report any such word usage and their related IPs to the associated authorities and agencies which can take appropriate actions on immediate basis. The system is aimed at monitoring mainly terrorist activities and is designed to be implemented in three major work zones that include the major Security agencies of the nation, the Cabinet Secretariat, RAW, and IB. The latter two are country's external and internal intelligence agencies, respectively. An allocation of 300 GB of memory space has been done to the above mentioned three security agencies for storing the internet traffic that they intercept for analysis. Another 100 GB has been assigned for the same purpose to the remaining law enforcement agencies.

3.3 *Channels and Target Audience*

The NETRA system majorly aims at observing the internet activities and trends of suspicious and doubtful people, businesses and organizations that have a history or an inclination to carry out heinous and opprobrious acts. The channels (as shown in Fig. 5) that will be affected by the implementation of the NETRA system include tweets on suspected Twitter accounts, status updates from Facebook, e-Mails, Instant Messaging Services,

Internet Calls, Blackberry Services, Blogs, Forums, along with intercepting suspicious voice traffic from Google Talk Services and Skype Messenger with their relevant IP addresses.

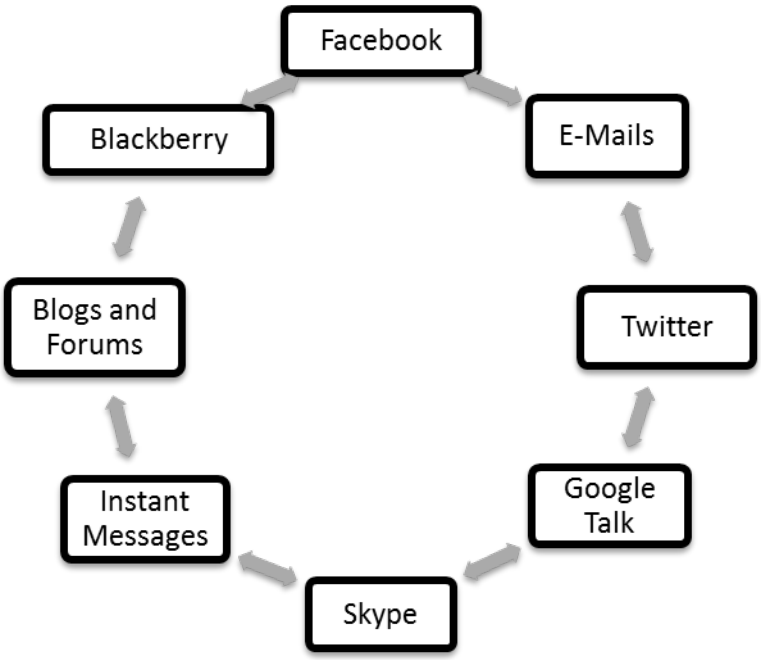

Figure 5. Channels for various target audience by NETRA system

3.4 Current status & Implementation

The working team for NETRA includes DRDO Scientists along with a team of 40 members, including scientists from Indian Institute of Science who are working on the NETRA program since 2010. The system has been tested at small scale by various security agencies and is now in its finishing touches stage. The NETRA was deemed to be launched in 2014 for which the status remains unclear from various officials even in 2015.

The government of India's inter-ministerial group constituting officials and members of Cabinet Secretariat, Home Affairs Ministry, and various intelligence agencies like IB, RAW along with development team from DRDO, CAIR and CERT have already worked on the deployment strategy for NETRA and are in planning mode for the expansion of the system to incorporate measures and techniques in reply to "computer security incidents, track system vulnerabilities and to promote efficient IT security practices throughout the nation" [22].

In addition, the Government of India has incorporated various state and regional agencies for the monitoring of region specific threats to the national security while channelizing the coordinated efforts of the sub intelligence bodies for the analysis of the data. As an instance, the Delhi Police has established a Centre for Analyzing Social Media for monitoring the digital content being posted on the various social media platforms with the purpose of gathering the general trends on the social media platforms and filtering out probable risks to the social harmony. Though the centre runs its independent dedicated server, the centre also contributes to the integrated national system of digital media monitoring [20].

There is also a growing demand for installation of additional NETRA systems in law

enforcement agencies due to the fact that the existing NETRA system that is being used by RAW is found to be ineffective and inconsistent with the demands of the Law Enforcement agencies as it mainly focuses on intercepting global messages specially from neighboring countries to look out for potential terrorist activities and attacks. The NETRA system installed with the RAW analyses large data consisting of international posts crossing through the Indian networks and additionally relies on the matching keywords that are more often than not of no use to the Law Enforcement agencies that are looking out for criminal offenders rather than terrorists.

Whereas RAW focuses on intercepting and scanning messages passing through mails, forums, social networks and blogs, the Law Enforcement agencies are more concentrated on the data transfer, voice traffic and message transmission through Skype, Google Talk, Twitter and Facebook. It has, therefore, been recommended by the Ministry of Home Affairs that the existing NETRA facility with RAW must not be used by the Law Enforcement agencies. Instead, another NETRA unit designed by CAIR will be installed for the exclusive use by Law Enforcement agencies.

4. Challenges & Issues faced by NETRA

NETRA, though an advanced national level security measure, is doomed not to be a 100% success as per the analysis because of the large number of challenges that it needs to face. NETRA, at the moment is prone to a partial success only due to the multiple issues that hinder its expected success as shown in Fig. 6. They are discussed below.

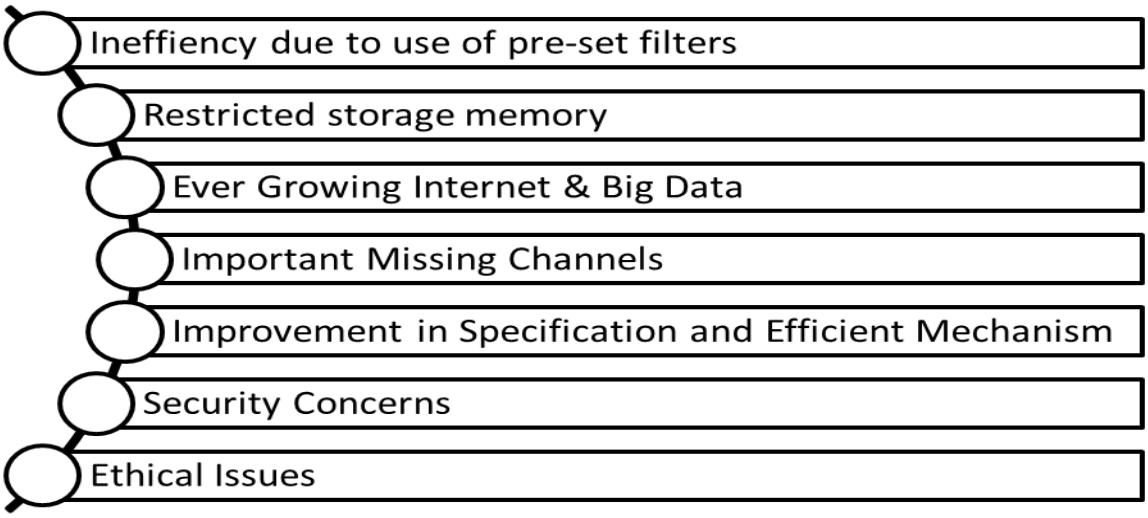

Figure 6. Challenges and Issues for the existing NETRA system

4.1 Inefficiency due to use of pre-set filters

NETRA as a system operates by using pre-defined filters that match keywords like ‘attack’ , ‘bomb’ , ‘blast’, ‘terrorist’ and ‘jehad’ among others [7]. But this could lead to an

inefficient system as the conversation or data that is being intercepted may end up having negligible relevance to national security. It will be difficult to draw conclusion about the intent behind using such words as only frequency count can't be a suitable method for this purpose. The system should be more adaptable towards words analysis.

