International Journal of Innovative Research in Engineering Science and Technology

APRIL 2018 ISSN 2320 –981X

CYBER STALKING

[1]Ms. Lavanya.L , [2]Ms.Manjula.G, [3]Mr.Muthu Kumar.S

1.Department of Computer Science and Engineering,

SNS College of Technology

Coimbatore,India 641035

lavanyalogu96@gmail.com

2.Department of Computer Science and Engineering,

SNS College of Technology

Coimbatore,India 641035

manjula.ganesan022@gmail.com

3.Department of Computer Science and Engineering,

SNS College of Technology

Coimbatore,India 641035

muthukumar.dn16@gmail.com

International Journal of Innovative Research in Engineering Science and Technology

APRIL 2018 ISSN 2320 –981X

CORRESPONDING AUTHOR:

Mr. Dr.S.RajaRanganathan M.Tech

Asst. Professor, SNS College of Technology

Coimbatore,India 641035

Email: rajaranganathan@hotmail.com

Contact:9787070077

Abstract- Cyber stalking is a PHP- MySql web based project that is very helpful to victims of internet and government. Cyber stalking is a criminal offense under various state anti-stalking, slander and harassment laws. A conviction can result in a restraining order, probation, or criminal penalties against the assailant, including jail.Cyber stalking cases differ from regular stalking in that it is technologically based, though some cyber stalkers escalate their harassment to include physical stalking as well. To make this cyber stalking cases easier to deal for the victim and to find out who has done the crime this project has developed a website which consists of all the basic information of the victim and the complaint the victim has posted.The project completely collects information from victims and stored details in database. Cyber police can view the complaint and generate a report on it.As soon as the complaint is posted by the victim with the use of their location their complaint is forwarded to the nearest police station and the nearest checkpost with that specified details the police will check for the problem and will provide the result.

Keywords:Cyber,stalking,complaint,theft, emergency.

1. **INTRODUCTION**

Cyber stalking is the use of the internet or other electronic means to stalk or harass an individual, group, or organization It may include false accusations, defamation, slander and libel It may also include monitoring, identity theft, threats, vandalism, solicitation or gathering information that may be used to threaten, embarrass or harass.

problem definition:

Cyber attack is done on internet users, immediately they have to report online. Our project completely collects information from victims and stored details in database. Cyber stalking cases differ from regular stalking in that it is technologically based, though some cyber stalkers escalate their harassment to include physical stalking as well. A cyber stalker acts of out of

anger, or a need to control, or gain revenge over another person through threats, fear, and intimidation Cyber police can view the complaint and generate a report on it. . This project is an online project, that is, all the details that are required by a customer are posted in the website, so the customer can complaint for crimes living anywhere.

2. EXISTING SYSTEM

The main problem in existing system is manual works has many disadvantages in it. In this busy world customers may find it difficult to visit the police station every time to made complaints. Bill books are having bill number and the name of the customers. Separate registers are maintained for keeping written records of details ,complaint information. So the existing system is inefficient to satisfy the customers. Managing huge reports information manually is a tedious and error prone task. In order to schedule officers as well as informers, we the scheduler should not how many vehicles are there on board and available for allocation. Keeping track of repair information is a must as some times vehicles might be referred for insurance. Existing system does not have such medium by users can place their complain from any location. They have to visit their nearest police location and take a copy of the complaint for future reference. Many citizens hesitate to visit any police station and thus informer information cannot be kept confidential. Sometimes conflicts occurs between police station regarding area, means which area comes under their police station and the person get frustrated before placing their complains. If any citizen is sufferer of cybercrime, even after dialing emergency number, police person do not able to locate the exact location of that citizen.

2.1 Drawbacks of Existing System

- Consumes more time.
- Clearing queries takes long time.
- Error while entering manually.
- It does not have online vehicle searching and complaining.
- Not safe in storing ledger.

