Imperial Journal of Interdisciplinary Research (IJIR)
Vol-2, Issue-3 , 2016
ISSN : 2454-1362 , http://www.onlinejournal.in

Cyberstalking and Cyberbullying: Effects and prevention measures

A. M. Chandrashekhar[1] , Muktha G S[2] & Anjana D K[3]
[1]Assistant. Professor, Dept of computer science and Engineering, Sri Jayachamarajendra College of Engineering, Mysuru, India.
[2&3]MTech Student, Computer Engineering, Dept of computer science and Engineering, Sri Jayachamarajendra College of Engineering, Mysuru, India.

Abstract

With the advancement in technology, online harassment is also becoming more prevalent. Cyberstalking and cyberbullying are two such social problems where a user is deliberately and persistently abused online. These issues have created new challenges for the detection, and prevention of such phenomenon as it is inadequate to just use the traditional methods such as identification by witnesses and enforcing restraining orders. The cyber stalkers and cyberbullies disguise themselves using the Internet without the fear of any consequence and target victims.

In this paper we examine the nature and extent of cyberstalking and cyberbullying and their impact on the victim's mindset. This study can help in figuring out some means for preventing such online abuse.

1. Introduction

Cybersecurity is a major issue for business organizations and individuals alike. The Internet has increasingly become a platform for online predators, wherein one party in a relationship seeks to control, ill-treat, exploit, or hurt the other party by harassment. Cyberstalking is the convergence of stalking and cyberspace wherein over a period of time the stalker gains access and control to a victim. Cyberbullying is the repeated, intentional and often anonymous act done to hurt another person through text messages from a cell phone, e-mail, social networking web sites, chat rooms, and instantaneous messaging. It can be committed by a single person or a gang of people. Anyone can become a target of cyberstalking. Cyberbullying usually refers to kids or adolescents being the victims or targets—more specifically students of public or private schools are the victims. When cyberbullying includes observing someone furtively, following and targeting people's online activities, it is called as cyberstalking.

1.1 Legal definition

Cyberbullying is specified in legal dictionary as "activity that uses information and communication technologies to support deliberate, continuous, and aggressive conduct by an individual or a group of people, that is intended to harm someone, physically or emotionally"[1].

The practice of cyberbullying or cyberstalking is not limited to kids or adolescents, the practice is recognized by the same meaning when it is done by adults also. The contrast in age groups refers to this online abuse as cyber stalking when committed by adults towards adults. Common strategy used by cyberstalkers or cyberbullies are accomplished in public platforms, social networking sites or online data sites and are intended to intimidate a target's salary, reputation, privacy, security or employment. Conduct may involve persuading others to pester the target and trying to influence a victim's online interaction. Cyberstalkers usually try to hurt the stature of their victim.

Motivation to perform cyber harassment [2] comes from due to different reasons. These reasons can range from harasser seeking entertainment to boredom to personal vendettas, and also include:

- Revenge
- Fear
- Jealousy
- Anger
- Righteousness
- Bigotry
- To get the attention of the target or others

Sometimes the cyber harasser has no motive at all, and the victim was targeted just because they were in the wrong place at the wrong time. It becomes a cybercrime of convenience.

Along with trying to figure out the motives behind these online harassment problems, it also necessary to know how severely such acts impact the victim. Sometimes the victims get so depressed that they might consider committing suicide or taking revenge on the attacker in the cruelest means possible. The victim might lose his/her own mental stability. So, there is high need of incorporating a system which detects online harassment like cyberstalking and cyberstalking. With the presence of such systems these issues can be highly reduced.

2. Literature Survey

Handbooks to guide the public, professors and parents conclude, "Cyberbullying is being brutal to others by dispatching or posting hurtful posts using a mobile phone or the internet." Investigation, legislation and schooling in the field are under process. Basic definitions and general rules to help identify and manage what is regarded as abuse of e-media and electronic intercommunications have been identified. Cyberbullying involves iterated intrusion with the intention to hurt the victim.