4.2 Restricted memory for storage

The specifications of the NETRA system reveal that three national security agencies, the Cabinet Secretariat, Intelligence Bureau and the Research & Analysis Wing will be given only limited combined storage space of 300 GB with law enforcement agency getting an additional 100 GB. Statistics reveal that in India, there are 216.5 million Social Media users [23] which increased drastically form the 134 million users of the social media in August 2015. As reported by the internet live stats, there are on an average 6000 tweets being tweeted on twitter every second of the day which combine at around 350,000 tweets per minute and over 500 million tweets per day, which are increasing day by day because of the introduction of new twitter accounts per day in the country (Internet live stats). Further in a report by Radicati, it was found that the global number of email accounts is expected to increase from 3.3 billion users in the year 2012 to 4.3 billion email account users by the end of the year 2016 [24]. The magnitude of the data that need to be deciphered and examined by the NETRA system is humongous and even if we ignore the ever increasing nature of the data, yet, NETRA will not be able to manage and intercept a large amount of data that is being transmitted and transferred on a daily basis. It is highly probable for the system to fail because a storage space of 300 GB for three Security agencies will exhaust in a very quick succession of time [21].

4.3 Ever Growing Internet& Big Data

Internet is a vast network that is growing at an exponential speed. Its monitoring and surveillance can be a much more difficult and handy task than was initially predicted. There are millions of social network users who transmit and transfer billions of messages and voice talks on a daily basis. Scrutiny and inspection of such a large number of users will require resources and technology that is much more advanced than what India presently owns. With so many communication applications growing at an exponential speed and large number of users switching to internet through mobiles and laptops, will make things worse. Big data technology will have to be implemented from the starting day so that scaling of data does not impact the surveillance system. Thus burgeoning internet usage and ever growing big data poses a serious threat to the NETRA's working. With the increase in use of internet, the websites as well as the service providers have started providing advanced levels of data encryption to ensure the user privacy but since the system of NETRA depends upon the data probes made, the decryption tools that are employed at the gateways do not work and hence, the system cannot decrypt the encrypted data making the entire exercise meaningless. Further, with the increasing popularity of the internet calling, the issue of deciphering the internet calls arises in which the authorities are hapless in decrypting the encrypted data making the whole purpose tracing the calls worthless for the authorities [25].

4.4 Important Missing Channels

Popular file sharing websites and channels such as Dropbox, Rapidshare and Fileshare [1] have not been included in the affecting channels by CAIR. Well in demand messenger services like Whatsapp and other mobile based Applications have also not been included. Such omissions leave huge gap in the proper implementation of the system and may hinder complete interception of online activities of suspicious individuals and groups. Moreover, constantly evolving such platforms and channels also make it difficult for the monitoring system to be more dynamic in its approach. And the advancement in the encryption technologies of these social media channels has caused the NETRA to face a number of challenges which can be attributed to the limited expertise in the cryptology by the program heads in India. The situation is such that the defense agencies have limited options left apart from taking the help from the major social media service providers like Facebook, Google, and Twitter etc. for providing them with the updated communication database [25].

4.5 Improvement in Specification and Efficient Mechanism

During a small scale demonstration in January of 2012, NETRA was able to pass only 3 GB traffic out of a total of 28 GB through its probes. It is the only high point, which worked as an advantage at that time. It was the only system out of those tested, that was able to capture the Internet data traffic without any stalling. Additionally, for a system such as NETRA that is aimed as a measure for providing security, quick response is a must and probably the most important feature. The system can save many lives in the nick of time and hence, a quick response is necessary. Based only on key-words filtration won't solve the efficiency part and improved big data mining techniques will have to be supported for future activities.

4.6 Security Concerns

CAIR needs to protect and safeguard the NETRA system against external hacking. An external hacking of the NETRA system can lead to chaos in internet traffic and probable threats being transmitted without any interception rendering the main function of using NETRA system useless. Also flooding attack of the keywords may create panic for the system. Thus, there must be a pattern recognizer that should be able to keep control over the system's filters and keep a track of abnormal behavior.

4.7 Ethical Issues

Surveillance of one's private talks and messages on platforms such as Google Talk and Skype is considered to be highly unethical. Even largely advanced economies like United States and China have not been completely successful in implementing their Internet monitoring systems due to the same reason. Internet surveillance can work and be successful only till an extent beyond which its success rate and effect becomes stagnant. Even one of the founding fathers of World Wide Web, Dr. Vint Cerf believes that Internet surveillance can never be successful as it goes against the basics of Internet, which in the first place is based on the freedom of expression and action [21].

5. Other Renowned Systems

Espionage, or casually monitoring involves a government, company or individual firm obtaining information about a person or firm that is confidential without the permission of the holder of information. Every nation is trying to develop a surveillance &monitoring system that can collect and analyses the data which can help them to detect terrorism activities well in advance. This section discusses about the various leaked international monitoring systems that officially didn't exist.

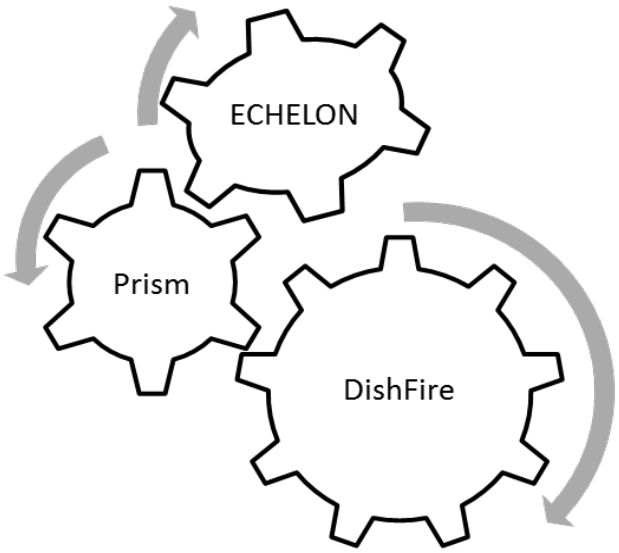

Figure 7. Other Renowned Systems for Monitoring traffic in foreign countries

5.1 ECHELON

ECHELON is not just a system but a code name which was used to describe collection of any signal's intelligence and analysis of its network. The code name was developed and devised by a joint operation by five different signatory nations namely, Australia, New Zealand, UK, USA, and Canada, thus also referred to by a number of abbreviations like AUSCANNZUKUS. Due to a secret treaty around late 1940s, these five nations formed Echelon under an Anglo-Saxon Club without any commercial implications. It was decided to divide world's communication activities into various regions by these nations which would be helpful in carrying out eavesdropping activities around the globe. The system was majorly oriented towards military spying and various diplomatic communications during the cold war of 1960s and 1970s. ECHELON in simple words, can be said to be a global network of various monitoring stations that can secretly listen to the communication on telephones, faxes and emails. ECHELON is directly linked to the headquarters of the US National Security Agency (NSA) at Fort Mead in Maryland [26].