- Customers find no time to visit police station.
- Data entry is very slow in manual work

3. PROPOSED SYSTEM

In the proposed system we are going to modify the entire architecture of the system. It has many advantages. user's information will be kept confidential and only users complain will be forwarded to its nearest police station. Users complain number will be forwarded from the server side automatically. For identifying location and authentic person, concept of cookies and IP addressing has been used. To eliminate the location conflicts between police station, server will play a vital role. It will search the address table using IP address and forward message to that police location from where the message has been received. The existing system is therefore found to be inefficient in various ways. These inabilities are solved by developing a new system. The proposed system is developed using PHP as Front-End and My SQL as Back-End. This project is an online project, that is, all the details that are required by a customer are posted in the website, so the customer can complaint for crimes living anywhere. All records can be accessed exclusively by the administrator. The administrator has all the rights to modify any record access. It works as highly interactive user interface. All vehicle details will be automated along with the staff information. Scheduling of trips and repair information is being fully automated to overcome chaos in the system.

3.1 Advantages of proposed system

- Reduces Redundancy.
- Attracting screens.
- Easy navigation inside a screen.
- Not in need of more employees.

- Customers need not visit the company always.

4. PROJECT DESCRIPTION

MYSQL database is going to be the database for this system with entire data of the applications is created in the DB's tables. It keeps all the vehicles and customer, employee, etc…details (large amount of data) stored. Javascript and CSS will help the system styling activity which replaces the flex builder style to light-weight plugins.

Front end :

php (hypertext preproces)

PHP: Hypertext Pre-processor. In its early development by a guy named Erasmus Leadoff, it was called Personal Home Page tools. When it developed into a full-blown language, the name changed to be more in line with its expanded functionality.

1) html-5

HTML5 is a markup language used for structuring and presenting content for the World Wide Web and a core technology of the Internet. It is the fifth revision of the HTML standard as of December 2012, is a candidate recommendation of the World Wide Web Consortium (W3C). Its core aims have been to improve the language with support for the latest multimedia while keeping it easily readable by humans and consistently understood by computers and devices

jsp

Java Server Pages technology is used to create web application just like Servlet technology. It can be thought of as an extension to servlet because it provides more functionality than servlet such as expression language, jstl etc.

css

Cascading Style Sheets (CSS) is a style sheet language used for describing the look and formatting of a document written in a markup language. While most often used to style web pages and interfaces written in HTML and XHTML, the language can be applied to any kind of XML document.

2) javascript

JavaScript (JS) is a dynamic computer programming language. It is most commonly used as part of web browsers, whose implementations allow client-side scripts to interact with the user, control the browser, communicate asynchronously, and alter the document content that is displayed. It is also being used in server-side programming, game development and the creation of desktop and mobile applications.

xampp server

XAMPP stands for "X (as in "cross-platform"), Apache, MySQL, PHP, Perl" and is a "solution stack package" that installs each of those items. Similarly there exists a WAMP, MAMP, and LAMP, standing for Windows, Mac, and Linux, respectively. I believe they condense the "P" to PHP/Perl/Python because Python is additionally included in the stack, whereas it's not in XAMPP. XAMPP is regularly updated to the latest releases of Apache,MariaDB, PHP and Perl.

A. backend:

B. mysql database

A database is a separate application that stores a collection of data. Each database has one or more distinct APIs for creating, accessing, managing, searching and replicating the data it holds. MySQL is an open-source relational database management system (RDBMS). MySQL is a central component of the LAMP open-source web application software stack. . MySQL is also used in many high-profile, large-scale websites, including Google, Facebook, Twitter, Flickr, and YouTube. MySQL is a very powerful program in its own right. It handles a large subset of the functionality of the most expensive and powerful database packages. MySQL Server can run comfortably on a desktop or laptop, alongside user other applications, web servers, and so on, requiring little or no attention. If user dedicates an entire machine to MySQL, user can adjust the settings to take advantage of all the memory, CPU power, and I/O capacity available.