2.1 Types of Cyberbullying and Cyberstalking

Seven Types of Cyberbullying and Cyberstalking are briefed below

1. **Trolling and Flaming:** This category includes posting mean spirited, rude or angry messages
2. **Excluding:** For malicious reasons leaving someone out of an online group.
3. **Masquerading:** Creating media profiles in Facebook, Twitter or other social networking sites as someone else in order to damage the reputation of the victim.
4. **Mobbing:** A group of people forming a gang and sending hundreds of text messages to the victim's system. This is similar to the Denial of Service problem.
5. **Denigrating:** Posting or sending some cruel and embarrassing material like personal text, photos, etc. about the individual to others and demeaning the person in other's view.
6. **Outing:** With the intent of embarrassing or harming a person, posting or sending out private information about someone without that person's permission.
7. **Harassing:** Repeatedly sending unwanted messages to another person.

Cyber stalking can touch anyone, including adults**.** Children, however, are popular victims. Other people who might be victims of cyberstalking include:

- Handicapped persons
- The elderly
- People who spend a lot of time on the Internet
- People who've attempted to break up with someone or divorce them
- Employers (by fired ex-employees)
- People who know or have been introduced to or who have worked with mentally ill individuals (who often form unhealthy or abnormal obsessions or liking for someone else).

2.2 Areas of victimization:

The recent use of cell phone apps and increase in use of smartphones have made cyberbullying more accessible. It is regarded that cyberbullying through these platforms will affect the victim to a greater extent than the usual more stationary internet platforms. Along with this, the amalgamation of Internet access and cameras and the instant availability of these new generation smartphone technologies have led to a different type of bullying that was not present earlier. People who are bullied through online means experience a broader range of bullying than those encountered elsewhere[3][4].

While most cases are considered to be cyberbullying, some teens argue that most events are simply drama. Percentage of where the teens are being Cyberbulled is shoen in figure 1. For example, Danah Boyd writes, "teens regularly used that word [drama] to describe various forms of interpersonal conflict that ranged from insignificant joking around to serious jealousy-driven relational aggression. Whereas adults might have labeled many of these practices as bullying, teens saw them as drama. Drama among teens has existed for years but now that it is easier to share information through social media, it seems that simple drama gets out of control"[5].

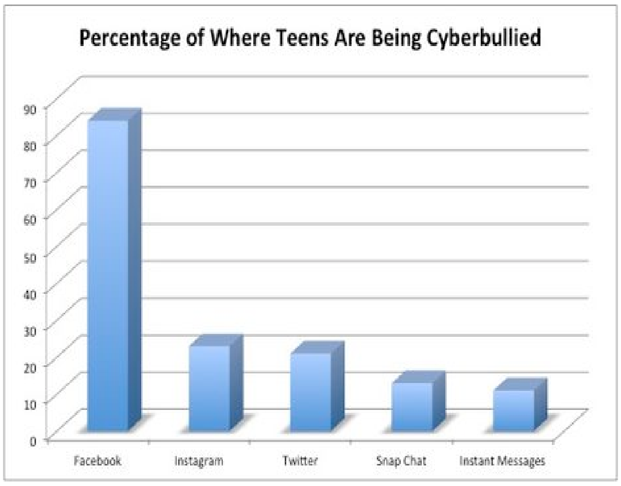

Fig. 1: Percentage of the teens being Cyberbulled

2.3 In social media

Cyberbullying can take place on social media sites such as Facebook, Myspace, and Twitter. "By 2008, 93% of young people between the ages of 12 and 17 were online. In fact, youth spend more time with media than any single other activity besides sleeping. There are many risks attached to social media sites, and cyberbullying is one of the larger risks. One million children were harassed, threatened or subjected to other forms of cyberbullying on Facebook during the past year, while 90 percent of social-media-using teens who have witnessed online cruelty say they have ignored mean behavior on social media, and 35 percent have done this frequently. 95 percent of social-media-using teens who have witnessed cruel behavior on social networking sites say they have seen others ignoring the mean behavior, and 55 percent witness this frequently. According to a 2013 Pew Research study, eight out of 10 teens who use social media share more information about themselves than they have in the past. This includes location, images, and contact information.