The ECHELON system has been designed to tackle multiple channels of communications for the message transfer. It can intercept and inspect the data transfer through facsimile, telephone conversations, messages through teletext, internet usage, e-mail communications and other digital communication forms taking place in different regions of

the world. SILKWORTH and SIRE are the functional programs that make up the core DNA of the ECHELON system and the interception was done through a satellite named VORTEX [26].

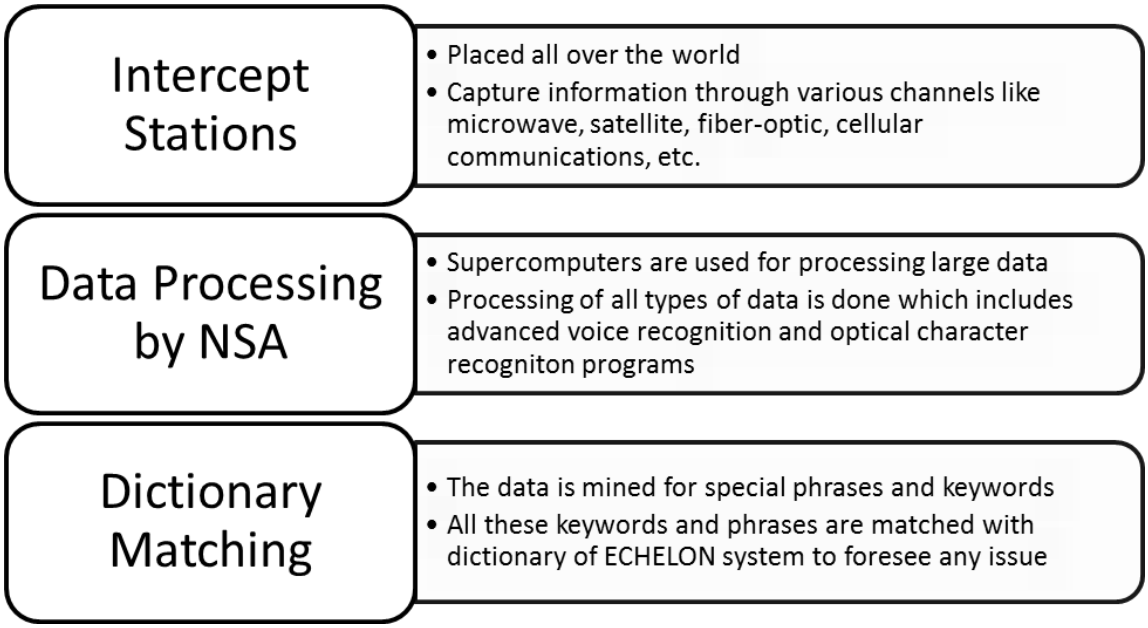

Figure 8. Working steps of ECHELON system (Source: [27])

The working of ECHELON system as shown in Fig. 8 is not a complicated task [27][28]. It has three major steps associated with the system and its working. The first is the data capture, second is data processing and third is data matching. Data Capturing is done through various inception points around the globe and capturing through various communication channels. NSA does the processing of all types of data thereafter with the help of supercomputers. Once the processing is done, the dictionary match for suspected words and phrases are carried out so that any malicious pattern can be detected and worked upon. The ECHELON system is well versed with different communication channels and platforms which can capture variety of data transmissions.

Each agency linked with ECHELON covers a part of the world by dividing the world up among the UK-USA parties. NSA from US covers the signals of both the continents of America. GCHQ of Britain covers up the region of Africa, Europe and western parts of Russia. DSD of Australia covers up the regions like Eastern side of Indian Ocean, Southwestern past of Pacific region and Southeastern part of Asian region. GSCB of New Zealand covers up portions like island nations from South Pacific. CSE of Canada is covering up the northern regions of Russia and Europe along with the American communications.

The ECHELON system came into existence when the European parliament issued a report on Echelon in 2001, and the allegations of gazing sensitive information from European region was made against the rivals from America and Britain. It was argues that the system is potentially hampering the privacy and secrecy of individuals and organizations by invading into their communication environment.

5.2 DishFire

Dish Fire is a surveillance system working at global level monitoring the traffic along with maintaining the database for the communication. It is handled by the security agencies of United States of America and United Kingdom – NSA and GCHQ, respectively. It is run on daily basis and it collects hundreds and millions of text messages around the world. A related analytical tool known a PREFER is used to analyze the data collected. This tool is used for processing the SMS sent through cellular network and extract vital information from the phone like call alerts, location of the phone, financial details of the payments done and electronic card processing. Dish Fire works by collecting and analyzing automated text messages such as missed call alerts or texts sent to inform users about international roaming charges [29]. This system also invades the privacy of the users and citizens. Moreover, this system also extracts the textual data for the analysis of any potential threat.

5.3 Prism

PRISM is a system the NSA uses to gain access to the private communications of users of nine popular Internet services. This system, launched in 2007, is also used for surveillance through monitoring and data mining by NSA in USA in association of GCHQ from Britain. The official nomenclature of PRISM is SIGAD US-984XN which is destined for data collection and analysis. The system is fully under legal bindings and adheres to the Section 702, FISA Amendments Act, 2008. It collects the stored communication from internet and compares it against the court-approved terms. It is more inclined towards the assessment of the encrypted data sets. NSA programs collect two kinds of data: metadata and content. Metadata, a sensitive byproduct of communications, such time, number of calls, phone records and contents, which the NSA PRISM Program includes i.e. emails, chats, VoIP calls, cloud-stored files, and more [30]. The system also has the similar comparative style of searched content and approved content within the legal boundaries.

5.4 Similarities & Differences of various systems with NETRA

All of the surveillance systems as discussed above including NETRA have similarities and differences amongst them. The similarity between all the systems is the common approach used that is data capture and data mining/analysis but the techniques are different. ECHELON and NETRA both uses the concept of matching the words from ECHELON Dictionary and NETRA Dictionary respectively. ECHELON intercepts transmissions from satellite and also from Public Switching telephone Networks whereas NETRA only aims at observing the internet activities of the citizens. Also, DishFire is one system that extracts anything it can by analyzing automated text messages and miss call alerts. The prism program on the other hand stores the contents of emails, chats, and more. NETRA only focuses on data from the internet services. The ECHELON system is treaty between 5 nations with 5 different agencies covering some part of the world, whereas NETRA has been covered by 3 securities agencies that include IB and RAW within Indian region only.