5. LITERATURE SURVEY

5.1.1 Learning the metrics about cyber security challenges for society

Ravi Sharma, Study of Latest Emerging Trends on Cyber Security and its challenges to Society, International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012 1 ISSN 2229-5518 IJSER © 2012

Cyber security is the activity of protecting information and information systems (networks,computers, data bases, data centres and applications) with appropriate procedural and technological securitymeasures. Firewalls, antivirus software, and other technological solutions for safeguarding personal data andcomputer networks are essential but not sufficient to ensure security.

As our nation rapidly building its Cyber-Infrastructure, it is equally important that we educate our population to work properly with this infrastructure.Cyber-Ethics, Cyber-Safety, and Cyber-Security issues need to be integrated in the educational process beginning at an early age. Security counter measures help ensure the confidentiality, availability, and integrityof information systems by preventing or mitigating asset losses from Cyber security attacks. Recently cyber security has emerged as an established discipline for computer systems andinfrastructures with a focus onprotection of valuable information stored on those systems fromadversaries who want to obtain, corrupt,damage, destroy or prohibit access to it.

An Intrusion Detection System (IDS) is a program that analyses whathappens or has happened during an execution and tries to find indications that the computer has been misused.A wide range of metaphors was considered, including those relating to: military and other types of conflict,biological, health care, markets, three-dimensional space, and physical asset protection. These in turn led toconsideration of a variety of possible approaches for improving cyber security in the future.

These approacheswere labelled “Heterogeneity” ,“Motivating Secure Behaviour” and “Cyber Wellness” .Cyber Security plays an important role in the development of information technology as well as Internet services. Our attention is usually drawn on “Cyber Security” when we hear about “Cyber Crimes”.Our first thought on “National Cyber Security” therefore starts on how good is our infrastructure for handling “Cyber Crimes”. This paper focus on cyber security emerging trends while adopting new technologies such asmobile computing, cloud computing, e-commerce, and social networking. The paper also describes the challenges due to lack of coordination between Security agencies and the Critical IT Infrastructure.

Keywords – cyber safety,e-commerce ,intrusion detection system (IDS), internet engineering task force (IETF),metaphors

5.1.2 Modelling the role of internet and disruptive technologies in cyber stalking

Thomas H. Karas and Lori K. Parrott , Judy H. Moore , Metaphors for Cyber Security ,Sandia National Laboratories

Internet is one of the fastest-growing areas of technical infrastructure development. In today’s business environment, disruptive technologies such as cloud computing, social computing, and next-generation mobile computing are fundamentally changing how organizations utilize information technology for sharing information and conducting commerce online [1]. Today more than 80% of total commercial transactions are done online, so this field required a high quality of security for transparent and best transactions.

The scope of Cyber Security extends not only to the security of IT systems within the enterprise, but also to the broader digital networks upon which they rely including cyber space itself and critical infrastructures. Cyber security plays an important role in the development of information technology, as well as Internet services. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic well-being[1]. Society has become dependent on cyber systems across the full range of human activities, includingcommerce, finance, health care, energy, entertainment, communications, and national defense .

Recent research findings also show that the level of public concern for privacy and personal information has increased since 2006 ,Internet users are worried that they give away too much personal information and want to be forgotten when there is no legitimate grounds for retaining their personal information.Exploration of the metaphors we use in the cyber security domain may help improve our thinking and discussion in four ways. First, we may gain a clearer understanding of the value and limitations of the concepts we have mapped from other domains into the cyber security domain. Second, trying out less common or new metaphors may feed the imagination of researchers and policy developers. Third, metaphors that work particularly well might be developed into a whole new models or sets of concepts for approaching cyber security problems. Fourth, a metaphor serves a heuristic purpose --bringing clearer understanding of abstract concepts from the field of cyber security into domains with which the non-specialist may be more familiar.