The most recent case of cyber-bullying and illegal activity on Facebook involved a memorial page for the young boys who lost their lives to suicide due to anti-gay bullying. The page quickly turned into a virtual grave desecration and platform condoning gay teen suicide and the murdering of homosexuals. Photos were posted of executed homosexuals, desecrated photos of the boys who died and supposed snuff photos of gays who have been murdered. Along with this were thousands of comments encouraging murder sprees against gays, encouragement of gay teen suicide, death threats etc. In addition, the page continually exhibited pornography to minors. In order to protect children, it's important that personal information such as age, birthday, school/church, phone number, etc. be kept confidential [6].

Cyberbullying can also take place through the use of websites belonging to certain groups to effectively request the targeting of another individual or group. An example of this is the bullying of climate scientists and activists.

2.5 In gaming

Sexual harassment as a form of cyberbullying is common in video game culture. A study by the Journal of Experimental Social Psychology suggests that this harassment is due in part to the portrayal of women in video games. This harassment generally involves slurs directed towards women, sex role stereotyping, and overaggressive language. Keza MacDonald writes in The Guardian that sexism exists in gaming culture, but is not mainstream within it.

A study from National Sun Yat-sen University observed that children who enjoyed violent video games were significantly more likely to both experience and perpetrate cyberbullying.

2.6 In search engines

Information cascades happen when users start passing on information they assume to be true, but cannot know to be true, based on information on what other users are doing. Information cascades can be accelerated by search engines' ranking technologies and their tendency to return results relevant to a user's previous interests. This type of information spreading is hard to stop. Information cascades over social media and the Internet may also be harmless, and may contain truthful information.

Cyberstalkers use Google bombs (a term applicable to any search engine) to increase the eminence of favored posts sorted by the most popular searches, done by linking to those posts from as many other web pages as possible. Google bombs can manipulate the Internet's search engines regardless of how authentic the pages are, but there is a way to counteract this type of manipulation as well.

According to Nelson, a lawyer against internet crimes, "cyber bullying is often very serious, including stalking and death threat. I can say anything I want. It's impersonal. Face to face is a little intimidating"[7-10] Cyberbullying incidents have been reported all over the world by many new stories. Cyberbullying also takes various forms and electronic communication tools - from email, mobile phone, listserve, to websites. Once such example of cyberbullying is of a 15 year old boy from Canada who became an unwilling celebrity when a film he made of himself emulating a Star Wars fight scene was posted on the Internet by some of his classmates. Millions of watchers downloaded the two-minute clip. He was so humiliated he sought counseling, and his family has launched a lawsuit against his tormentors" (Snider & Borel, 2004).

3. Proposed system

This section discus the different problems associated.

3.1 The Cyberstalker's problem:

The Cyberstalker's problem[11] is a three party communication game involving a Victim (Alice), the

Stalker (Bob) and a Monitor see Figure 2. Bob and Alice are linked by a communication channel which can be accessed by the Monitor. The goal of Bob is to harass Alice while the goal of the Monitor is to record any such activity. In the traditional cryptographic terminology, Bob wants to establish a (virtual) harassment channel, while the Monitor wants to track it and record its content.

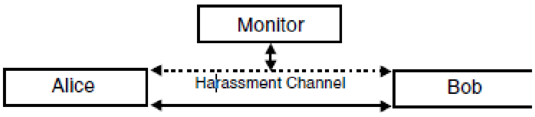

Figure 2: The Cyberstalker's problem: The Monitor has to capture harassment data exchanged by Alice and Bob.

