Cyber crime in Indian scenario – a literature snapshot

Janhavi J Deshmukh and Surbhi R Chaudhari
Dept. of Computer Science & Engineering,
Jawaharlal Darda Institute of Engineering & Technology,
Yavatmal – 445001, India.
janhavideshmukh0@gmail.com and surbhichaudhari12@gmail.com

Abstract— **There has been tremendous growth in use of Internet .Technology give rise to Cyber Crime. Cyber Crime is technology based crime committed by technocrats. This paper deals with variants of cyber crime like Salami Attack, Packet Sniffing, Tempest Attacks, and Bot Networks. It also includes real world cyber crime cases their scenario and modus operandi. The global spam rate, malware rate and phishing rate is increasing rapidly. And there is a potential impact of cyber crime on economics, consumer trust and production time. The counter measures like GPRS Security architecture, Intrusion Detection and prevention System and Agent Based Distributed Intrusion Detection System are used for security purposes.**

Keywords- Bot networks, Modus operandi, Salami Attack, Tempest Attack.

I. INTRODUCTION

Advancements in modern technology have helped countries develop and expand their communication networks, enabling faster and easier networking and information exchange. Currently, there are nearly 2 billion internet users and over 5 billion mobile phone connections worldwide. Every day, 294 billion emails and 5 billion phone messages are exchanged. Most people around the world now depend on consistent access and accuracy of these communication channels. [1] The growing popularity and convenience of digital networks, however, come at a cost. As businesses and societies in general increasingly rely on computers and internet-based networking, cyber crime and digital attack incidents have increased around the world. [2] These attacks — generally classified as any crime that involves the use of a computer network — include financial scams, computer hacking, downloading pornographic images from the internet, virus attacks, e-mail stalking and creating websites that promote racial hatred. The first major instance of cyber crime was reported in 2000, when a mass-mailed computer virus affected nearly 45 million computer users worldwide. [1]

II. LITERATURE REVIEW OF CYBER CRIME SCENARIO IN INDIA

A. Meaning of cyber crime

Cyber crime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It is also used to include traditional crimes in which computers or networks are used to enable the illicit activity. [3]

Cyber crimes are technology based crimes and the computer or internet itself can be used as a weapon or means to do such crimes quite freely. They are organized and white collar crimes like cyber frauds, hacking, data theft, phishing, identity theft etc. Cyber crimes are committed with the help of technology and cyber criminals have deep understanding of technology. In fact, cyber criminals are technocrats who understand the intricacies of information technology. Cyber crimes do not consider any boundaries or territorial barriers. [4]

According to Information Technology Act, 2000 Cyber Crime is "the acts that are punishable by the Information Technology Act". It is not exhaustive as the Indian Penal Code also covers many cyber crimes, such as email spoofing and cyber defamation, sending, threatening emails. [5]

III. CYBER CRIME VARIANTS

Cyber Crime refers to all activities done with criminal intent in cyberspace. These fall into three slots.

- Those against persons.
- Against Business and Non-business organizations.
- Crime targeting the government [6]

A. Malware

Malware is software that takes control of any individual's computer to spread a bug to other people's devices or social networking profiles. Such software can also be used to create a 'botnet'— a network of computers controlled remotely by hackers, known as 'herders,' — to spread spam or viruses. [1]

B. Cyber Pornography

This form includes act of publishing and printing pornographic material and the use of the internet to transmit such pornographic material. [6]

C. Salami Attack

Those attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed e.g. A

bank employee inserts a program into bank's servers, that deducts a small amount from the account of every customer.[6]

D. Hacking

A hacker is an unauthorized user who attempts to or gains access to an information system. Hacking is a crime even if there is no visible damage to the system, since it is an invasion in to the privacy of data. There are different classes of Hackers.

- White Hat Hackers - They believe that information sharing is good, and that it is their duty to share their expertise by facilitating access to information. However there are some white hat hackers who are just "joy riding" on computer systems.
- Black Hat Hackers -They cause damage after intrusion. They may steal or modify data or insert viruses or worms which damage the system. They are also called 'crackers'.
- Grey Hat Hackers - Typically ethical but occasionally violates hacker ethics Hackers will hack into networks, stand-alone computers and software. Network hackers try to gain unauthorized access to private computer networks just for challenge, curiosity, and distribution of information. Crackers perform unauthorized intrusion with damage like stealing or changing of information or inserting malware (viruses or worms) [7]

E. Phishing

Phishing is just one of the many frauds on the Internet, Phishing trying to fool people into parting with their money. Phishing refers to the receipt of unsolicited emails by customers of financial institutions, requesting them to enter their username, password or other personal information to access their account for some reason. Customers are directed to a fraudulent replica of the original institution's website when they click on the links on the email to enter their information, and so they remain unaware that the fraud has occurred. The fraudster then has access to the customer's online bank account and to the funds contained in that account. [8]

F. Vishing

Vishing is the criminal practice of using social engineering and Voice over IP (VoIP) to gain access to private .personal and financial Information from the public for the purpose of financial reward. The term is a combination of "voice" and phishing. [8]

G. Bot networks

A cyber crime called 'Bot Networks', wherein spamsters and other perpetrators of cyber crimes remotely take control of computers without the users realizing it, is increasing at an alarming rate. Computers get linked to Bot Networks when users unknowingly download malicious codes such as Trojan horse sent as e-mail attachments. Such affected computers, known as zombies, can work together whenever the malicious code within them get activated, and those who are behind the Bot Networks attacks get the computing powers of thousands of systems at their disposal. Attackers often coordinate large groups of Bot-controlled systems, or Boot networks, to scan for vulnerable systems and use them to increase the speed and breadth of their attacks. Boot networks create unique problems for organizations because they can be remotely upgraded with new exploits very quickly and this could help attackers pre-empt security efforts. [8]