Cyber security depends on the care that people take and the decisions they make when they set up, maintain, and use computers and the Internet. Cyber-security covers physical protection (both hardware and software) of personal information and technology resources from unauthorized access gained via technological means.Albert Einstein was quoted as saying .Problems cannot be solved with the same level of awareness that created them.The problem of End-User mistakes cannot be solved by adding more technology; it has to be solved with a joint effort and partnership between the Information Technology community of interest as well as the general business community along with the critical support of top management.

5.1.3. Threats To Cyber Security

Threats to cyber security can be roughly divided into two general categories: actions aimed at andintended to damage or destroy cyber systems (.cyber attacks.) and actions that seek to exploit the cyberinfrastructure for unlawful or harmful purposes without damaging or compromising that infrastructure(.cyber exploitation.) . While some intrusions maynot result in an immediate impact on the operation of a cyber systems, as for example when a .TrojanHorse. infiltrates and establishes itself in a computer, such intrusions are considered cyber attacks when they can thereafter permit actions that destroy or degrade the computer’s capacities . Cyber

exploitation includes using the Internet and other cyber systems to commit fraud, to steal,to recruit and train terrorists, to violate copyright and other rules limiting distribution of information,to convey controversial messages (including political and .hate. speech), and to sell child pornography or other banned materials.Following are some new threats to cyberspace

5.1.4 Current..Cyber-Security Measures

The Internet currently is secured primarily through private regulatory activity, defensive strategies and products, national laws and enforcement, and some limited forms of international cooperation and regulation.

5.1.4.1 Private Measures

Non-governmental entities play major roles in the cyber security arena. Technical standards for theInternet (including current and next-generation versions of the Internet Protocol) are developed andproposed by the privately controlled Internet Engineering Task Force (.IETF.)[2]; the Web Consortium,housed at the Massachusetts Institute of Technology, defines technical standards for the Web.Other privately controlled entities that play significant operational roles on aspects of cyber securityinclude the major telecommunications carriers, Internet Service Providers (.ISPs.), and many other organizations, including:

- The Forum of Incident Response and Security Teams (.FIRST.), which attempts to coordinatethe activities of both government and private Computer Emergency Response Teams (.CERTs.) and is also working on cyber security standards;
- The Institute of Electrical and Electronics Engineers (.IEEE.), which develops technical standards through its Standards Association and in conjunction with the U.S. National Institute of Standards and Technology (.NIST.);
- The Internet Corporation for Assigned Names and Numbers (.ICANN.), which operates pursuantto a contract with the U.S. Department of Commerce (September 2009) transferring to ICAAN the technical management of the Domain Name System[11].

5.1.4.2.National Measures

Many national governments have adopted laws aimed at punishing and thereby deterring specific forms of cyber attacks or exploitation. The U.S., for example, has adopted laws making criminal various forms of conduct, including improper intrusion into and deliberate damage of computer systems.These laws have little or no effect, however, on individuals, groups, or governments over whom the U.S. lack sor is unable to secure regulatory or criminal jurisdiction.US national security experts almost exclusively emphasize the need for national measures forenhancing cyber security[2]. They recommend national laws to protect the sharing of information about threats and attacks; methods for government bodies, such as the NSA, to cooperate with private entitiesin evaluating the source and nature of cyber attacks; and more effective defenses and responses to cyber attacks and exploitation developed through government-sponsored research and coordination pursuant to cyber security plans. The GAO's July 2010 report details the specific roles being played by many U.S. agencies in efforts to enhance .global cybersecurity., but ultimately concludes that these efforts are not part of a coherentstrategy likely to advance U.S. interests.