3.2 Prisoner's Problem:

This problem is related to the classical Prisoner's problem [12-14] in Steganography (Information Hiding) which also involves three parties. In this case, Bob is incarcerated, Alice is free and the Monitor (Wendy) is a Warden see Figure 3. Alice has hatched out an escape plan and visits Bob with the intention of passing on details of her plan. Any exchange of information must take place in the presence of Wendy. To succeed, Alice must hide her escape plan in what appears to be innocuous information. If Wendy detects that secret information is hidden in their communication then the Bob's escape will be thwarted. The channel that Alice and Bob want to establish is called a subliminal (or covert) channel.

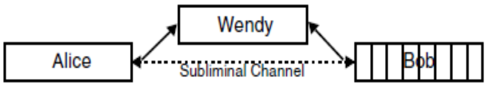

Figure 3: The Prisoners's problem: Wendy has to prevent Alice from sending Bob a covert message.

3.3 Man-in-the-middle problem:

The man-in-the-middle problem is a similar problem that has been extensively studied in Cryptography. In this case the Monitor is the adversary (Eve) see Figure 4. Eve may be passive and simply eavesdrop on the communication between Alice and Bob, and/or active. An active adversary can corrupt messages sent to Bob (or Alice) by Alice (Bob) or impersonate one party to the other.

The last two problems are fundamental to Steganography and Cryptography, and define their respective threat models. Dealing with them has been the focus of research in these disciplines. What characterizes all three problems is their adversarial nature. In the Cyberstalker's problem the Stalker is the adversary and the other two collaborate to detect and record any harassment.

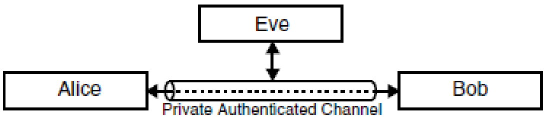

Figure 4: The man-in-the-middle problem: Alice and Bob have to establish a private and/or authenticated communication channel in the presence of Eve.

In the Prisoner's problem, Alice and Bob conspire to establish a subliminal channel. For this problem, they are the adversary. The Warden's goal is to make sure that their communication channel is subliminal-free. In the man-in-the-middle problem, Eve is the adversary. Eve's task is to undermine the privacy and/or authenticity of the communication between Alice and Bob. Alice and Bob want to establish a private and/or authentication channel to secure their communication.

The Cyberstalker's problem focuses on capturing harassment data rather than direct prevention of harassment, while the other two problems focus on prevention. This makes it easier in some respects to deal with cyberstalking at least from a cryptographic point of view. The main difficulties are the forensics aspects of (i) the data capturing process and (ii) the verification of the captured data. Security is based on the data's evidentiary value.

3.4 A Cyberstalker Monitor system

Next the secure solutions to these problems are considered. These will be based on a monitoring system that captures harassment data in such a way that both the capturing process and the data will be admissible evidence in a criminal court.

The Monitor is a tool meant to complement traditional forensics tools[15-18]. It may not directly identify the stalker, but will allow investigators to uncover patterns of behavior, trails to computers that the stalker may have used, and other potentially relevant forensic data that would have been discarded otherwise.

First approach: a low-tech analog solution

To have a law enforcement agent alongside the victim to monitor cyberstalking sessions is an obvious solution. A more practical solution is to replace the agent by a closed-circuit television camera and a recorder to monitor the sessions see Figure 5. Although both these solutions provide evidence of stalking, they offer only a weak binding of the stalker to the session. To strengthen the link, evidence from the actual TCP/IP packets received could be helpful.

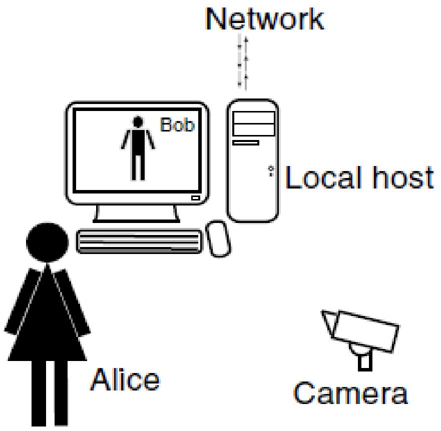

Figure 5: A low-tech solution: harassment data is captured on a closed-circuit television camera.