5.5 Adoption of features for NETRA

Some of the features of the international systems can be extracted which can help make

NETRA– a better system. One of those features can be taken from Dish Fire that is to use a tool like PREFER that can extract information from miss call alerts, travel alerts and automated messages and more. The other feature that could be extracted is from ECHELON network i.e. the capability to intercept transmission from PSTN (public switched telephone network) that can listen to and analyze telephone conversations, fax transmission and more. Like ECHELON the 3 agencies can be provided 3 different locations to cover and then integrate as one to analyze the data and then send to its required department. More detailed improvement features are discussed in next section.

6. Recommendations

There are certain proposals that can effectively enhance the working, operation and probability of the success of the NETRA system in India. They are based upon existing systems and past researched concepts which can be utilized to improve the current form of NETRA.

6.1 Use of Efficient Algorithms

Table 1. Accuracy for Classification using different methods in Sentiment Analysis (Source: [31])

	Algorithm & Features	**Red Tomato**	**Yelp**	**IMDB**
Unigram	Linear Support Vector Machine	76.2	91.87	87.80
	Logistic	76.9	91.90	88.19
	Naïve Bayes Support Vector Machine	78.1	92.13	88.29
	Multi-theme Sentiment Analysis	78.0	92.20	88.57
	Multi-theme Sentiment Analysis (fixed negation)	78.3	92.20	88.48
	Multi-theme Sentiment Analysis (NB)	78.3	92.52	88.81
	Multi-theme Sentiment Analysis (shifter)	78.4	92.78	88.82
	Multi-theme Sentiment Analysis (NB + Shifter)	78.8	93.08	88.97
Bigram	Linear Support Vector Machine	77.7	91.93	89.16
	Logistic	78.1	92.99	89.18
	Naïve Bayes Support Vector Machine	79.4	93.99	91.22
	Multi-theme Sentiment Analysis (NB + Shifter)	81.3	94.07	90.44

NETRA system uses pre-set filters to match the intercepted conversations with a set of pre-defined keywords. Instead of using only filters, the NETRA system should switch to sentiment analysis in order to understand the intent behind usage of the keywords. Usage of phrases and sentences should also be considered within the text mining. And also the system will have to use real time text mining rather than a static implementation of the algorithms. With the emergence of multi-theme sentiment analysis, even the shift in the sentiments of the statement and phrases can now be correctly classified with the help of various algorithms. Table 1 shows the predictive accuracy for various algorithms on sentiment analysis done through three datasets in R Language – Red Tomato, Yelp and IMDB Dataset.

Such algorithm usage will be helpful in analyzing data packets in the network

surveillance with higher accuracy levels.

6.2 Use of Better Hardware Infrastructure & Technology access

Also, the usage of algorithms as used by NSA and GCHQ can be done [32]. These two USA and UK based agencies have used ubiquitous encryption schemes in the internet world to be able to access emails and data records stored around various servers. They used super computers to extract the information be it by brute force or other decryption schemes but usage of super computers is limited in Indian Surveillance Environment. The usage of backdoors and trapdoors was also done by the agencies around the world in collaboration with technology companies. The same can be used by the Indian counterparts. Companies like Microsoft have worked with NSA in past to compromise on the encrypted data in their products in the past [32]. Similarly, Indian surveillance and monitoring agencies can tie up with the Indian tech companies to be able to monitor the encrypted data in Indian network.

6.3 Use of Expandable Memory techniques

The use of expandable memory techniques is a must for the NETRA system as the current allocated memory does not look to be sufficient enough to store such humongous data. Storage services using Cloud can resolve the issue of restricted memory allocation to the Security Agencies for the storage of intercepted data and will be better used for the protection of data stored on them. Government has already launched MeghRaj as its official cloud platform for various government applications. Also better applications with larger memory space and faster access like Wild Packets can also be integrated with the applications [33].

6.4 Inclusion of Other Popular Channels

The NETRA system will have to expand its targeted channels. The whole system will have to be built around the dynamic environment so that every new application developed in the market could fit into the surveillance system. Currently NETRA will need to include various popular file sharing and messenger services like Fileshare, Dropbox and WhatsApp among others to widen its range of monitoring that it seeks to intercept data transmission from. NETRA system’s limited accessibility can soon be turned into its weakest zone.

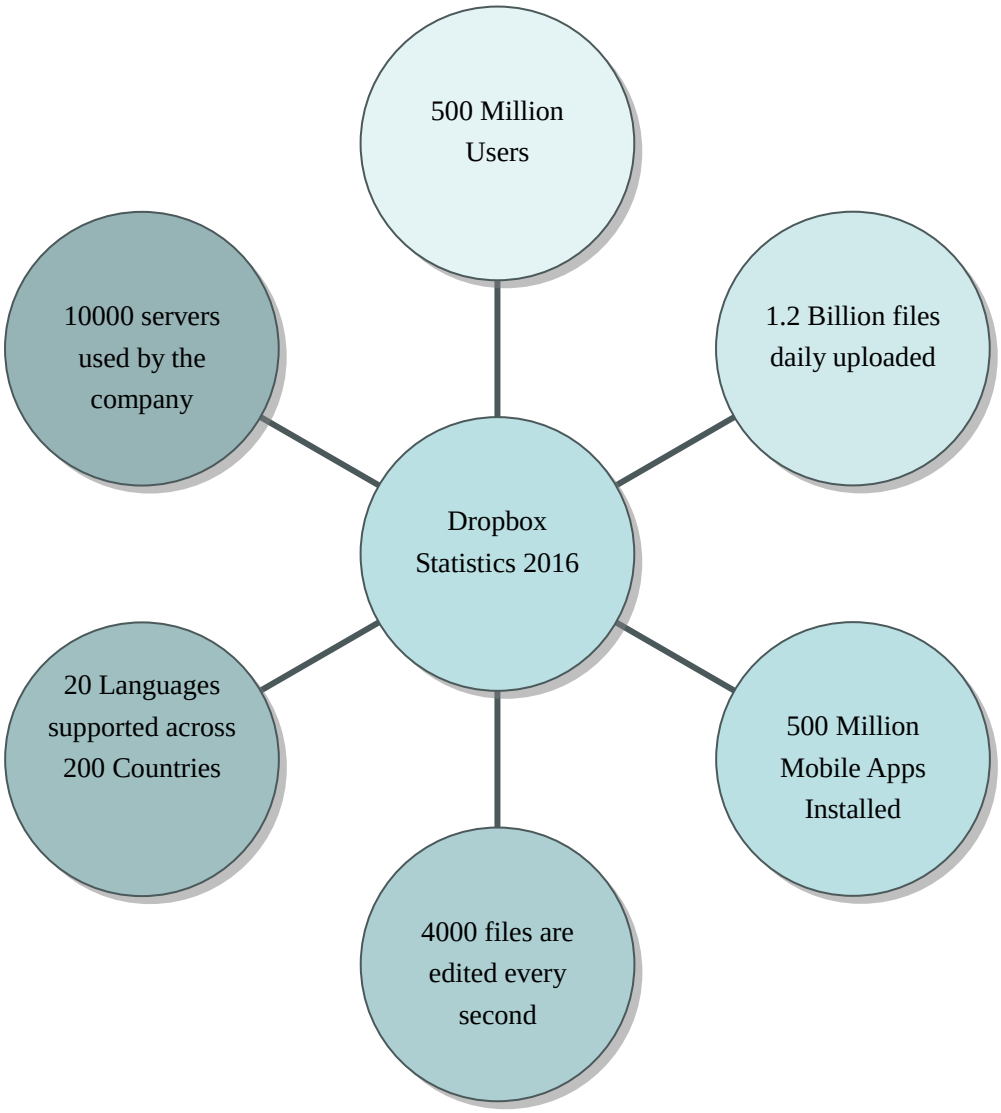

Figure 9. Some numbers in support of Dropbox like channels to be included (Source: [34])