5.1.4.3.International Measures

National governments often cooperate with each other informally by exchanging

information,investigating attacks or crimes, preventing or stopping harmful conduct, providing evidence, and evenarranging for the rendition of individuals to a requesting state. States have also made formal,international agreements that bear directly or indirectly on cyber security.. The international agreements apply to the criminal activities specified, including situations in which the alleged criminals have used cybersystems in those activities.International agreements that potentially bear upon cyber-security activities also include treaties(the UN Charter and Geneva Conventions) and Universally accepted rules of conduct (customary law).International law also provides rulesrelated to the use of force during armed conflict that presumably apply

to cyber attacks, including for example requirements that noncombatants and civilian institutions

such as hospitals not be deliberately attacked, and that uses of force be restricted to measures that are necessary and proportionate.

5.1.5. Metaphors Of Cyber Era

Computer networks in which all the components have the same vulnerabilities are easier for attackers to bring down, but more diverse systems would deprive attackers of sufficient target knowledge to do as much damage.It can thus be argued that diversity is one of the ways of .baking. security into systems—designing them from the start to be more secure, as opposed to adding on security measures later.

A second approach,.Motivating Secure Behaviour,. took a market perspective on the adoption of cyber security measures. The central concept is that many of the vulnerabilities in current systems can be traced to human behaviours shaped by the structure of incentives facing both suppliers and users of information technology.The third approach was called .Cyber Wellness,. exploring analogies with efforts to improve individual and public health. Its objective is to keep the population (of users and networked systems) as healthy as possible: resistant to attacks, resilient under stresses, wary of dangerous environments, treatable if diseased, and able to limit contagions. Generally speaking, the literature on cyber security usually refers to three characteristics of information systems that need protection:

1. Confidentiality -privacy of information and communications. In government this might mean, for example, assuring access to classified information only by authorized individuals. In commerce, it might mean the protection of proprietary information.

2. Integrity -assurance that information or computing processes have not been tampered with or destroyed. In the case of critical infrastructures (say, for example,the power grid), loss of data integrity could take the form of destructive instructions to the system resulting in financial, material, or human losses.

3. Availability- assurance that information or services are there when needed. Denial of service attacks, which overload system servers and shut down websites, are examples of interfering with availability.

Two important characteristics of the much of the discourse on this subject (as well as most discourse on most subjects). that is, first, metaphors are hard to avoid, even if we are not consciously using them. Second, how a problem is framed frequently implies certain kinds of solutions, while implicitly reducing the likelihood that others will be considered.The newer or rarer metaphors were then grouped into several categories to facilitate further elaboration.

5.1 Predominant Metaphors

As mentioned above, a common metaphor in cyber security is that of the fortress. Avalued body of information is held within a walled enclosure, perhaps encircled by a moat,accessed by portals or gates, and guarded by watchmen assigned to keep out theunauthorized. A second common metaphor is that of cops and robbers: criminals (or maybejust vandals) break into the house and steal valuables. Forensic measures are taken to trackthem down, after which they are identified and legally prosecuted. A third common metaphoris that of warfare: enemies, using various weapons and tactics, attack and steal or destroyproperty (or perhaps just commit espionage) in order to achieve some strategic goal.

5.1.6 Some Counter Measures For Cyber Security

GPRS Security Architecture In order to meet security objectives, GPRS employs a set of security mechanisms that constitutes the GPRS security architecture. Most of these mechanisms have been originally designed for GSM,but they have been modified to adapt to the packet oriented traffic nature and the GPRS network components. The GPRS security architecture, mainly,aims at two goals: a) to protect the network again stun authorized access, and b) to protect the privacy of users. It includes the following components:

- Subscriber Identity Module (SIM)
- Subscriber identity confidentiality
- Subscriber identity authentication
- GPRS backbone security

6.PROBLEM DEFINITION

6.1 Primary Objective

- To develop a platform for the purpose of crime controlling which minimizes the crime that is happening.
- The details of the pubic will not be provided to any other sources.it helps the victim to post thier complaints without anybodys knowledge if he/she has any hesitation to move to the police station.

6.2 Secondary Objective

- To provide ease of access to the public.The crime information that they provided will be immediately processed by the officers and the victims need is fulfilled .
- The victim can directly contact with the officer about their case status as each case is provided with a different officers.