Second approach: A basic Cyberstalker Monitor system

A blackbox monitor[19-21] that captures the local host data and also the relevant network data is used in this approach. (see Figure 6). The local host data includes data on the personal computer of the victim: the contents of the audio buffer, screen buffer, mouse data and keystrokes, so on. Excluding machine generated overhead, all the incoming/outgoing network packets data are included in relevant network data. The data is captured and stored in the monitor (most possibly a hard drive) locally.

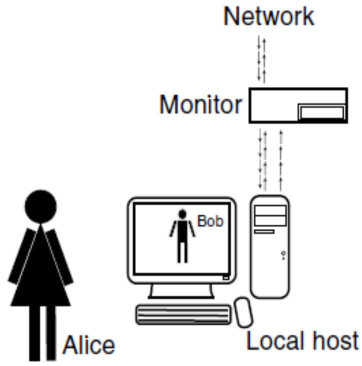

Figure 6: The Cyberstalker Monitor System captures and stores local host data and network data.

The Monitor contains a transparent network bridge with connections to the network (Internet) and the local host (the victim's personal computer) and a storage device (see Figure 7). The storage device has two modules.

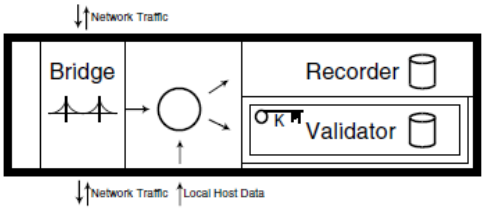

Figure 7: The Monitor has a transparent network bridge, a Recorder and a Validator.

The Recorder captures local host data and network data. The Validator is a physically secure entity that stores evidence, integrity data and a cryptographic key (K). The Monitor operates on the concept of a session. The session is an integral quantity in this model. A session is initiated upon the victim's connection to the network and lasts until the victim disconnects. During the session, the local host data is stored on the Recorder and authenticated using a keyed hash function HMAK with hash function SHA-1[22-24].

The hash function produces a digest which is the evidence integrity data. A symmetric key is used that is stored in a secured (tamper-resistant) region of the Validator (and cannot be extracted). A duplicate key is kept in the forensics lab of the law enforcement agency. To validate captured data for use as evidence in court, the data and its integrity validator are extracted and the duplicate key is used to validate the data. The cryptographic details of the process of validation of the integrity of the evidence data are as follows. Let

$$data_{session(sn)} = \left(cn, sn, T_{lh}, T_{mon}, \{data_{lh}, data_{mon}\}, T^*_{lh}, T^*_{mon}\right)$$

be the data with case number *cn*, session number *sn*, start timestamps ; , end timestamps ; , for the local host and Monitor respectively, and session stream data ; }, formatted in such a way that it can be hashed as a stream, and let

$$\mathrm{HMAC}_{K_{cn}}^{\mathrm{SHA}}(data_{session(sn)})$$

be its HMAC digest with hash function SHA-1 and key Kcn. The data integrity validator [25] is,

$$integrity\_validator_{session(sn)} = \left(cn, sn, \mathrm{HMAC}_{K_{cn}}^{\mathrm{SHA}}(data_{session(sn)})\right).$$

To validate extracted data, the duplicate key is used to compute its keyed digest and the result is compared with the integrity validator for that session. If the values agree, then the data has not been corrupted.

Although it might be tempting to send the integrity validation data (the digest) through the existing network directly to the forensics lab for secure storage, this should be avoided because it violates the transparency of the bridge. This makes it possible for the stalker to detect the presence of the Monitor. A crucial security requirement is the separation of the functions of the local host and of the monitor.