6.5 Implementation of Lightweight Algorithms

The system will also have to develop and use lightweight algorithms as an alternate to expandable memory in order to watchdog through all conversations among suspicious individuals and groups without the storage space provided becoming a hindrance. Specific lightweight algorithms are available [35] and which can cover both text data and multimedia data.

6.6 Appropriate Security Measures

The system can start adding alternate keywords to broaden its range of relevant intercepted conversations. As an addition, it can also seek to strengthen its systems against probable external hacking. The system should further prevent spamming through the pre-defined keywords. Also an exhaustive IP Traffic Monitoring scheme will be useful in enhancing the security [36], along with Network Monitoring tools integration like NetFlow [37].

6.7 Type of data expansion

Currently NETRA only uses the surveillance system for textual type of data only. Rising multimedia data will be a concern for the monitoring agencies and mostly text based data is converted into images or videos and is then spread across the various channels. NETRA will have to take care of both types of data in order to be more efficient and effective in its implementation. Also deep packet inspection [38] can also help in much exhaustive analysis for the Government Surveillance System.

6.8 Text Mining Techniques

There are various text mining techniques that can be used to mine the data. One of the latest algorithms being used is the KID which mines the data on the basis of some keywords. Some of the old mining techniques are Natural Language Processing, Information Execution, and Transforming Word Frequencies. Otherwise too, government operations and transactions should be mined frequently in order to detect any unwanted patterns in the data [39].

6.9 Network Breach techniques

Accessing traffic in each zone can be accomplished by hubs, span ports, taps, inline devices and more. Some of the most common ways for breaching a network is Social Hacking, Cracking, Network Sniffing, and Packet Sniffing. Quantum Insert is a leaked NSA technique where fake servers are created to mimic real websites between traffic on a targeted network and the real website. Serendipity was a NSA tool developed to capture data from Google network. SNACKS, Social Networking Analysis Knowledge Collaboration Services, is a NSA application that looks at SMS text messages, to derive organizational structures. EDGEHILL, UK's anti encryption technique aimed at cracking all the major internet company's encryption technique [40].

6.10 Inclusion of Self Similarity Models in NETRA

Self-similarity models, as studied by various researchers in past, can be utilized within NETRA system for better efficiency. According to statistics, the idea of self-similarity can be used to describe traffic i.e. bursts on wide range of scales. Self-similar process can exhibit long range dependence as it has noticeable bursts at wide range of time scales. "Self-similarity is a property which links with one type of fractal; where an object's appearance is unchanged despite of the scale at which it is viewed" [41]. Self-similarity can be explained mathematically as,

$$Xt=m^{-H} \sum (i= (t-1)\ m+1 \text{ to } tm)\ Xi, \text{ for all } m \in N \qquad (1)$$

If X is H-self-similar, it has the same autocorrelation function

$$r(k) = E[(Xt - \mu)(Xt+k - \mu)]/ \sigma^2 \text{ as the series } X^m \text{ for all } m \qquad (2)$$

Various traffic models and conditions of its self-similarity have been described in the past which can be very well utilized while strengthening NETRA system as a whole. Another model has the buffer content distribution in a fluid queuing system which receives input from N independent on/off sources. "It considers a traffic which is a superposition of N sources. A

source j constantly transmits at rate Rj> 1 when active, contributing RjAij volume to the traffic during its ith active period" (Boxma, 1996 [42]; Tsybakov & Georganas, 1998 [43]). The results on self-similarity of considered traffics are not provided by this model. They present steady-state distribution of infinite-buffer content at some specific time moments, for a queue supplied by each of these traffics. Fluid flow model includes statistical multiplexing without buffering. The no buffering is possible when the combined input rate is maintained below link capacity. The overall loss rate is the ratio of expected excess traffic to expected offered traffic if all excess traffic is lost (formally, "loss rate = E [(Δt-c) +]/EΔt" where Δt is the input rate process and c is the link capacity). "This loss rate only depends on the stationary distribution of the combined input rate Lt". Buffer-less multiplexing has an advantage with respect to the quality of service that can be controlled, also when the peak rate of an individual flow is small as compared to the link rate the buffer-less multiplexing is efficient [44].

Web traffic similarity model appears to be more relevant in context to the NETRA which can improve the monitoring capabilities of the system through the web mode.

6.11 SCNM Implementation

The Fig. 10 shown below explains the hardware components of Self-Configuring Network Monitoring (SCNM) system.