7. RELATED WORK

The future enhancement of the application is related to user complaint status ,once the complaint is posted in website the status of the complaint should be updated .In case of any delay in action the user may further post comments in website regarding the status.Such that those complaints will be prioritized first in website ,this helps the user to make a remainder about the complaint to officers .This process helps in quick response to the user complaint.It is important to know about the complaint status of the user and this helps the other officers and users to check whether the actions are properly taken by police.If you have made a complaint against the police and you are not happy with the way it has been handled, you may be able to appeal to:

The Appropriate Authority, who is the Professional Standards Directorate Appeal Decision Maker on behalf of the Commissioner of the city.

CONCLUSION

Many citizens hesitate to visit any police station and thus informer information cannot be kept confidential. If any citizen is sufferer of cybercrime, even after dialing emergency number, police person do not able to locate the exact location of that citizen. user's information will be kept confidential and only users complain will be forwarded to its nearest police station.

For identifying location and authentic person, concept of cookies and IP addressing has been used. To eliminate the location conflicts between police station, server will play a vital role. It will search the address table using IP address and forward message to that police location from where the message has been received.

This helps the user to identify all sorts of information which they need to know for any references.in general the public may not know for what purpose this website is used and the benefits that are acquired from this site. The admin has all the rights to edit delete the complaint once it is solved and once a complaint is posted it will be seen by the admin officers. The seen statement will be sent to the victim who posted the complaint.

REFERENCES

[1]Abraham D.Soafaer,DavidClark,Whitefield Diffie,produceedings of aworkshop on deterring cyber Attacks:Informing Strategies and Developing Option for U.S Policy

http://WWW.nap.edu/catealog/12997 html Cyber Security and International Agreements,Internet Corporation for Assigned Names and Numbers

[2]AdmiralDennis C.Blair,Annual Threat Assessment, House Permanent Select Committee on Intelliegence,111th Congress,1st session 2009.

[3]Ajith Abrahim,Crina GrosanCyber Security and theEvolution of Intrusion Detection System Information Science and Engineering Jinan University,Jinan 250022,P.R.China.

[4]AmichanShulan, Application Defence Center(ADC), AmichaRegu-larlyLectures, Security,2011.

[5]Audry Watters, Read Write Cloud, RWW Solution Series,2010.

[6] Bibliothequesolvary,parcLeopold,security and defense Agenda,137 rue Belliard,B-1040 Brussels,Belgium

[7]BinaKotiyal,R H Goudar and Senior Member, ACyber Era Approach for Building Awareness in Cyber Security for Educational sytsem in India PritiSaxena,IACSIT International Journal Of Information and Education Technology, vol 24061,United States b Verizon Business security

[8] Cisco,Cisco 2009 AnnualSecurityReport:Highlighting Global Security Threats and Trends,December 4,2009.

[9] Denning D,An Intrusion-Detection Model, IEEE Transactions on Software Engineering, vol SE-13,no.2,pp.222-232,1987.

[10] D.J.Bodeau,R.Graubart,and J.Fabius-Greene,"Improving Cyber Security and Mission assurance via cyber Preparedness " levels,September 9,2010.

[11]. Mike McConnell," Mike McConnell on How to win the cyber-war we're Losing,"February 28,2010,(accessed on July 19 2010).

[12] Ravi sharma,study of Latest Emerging Trends on cyber security and its challenges to society ,international journal of scientific &engineering Research Volume3,issue6,june-2012 1ISSN 2229-5518 IJSER 2012

[13] ThillaRajaretnam Associate Lecture, School of law,University of Western Sydney. The Society of Digital Information and Wireless Communication (SDIWC),International journal of cyber-security and digital forensics (IJCSDF).ISSN:2305-0012

[14]Thomas H.Karas and Lori K.Parrott,judy H Moore,Metaphors for cyber security ,Sandia National Laboratories P.O Box 5800 Albuquerque,NM87185-0839