3.5 Securing the Cyberstalking Monitor

The symmetric key used in the Cyberstalker Monitor[26] can be replaced with an asymmetric key, *e.g.*, a DSS key. In this case a private key SKcn is stored in the Validator module and the corresponding public key PKcn is stored in the forensics lab (see Figure 8). This strengthens the evidentiary value of the captured data and extends the chain-of-custody (secrecy is not needed for the public key PKcn), but does not offer any other significant advantage.

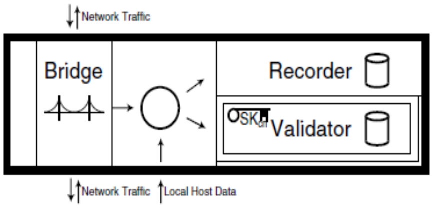

Figure 8: The Monitor with an asymmetric key.

A significant security advantage is achieved by separating the duties of the Recorder and Validator. For this purpose, an independent communication channel (one that is not associated with the victim in any way) can be used to send the evidence integrity validation (the digest) to the forensics lab, where it is securely logged. For practical purposes we may use wireless communication technology to broadcast securely to a network controlled by the law enforcement agency. Figure 9 illustrates an application which uses wireless technologies.

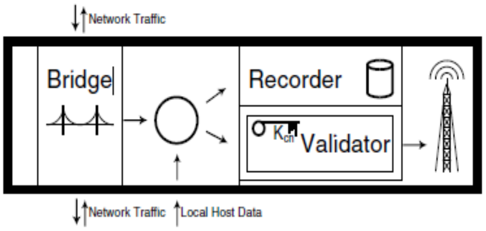

Figure 9: The Monitor with a wireless device.

Additional functionality can be enabled using the independent communication channel to make the system more flexible.Virtual Network Computing(VNC) can be used with a high bandwidth channel to allow the investigator to remotely monitor and control the victim's desktop[27-29]. Important system information present in session "reports" (information such as remaining disk space, amount of data recorded, etc.) can also be sent to the investigator. Snapshots of important events (images of text messages) that have been tagged by the victim can also be included in the reports. Finally this channel can be used to synchronize the clock of the Monitor to the clock of the forensics lab. Such enhancements help the investigator to monitor the case more closely and then respond in person if required.

3.6 Responding to Cyberharassment

The Internet cyberstalking law is designed to prosecute people for using electronic means to repeatedly threaten, disturb or harass someone online.

Cyberstalkers can hide their identities when contacting their victim's students. Further, cyberharassment can cross over into physical assaults. Online harassment has led to fights, and in some cases, stabbings, murder and suicide[30].

Cyberstalking and Cyberbullying poses unique challenges to officials because:

- Police may be hesitant to provide protection when targets can't identify anonymous stalkers.
- Assuming online partners will never meet, authorities may minimize reports.
- Cyberstalkers can sometimes learn a target's true identity, location and routines while the target can't pinpoint them.
- Cyberstalkers can use cyberspace to publicly compound a target's distress.

Justice Department recommends advising a target to take the following steps[31]:

1. Tell the person not to make contact again.
2. Save all communications for evidence. Do

not alter them in any way. Keep electronic copies, not just print-outs.

3. Save any information that suggests a violent threat and contact law enforcement.
4. If the harassment continues, contact the harasser's Internet service provider[32]. The ISPs prohibit using their service for abusive purposes. An ISP can often intervene by directly contacting the stalker or closing his account.
5. Keep a record of your contacts with ISP officials or law enforcement officials.
6. When contacting police, provide specific details such as any tangible evidence you've collected. In cases of a serious threat, police can refer the matter to state or federal authorities for investigation. The stalker may be prosecuted in court.
7. If the target is afraid to act, find help through other resources, such as Wired Safety [33].

4. Conclusion

Cyberstalking and cyberbullying is a crime. This can mentally and physically affect the victim and there can be dangerous consequences to such harassment. These online harassments are felonies if they involve a “credible threat”. If the victim is in fear for his/her own safety or the safety of his/her family members then it is called a credible threat. The threat is made with the obvious intention to perform the threat and cause harm. It does not matter whether the person who made the threat actually intended to carry it out or not. Cyberstalking and cyberbullying is becoming an increasingly significant problem for schools and society in general. Therefore this paper outlines the nature and extent to which these problems are prevalent in today's society and provides solutions to put a brake to such online harassment. The society should be more aware of the existence of such problems and take measures in order to not fall prey to cyber stalkers and bullies.