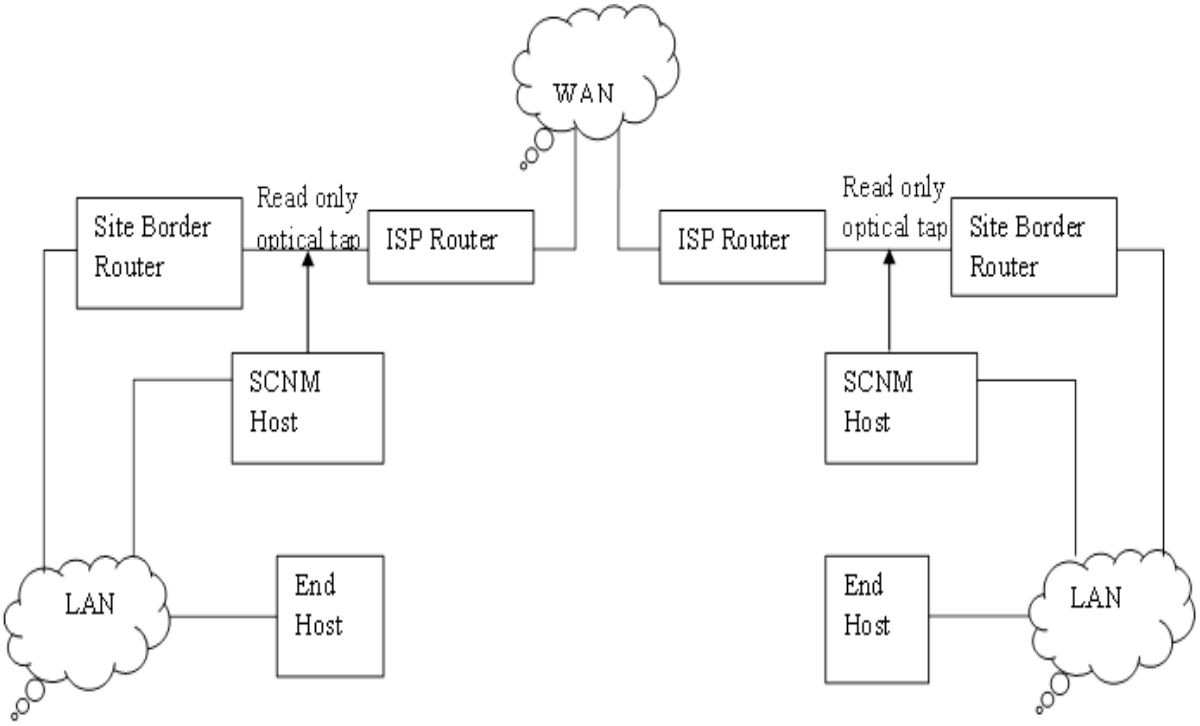

Figure 10. SCNM hardware components (Source: [45])

The SCNM provides a function to detect network problems, by allowing users to monitor their individual data. It also allows users to monitor specific data streams without providing special access privileges or intervention by network administrators. The architecture shows the arrangement between two end hosts through a WAN. A read only optical tap is positioned

on Demilitarized zone (DMZ) between the site border router and ISP router. Also SCNM monitoring host is connected to the read only optical tap. The SCNM monitoring host has a network interface which is used for sending output data and managing the SCNM host. Also the SCNM monitoring host sends the resulting data to the source or destination of the monitored traffic only. This model allows user to only monitor their individual data [45]. With the implementation of SCNM, the three agencies involved in NETRA would be able to manage and monitor the traffic at their respective ends.

6.12 Smart Monitoring

The need of the hour for the various surveillance systems in India is to adopt a holistic approach. Just merely keyword detection would not be enough to solve the problem of cyber and terrorist attacks [46]. It could be just one step towards developing a robust network but there is a need to develop smarter systems which can monitor the network and give warnings on the possible intrusions based on network characteristics too [47]. Based on the various statistical [44] and network characteristics, the unwanted patterns can be identified and intrusions can be picked up. The intrusions would be more beneficial in the longer run rather than keyword monitoring and tracking as these text-based keywords can easily be used to fool around the monitoring agencies. An intrusion once detected through the network monitoring can be looked down further for the keyword tracking. It is highly likely that an activity with malicious behavior will have the text message to be containing objectionable keywords in direct or indirect form. Therefore, intrusion detection at first phase, and keywords checking at second phase will be helpful in smart monitoring and a dual classification scheme as shown in Fig. 11.

Figure 11. Smart Monitoring Process flow chart

The role of dual classification based surveillance will enhance the monitoring capabilities and will classify the current research problem under Multi-objective optimization. Multi-objective problems can be solved using the evolutionary algorithms or soft computing [48].

6.13 Proposed Framework for the NETRA like Surveillance System

The need for a more comprehensive approach is required for improving and developing a surveillance system like that of NETRA. Based on the recommendations above, a generalized layered framework, as shown in Fig. 12, can be proposed for the surveillance system which can monitor the traffic and can also track the keywords.

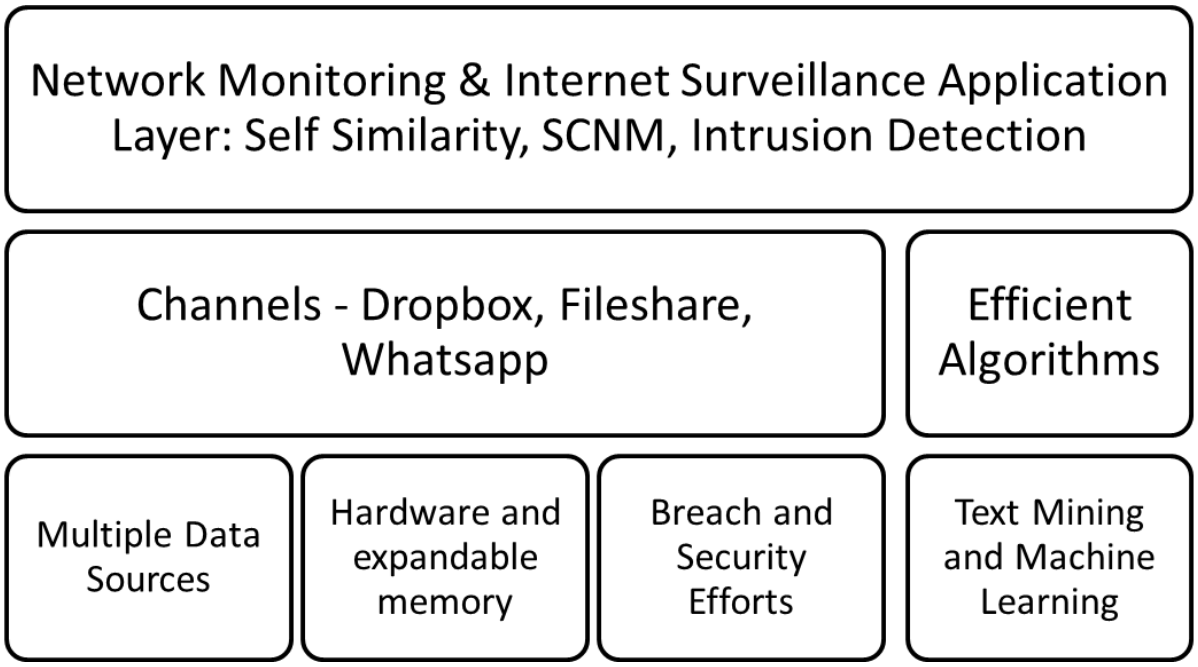

Figure 12. Proposed framework for improvements in the NETRA system

The suggested techniques can have an individual strength of improving the framework by a considerable amount as suggested in Table 2.

Table 2. Improvement Margins for each suggested factor for NETRA improvement

Factor Affecting the System	*Parameter for Improvement*	*Improvement Margins*
1. Efficient Algorithm	Accuracy Improvement using Sentiment Analysis	4-5%
2. Hardware Technology	Revenue expenses on better hardware and Technology	500-800%
3. Expandable Memory	Storage Space increment	300-500%
4. Channel diversification	More data points from multiple channels	1000-2000%
5. Lightweight Computing	Speed for execution	5-8%
6. Text Mining	Machine learning based improvement in predictions	5-10%
7. Self-Similarity Models	User congestion while Active and Inactive Mode	10-15%
8. Self-Configuring Network Monitoring	Congestion in Monitoring Host	35-40%
9. Smart Monitoring	Intrusion Detection Scheme based accuracy in predictions	5-10%

The margins for improvement have been taken from Literature on individual basis and

the range for margin has been reported based on selected parameter for the various factors. It can be seen that hardware technology, expandable memory and channel diversification are the most critical factors which needs to be considered in the existing system. However, other critical factors self-similarity, SCNM and Smart Monitoring are also required to be included in the system. The remaining factors will be useful in optimization of the current system and will be useful once the system gets stable and self-sustainable.