REFERENCES:

[1]. Cyberbullying A school psychology by Nicole M. Aune

[2]. Cyberbullies on Campus by Darby Dickerson

[3]. Bullying in the new playground: Research into cyberbullying and cyber victimization Qing Li, University of Calgary

[4].Cyberstalking: Dangers on the Information Superhighway *By: Trudy M. Gregorie, Director of Training, National Center for Victims of Crime, 2001*

[5].Machine Learning Solutions for controlling Cyberbullying and Cyberstalking by Zinnar Ghasem, Ingo Frommholz, Carsten Maple, University of Bedfordshire.

[6]. ICT Penetration and Cybercrime in India: A Review

By Anand Kumar Shrivastav *Research Scholar, Department of Computer Science, Mewar University, Chittorgarh, India* Dr. Ekata, *Associate Professor, Deptt. of Applied Science, Krishna Institute of Technology, Ghaziabad, India*

[7].Cyberstalking: an exploratory study of students at a mid-atlantic university.

[8].A.M.Chandrashekhar and K. Raghuveer, “Fusion of Multiple Data Mining Techniques for Effective Network Intrusion Detection – A Contemporary Approach”, Proceedings of The 5th International Conference on Security of Information and Networks (SIN 2012), 2012, pp 33-37.

[9].A.M.Chandrashekhar and K. Raghuveer , “Intrusion Detection Technique by using K-means, Fuzzy Neural Network and SVM classifiers”, 2013 IEEE International Conference on Computer Communication and Informatics (ICCCI -2013), 4~06,Jan2013, IEEE Catalog Number: CFP1308R-ART, ISBN Number: 978-1-4673-2907-1.

[10].A.M.Chandrashekhar and K. Raghuveer, “An Effective Technique for Intrusion Detection using Neuro-Fuzzy and Radial SVM Classifier”, The Fourth International Conference on Networks & Communications (NetCom-2012), 22~24, Dec-2012.

[11].Tracking cyberstalkers: a cryptographic approach by Mike Burmester, Peter Henry, Leo S. Kermes, Department of Computer Science, Florida State University, Tallahassee

[12].A.M.Chandrashekhar and K. Raghuveer, “Confederation of FCM Clustering, ANN and SVM Techniques of Data mining to Implement Hybrid NIDS Using Corrected KDD Cup Dataset”, IEEE International Conference on Communication and Signal Processing (ICCSP),2014, pp 672-676.

[13].A.M.Chandrashekhar and K.Raghuveer, “Hard Clustering Vs. Soft Clustering: A Close Contest for Attaining Supremacy in Hybrid NIDS Development”, Proceedings of International Conference on Communication and Computing (ICC - 2014), Elsevier science and Technology Publications.

[14].A.M.Chandrashekhar and K.Raghuveer, “Amalgamation of K-means clustering algorithem with standard MLP and SVM based neural networks to implement network intrusion detection system”, Advanced Computing, Networking, and Informatics –Volume 2(June 2014), Volume 28 of the series Smart Inovation, Systems and Technologies pp 273-283.

[15].A.M.Chandrashekhar and K.Raghuveer, “Diverse and Conglomerate Modi-operandi for Anomaly Intrusion Detection Systems”, International Journal of Computer Application (**IJCA)** Special Issue on “Network Security and Cryptography (NSC)”, 2011.

[16].A.M.Chandrashekhar and K. Raghuveer, "Performance evaluation of data clustering techniques using KDD Cup-99 Intrusion detection data set", International Journal of Information and Network Security (**IJINS**), ISSN: 2089-3299, Vol-1, No.4, October 2012, pp. 294~305.