7. Conclusion

NETRA seems to be an innovative approach towards internet surveillance by the Government of India. But in order to ensure its efficient and effective implementation, the key concerns pointed out need to be addressed. The ethicality of the system will always remain a controversial issue, but system's fair use and positive results can overshadow the doubts concerning the citizen's breach of privacy. In such tough situation where India is facing terrorist and criminal activities on high instances, NETRA may prove to be a constructive measure towards a pragmatic change.

For monitoring huge amount of internet traffic flowing at high speed, trade-off between different parameters has to be practically addressed. Theoretically, many things look promising but these may not be practically feasible. In this regard, capabilities of this application are limited right now but scope for improvements looks promising. If high channel and bandwidth issues can be monitored along with the concerned problems identified in the study, NETRA could become a powerful internet monitoring tool for government of India.

Moreover, NETRA alone looks to be weak in spying the content and measure unwanted activities in the Internet Traffic. Based on the analysis of the surveillance system, a mini but customized monitoring application can be developed to monitor specific application's data. It will work on multiple types of data with implementation of lightweight schemes. However, the real implementation needs to be done with the help of support from Government or Technology Partner. Nevertheless, this study can be helpful in preparing the framework and consider critical factors while preparing the design of a new system.

References

[1]UNODC, "UNODC Report on the Use of Internet for Terrorist purposes". 2012. Available at http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf on 10th June 2016

[2]Pradhan, S.D., "Cyber security: Need for an overall national cyber strategy". Times of India. January 18, 2016. Available at http://blogs.timesofindia.indiatimes.com/ChanakyaCode/cyber-security-need-for-an-overall-national-cyber-strategy/

[3]Berger, J.M., “The Evolution of Terrorist Propaganda: The Paris Attack and Social Media”. January 27, 2015. Available at https://www.brookings.edu/testimonies/the-evolution-of-terrorist-propaganda-the-paris-attack-and-social-media/

[4]Bhattacharya, R., “Indian companies faced cyber-attack in 2015: KPMG survey”. The Economic Times. December 1, 2015. Available at http://articles.economictimes.indiatimes.com/2015-12-01/news/68688315_1_cyber-risks-cyber-forensicskpmg-survey

[5]Sukumar, A. M., & Sharma, C. R., “The Cyber Command: Upgrading India's National Security Architecture”. 2016. Available at http://www.orfonline.org/wp-content/uploads/2016/03/SR_9_Arun-Mohan-Sukumar-and-RK-sharma.pdf on 15th September 2016

[6]Caceres, R., Duffield, N., Feldmann, A., Friedmann, J. D., Greenberg, A., Greer, R., & van der Memle, J. E., “Measurement and analysis of IP network usage and behavior”. Communications Magazine. IEEE. Vol. 38, Issue 5. Pp 144-151. 2000. http://dx.doi.org/10.1109/35.841839

[7]Wadhwani, D., “NETRA – You will be under surveillance by Indian Internet Spy System”. Security. Home page. 2014. Available at http://newtecharticles.com/netra-indian-government-internet-spy-system/ on 9th June, 2016

[8]Zander, S., Nguyen, T., & Armitage, G., “Automated traffic classification and application identification using machine learning”. In The IEEE Conference on Local Computer Networks 30th Anniversary (LCN'05) l. Pp. 250-257. November, 2005. http://dx.doi.org/10.1109/LCN.2005.35

[9]Zander, S., Nguyen, T., & Armitage, G., “Self-learning IP traffic classification based on statistical flow characteristics”. In International Workshop on Passive and Active Network Measurement. Springer Berlin Heidelberg. Pp. 325-328. March, 2005. http://dx.doi.org/10.1007/978-3-540-31966-5_26

[10]Boyd, J. E., Meloche, J., & Vardi, Y., “Statistical tracking in video traffic surveillance”. In Computer Vision. The Proceedings of the Seventh IEEE International Conference Vol. 1. pp. 163-168. 1999. http://dx.doi.org/10.1109/ICCV.1999.791213

[11]Wang, X., Chen, S., & Jajodia, S., “Tracking anonymous peer-to-peer VoIP calls on the internet”. In Proceedings of the 12th ACM conference on Computer and communications security. Pp. 81-91. November, 2005. http://dx.doi.org/10.1145/1102120.1102133

[12]Gavalas, D., Greenwood, D., Ghanbari, M., & O'Mahony, M., “Advanced network monitoring applications based on mobile/intelligent agent technology”. Computer Communications. Vol.23, Issue 8. Pp. 720-730. 2000. http://dx.doi.org/10.1016/S0140-3664(99)00232-7

[13] Anagnostakis, K. G., Ioannidis, S., Miltchev, S., Greenwald, M., Smith, J. M., & Ioannidis, J., "Efficient packet monitoring for network management", In Network Operations and Management Symposium (NOMS 2002). IEEE/IFIP, pp. 423-436. 2002. Available at http://repository.upenn.edu/cgi/viewcontent.cgi?article=1041&context=cis_papers

[14] Liotta, A., Pavlou, G., & Knight, G., "Exploiting agent mobility for large-scale network monitoring". IEEE network. Vol. 16, Issue 3. Pp. 7-15. 2002. http://dx.doi.org/10.1109/MNET.2002.1002994

[15] Chen, Y., Bindel, D., Song, H., & Katz, R. H., "An algebraic approach to practical and scalable overlay network monitoring". In ACM SIGCOMM Computer Communication. Review. Vol. 34, Issue 4. Pp 55-66. August, 2004. http://dx.doi.org/10.1145/1015467.1015475

[16] Ho, T., Leong, B., Chang, Y. H., Wen, Y., & Koetter, R., "Network monitoring in multicast networks using network coding". In Proceedings. International Symposium on Information Theory (ISIT 2005). IEEE. Pp. 1977-1981. September, 2005. http://dx.doi.org/10.1109/ISIT.2005.1523691

[17] Leners, J. B., Wu, H., Hung, W. L., Aguilera, M. K., & Walfish, M., "Detecting failures in distributed systems with the falcon spy network". In Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles. Pp. 279-294. October, 2011. http://dx.doi.org/10.1145/2043556.2043583

[18] Turon, M., "Mote-view: A sensor network monitoring and management tool". In The Second IEEE Workshop on Embedded Networked Sensors. EmNetS-II. Pp. 11-17. May, 2005. http://dx.doi.org/10.1109/EMNETS.2005.1469094

[19] Han, S. H., Kim, M. S., Ju, H. T., & Hong, J. W. K., "The architecture of ng-mon: A passive network monitoring system for high-speed ip networks1". In International Workshop on Distributed Systems: Operations and Management. Springer Berlin Heidelberg. pp. 16-27. October, 2002. http://dx.doi.org/10.1007/3-540-36110-3_5

[20] Xynou, M., "Report on the 3rd Privacy Round Table meeting". Centre for Internet & Society. Internet-governance. May, 2013. Available at http://cis-india.org/internet-governance/blog/report-on-the-third-privacy-round-table-meeting

[21] Ghosh, M., "Beware, Government Plans To Spy On Your Internet Activity Using Netra". Trak.in_tags_business. 2013. Available at http://trak.in/tags/business/2013/12/17/govt-spy-internet-netra/ on 9th June, 2016.

[22] Parbat, K., "Government to launch 'Netra' for internet surveillance". Home Ministry. Collections. Home. 2013. Available at http://articles.economictimes.indiatimes.com/2013-12-16/news/45256400_1_security-agencies-drdo-cabinet-secretariat on 9th June, 2016

[23] "Statistics and facts about Facebook". Statista. Home. Industries. Internet. Social Media & User-Generated Content. Facebook - Statistics & Facts. 2016. Available at https://www.statista.com/topics/751/facebook/

[24] Radicati, S., & Hoang, Q., "Email statistics report, 2012-2016". The Radicati Group. Inc., London. 2012. Available at http://www.Radicati.com/wp/wp-content/uploads/2012/04/Email-Statistics-Report-2012-2016-Executive-Summary.pdf

[25] Singh, V.P., "Myopic Netra: why the new system has failed to deliver". February 2, 2015. Available at http://www.governancenow.com/gov-next/egov/myopic-netra-new-cyber-tracking-system-failed-deliver

[26] Chandler, P., "ECHELON -- The Spy System That Knows Everything, philipcfromnyc". 2013. Available at http://philipcfromnyc.hubpages.com/hub/ECHELON----The-Spy-System-That-Knows-Everything/ on 4th March, 2016.

[27] Bomford, A., "The Echelon spy network". Echelon spy network revealed. November 3, 1999. Wednesday, 11:35 GMT. Available at http://news.bbc.co.uk/2/hi/503224.stm

[28] ECHELON. "Exposing the NSA's Global Spy Network". Alexandra Valiente. 2013.

[29] Hahn, D, J., "DISHFIRE: The Program That Lets the NSA Capture Almost 200 Million Texts a Day". 2014. Available at http://www.complex.com/pop-culture/2014/01/dishfire-nsa-collects-texts on 4th march, 2016.

[30] Greenwald, G. & MacAskill, E., "NSA Prism program taps in to user data of Apple, Google and others". 2013. Available at http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-dataon 4th march, 2016.

[31] Yu, Hongkun, Jingbo Shang, Meichun Hsu, Malu Castellanos, and Jiawei Han. "Data-Driven Contextual Valence Shifter Quantification for Multi-Theme Sentiment Analysis." In *Proceedings of the 25th ACM International on Conference on Information and Knowledge Management*, pp. 939-948. ACM, 2016. http://dx.doi.org/10.1145/2983323.2983793

[32] Ball, J., Borger, J. and Greenwald, G., "Revealed: how US and UK spy agencies defeat internet privacy and security", The Gaurdian, 2013. Available at https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security on 14th July 2016

[33] Wild Packets., "Network Forensics in a 10G World". White Paper. 2013. Available at http://www.wildpackets.com/elements/whitepapers/network_forensics_in_a_10_g_world.pdf

[34] Smith, C., "By the Numbers: 17 Staggering Dropbox Statistics (May 2016)", DMR Stats. Accessed from http://expandedramblings.com/index.php/dropbox-statistics/ on November 12, 2016

[35] Gupta, R., Aggarwal, A., & Pal, S. K., "Design and Analysis of New Shuffle Encryption Schemes for Multimedia". Defence Science Journal. Vol. 62, Issue 3. Pp. 159-166. 2012. http://dx.doi.org/10.14429/dsj.62.1008

[36] Wei, D., & Ansari, N., "IP traffic monitoring: An overview and future considerations". In Advances in Multimedia Information Processing—PCM. Springer Berlin Heidelberg. Pp. 335-342. 2001. http://dx.doi.org/10.1007/3-540-45453-5_43

[37] Cecil, A., "A summary of network traffic monitoring and analysis techniques". Computer Systems Analysis. Pp. 4-7. 2012. Available at http://www1.cse.wustl.edu/~jain/cse567-06/ftp/net_monitoring.pdf

[38] Bendrath, R., & Mueller, M., "The end of the net as we know it? Deep packet inspection and internet governance". New Media & Society. Vol.13, Issue 7. Pp 1142-1160. 2011. http://dx.doi.org/10.1177/1461444811398031

[39] Gupta, R., Muttoo, S. K., & Pal, S. K., "Web Mining and Analytics for Improving E-Government Services in India". Web Usage Mining Techniques and Applications Across Industries. Pp. 223-247. 2016c.

[40] Takhar. S, et al., "If I Was ... Analyzing Edward Snowden". National Security Agency, USA. 2014.

[41] Crovella, M. E., & Bestavros, A., "Self-similarity in World Wide Web traffic: evidence and possible causes". Networking. IEEE/ACM Transactions. Vol. 5, Issue 6. Pp. 835-846. 1997. http://dx.doi.org/10.1109/90.650143

[42] Boxma, O. J., "Fluid queues and regular variation". Performance Evaluation. Vol. 27. Pp 699-712. 1996. http://dx.doi.org/10.1016/S0166-5316(96)90052-8

[43] Tsybakov, B., & Georganas, N. D., "Self-similar processes in communications networks". IEEE Transactions on Information Theory, Vol. 44, Issue 5. Pp. 1713-1725. 1998. http://dx.doi.org/10.1109/18.705538

[44] Roberts, J. W., "Traffic theory and the Internet". Communications Magazine. IEEE. Vol. 39, Issue 1. Pp. 94-99. 2001. http://dx.doi.org/10.1109/35.894382

[45] Agarwal, D., González, J. M., Jin, G., & Tierney, B., "An infrastructure for passive network monitoring of application data streams", Lawrence Berkeley National Laboratory. 2003. Available at http://escholarship.org/uc/item/66j721d5

[46] Gupta, R., Pal, S. K., & Muttoo, S. K., "Network Monitoring and Internet Traffic Surveillance System: Issues and Challenges in India". In Intelligent Systems Technologies and Applications. Springer International Publishing. Pp. 57-65. 2016a. http://dx.doi.org/10.1007/978-3-319-23258-4_6

[47] Gupta, R., Muttoo, S. K., & Pal, S. K., “Binary Division Fuzzy C-Means Clustering and Particle Swarm Optimization based Efficient Intrusion Detection for E-Governance Systems”. International Review on Computers and Software (IRECOS). Vol. 11, Issue 8. Pp. 672-681. 2016b. https://doi.org/10.15866/irecos.v11i8.9546

[48] Elhag, Salma, Alberto Fernández, Abdullah Bawakid, Saleh Alshomrani, and Francisco Herrera. "On the combination of genetic fuzzy systems and pairwise learning for improving detection rates on Intrusion Detection Systems." Expert Systems with Applications. Vol. 42, Issues 1, Pp. 193-202, 2015. http://dx.doi.org/10.1016/j.eswa.2014.08.002

Copyright Disclaimer