[17].A.M.Chandrashekhar and K. Raghuveer, "Fortification of hybrid intrusion detection system using variants of neural networks and support vector machines", International Journal of Network Security & Its Applications (IJNSA) ISSN: 0974-9330[online]& 0975-2307[print].Vol.5, Number 1, January 2013.

[18].A.M.Chandrashekhar and K.Raghuveer , "Improvising Intrusion detection precision of ANN based NIDS by incorporating various data Normalization Technique – A Performance Appraisal", International Journal of Research in Engineering & Advanced Technology(IJREAT), Volume 2, Issue 2, Apr-May, 2014.

[19].,A.M.Chandrashekhar, Puneeth L Sankadal "Network Security situation awareness system" International Journal of Advanced Research in Information and Communication Engineering(IJARICE), Volume 3, Issue 5, May 2015.

[20]A.M.Chandrashekhar,.Prashanth G M, "Secured infrastructure for multiple group communication" International Journal of Advanced Research in Information and Communication Engineering (IJARICE), Volume 3, Issue 5, May 2015.

[21].Sowmyashree K.K, A.M.Chandrashekhar, "Pyramidal aggregation on Communication security" International Journal of Advanced Research in Computer Science and Applications (IJARCSA), Volume 3, Issue 5, May 2015.

[22].Huda Mirza Saifuddin, A.M.Chandrashekhar, "Exploration of the ingredients of original security" International Journal of Advanced Research in Computer Science and Applications(IJARCSA), Volume 3, Issue 5, May 2015.

[23].Syed Tahseen Ahmed, A.M.Chandrashekhar, "Analysis of Security Threats to Database Storage Systems" International Journal of Advanced Research in data mining and Cloud computing(IJARDC), Volume 3, Issue 5, May 2015.

[24].Yadunandan Huded, A.M.Chandrashekhar, "Advances in Information security risk practices" International Journal of Advanced Research in data mining and Cloud computing (IJARDC), Volume 3, Issue 5 May 2015.

[25].Madhura S Hegde, A.M.Chandrashekhar, "A Survey:Combined impact of cryptography and steganography" International Journal of Engineering Research (IJOER), Volume 3, Issue 5, May 2015.

[26].Koushik P, A.M.Chandrashekhar, Koushik P, "Information security threats, awareness and coginizance" International Journal for Technicle research in Engineering(IJTRE), Volume 2, Issue 9, May 2015.

[27].Rahil kumar Gupta and A.M.Chandrashekhar, "Role of information security awareness in success of an organization" International Journal of Research(IJR) Volume 2, Issue 6, May 2015.

[28].A.M.Chandrashekhar, Arpitha, Nidhishree G, "Efficient data accessibility in cloud with privacy and authenticity using key aggregation cryptosystem", International Journal for Technological research in Engineering (IJTRE), Volume 3, Issue 5, JAN-2016.

[29] A. M. Chandrashekhar, Sahana K, Yashaswini K, "Securing Cloud Environment using Firewall and VPN", "International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), Volume 6, Issue-1, January-2016.

[30].A.M.Chandrashekhar, Hariprasad M, Manjunath A, "The Importance of Big Data Analytics in the Field of Cyber Security", International journal of scientific research and development(IJSRD),*Volume 3, Issue 11, JAN-2016.*

[31].A.M.Chandrashekhar, Chitra K V, Sandhya Koti, "Security Fundamentals of Internet of Things", *International Journal of Research (IJR**), Volume 3, Issue no1, JAN-2016.***

[32].A.M.Chandrasekhar, Jagadish Revapgol, Vinayaka Pattanashetti, "Security Issues of Big Data in Networking", International Journal of Scientific Research in Science, Engineering and Technology (*IJSRSET),* Volume 2, Issue 1, JAN-2016.

[33] A. M. Chandrashekhar, Sahana K, Yashaswini K, "Securing Cloud Environment using Firewall and VPN", "International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), Volume 6, Issue-1, January-2016.