H. Packet Sniffing

This is used by hackers and forensic experts. Data travels in the form of packets and vary in size depending on the network bandwidth and amount of data. The hacker intercepts the transmission between computer A and B. All the hacker needs is the IP address from one of the computers and any data can be stolen. The data is not stolen because sniffers don't do that. Instead they copy the hex and translate it into original data. This is why it is hard for firewalls to detect this because they only provide application level security. [9]

I. Tempest attacks

This is an acronym for Transient Electromagnetic Pulse Emanation Standard. Data that passes though circuitry and mechanical devices produce electro-magnetic emanation. This allows hackers to monitor and put data from network cables. The hacker has to be in range of the network cables so they may be in a parking lot or adjacent room in the building. [9]

J. Buffer overflow

This is the most common way of breaking into a computer. Buffers are created to hold a finite amount of data. When it overflows, it goes into adjacent buffers which can cause data to be overwritten. In buffer overflow attacks, the extra data can contain instructions that trigger specific actions. These actions can cause damage to files and/or change data. [9]

K. Cyber Stalking

Cyber stalking is essentially using the Internet to repeatedly harass another person. This harassment could be sexual in nature, or it could have other motivations including anger. People leave a lot of information about themselves online. Such information can leave one vulnerable to cyber stalking. [10]

L. Bacteria or Rabbit Programs

Bacteria or rabbits are programs that are meant to replicate themselves. Thus they reproduce themselves exponentially and take up all the processor capacity, memory, or disk space. [11]

M. E-mail spoofing and E-mail bombing

A spoofed email is one that appears to originate from one source but actually has been sent from another source. This can also be termed as E-Mail forging. [6]

In this case, the goal of the attacker is to interrupt the

victim's e-mail service by sending him a large number of e-mails. [11]

N. Trojan and Rats

Trojan horses are programs that appear to be doing what the user wants while they are actually doing something else such as deleting files or formatting disks. All the user sees is the interface of the program that he wants to run. RATs are remote access Trojans that provide a backdoor into the system through which a hacker can snoop into your system and run malicious code. [11]

O. Data Diddling

Data diddling involves changing data prior or during input into a computer. In other words, information is changed from the way it should be entered by a person typing in the data, a virus that changes data, the programmer of the database or application, or anyone else involved in the process of having information stored in a computer file. The culprit can be anyone involved in the process of creating, recording, encoding, examining, checking, converting, or transmitting data. This is one of the simplest methods of committing a computer-related crime, because it requires almost no computer skills whatsoever. Despite the ease of committing the crime, the cost can be considerable. [12]

IV. CYBER CRIME CASES

A. Email account hacking

Emails are increasingly being used for social interaction, business communication and online transactions. Most email account holders do not take basic precautions to protect their email account passwords. Cases of theft of email passwords and subsequent misuse of email accounts are becoming very common.

The scenario-The victim's email account password is stolen and the account is then misused for sending out malicious code (virus, worm, Trojan etc) to people in the victim's address book. The recipients of these viruses believe that the email is coming from a known person and run the attachments. This infects their computers with the malicious code.

Modus Operandi- The suspect would install key loggers in public computers (such as cyber cafes, airport lounges etc) or the computers of the victim. [13]

B. Source code theft

Computer source code is the most important asset of software companies. Simply put, source code is the programming instructions that are compiled into the executable files that are sold by software development companies. As is expected, most source code thefts take place in software companies. Some cases are also reported in banks, manufacturing companies and other organizations that get original software developed for their use.

The scenario- The suspect (usually an employee of the victim) steals the source code and sells it to a business rival of the victim.

Modus Operandi- If the suspect is an employee of the victim, he would usually have direct or indirect access to the source code. He would steal a copy of the source code and hide it using a virtual or physical storage device [13]

C. Software piracy

Many people do not consider software piracy to be theft. They would never steal a rupee from someone but would not think twice before using pirated software. There is a common perception amongst normal computer users to not consider software as "property". This has led to software piracy becoming a flourishing business.

The scenario- The software pirate sells the pirated software in physical media (usually CD ROMs) through a close network of dealers.

Modus Operandi-The suspect uses high speed CD duplication equipment to create multiple copies of the pirated software. This software is sold through a network of computer hardware and software vendors [13]

D. Web defacement

Website defacement is usually the substitution of the original home page of a website with another page (usually pornographic or defamatory in nature) by a hacker.

Religious and government sites are regularly targeted by hackers in order to display political or religious beliefs.

The scenario - The homepage of a website is replaced with a pornographic or defamatory page. In case of Government websites, this is most commonly done on symbolic days (e.g. the Independence Day of the country).

Modus Operandi - The defacer may exploit the vulnerabilities of the operating system or applications used to host the website. This will allow him to hack into the web server and change the home page and other pages.

Alternatively he may launch a brute force or dictionary attack to obtain the administrator passwords for the website. He can then connect to the web server and change the WebPages. [13]

E. Email scam

Emails are fast emerging as one of the most common methods of communication in the modern world. As can be expected, criminals are also using emails extensively for their illicit activities.

The scenario- In the first step, the suspect convinces the victim that the victim is going to get a lot of money (by way of winning a lottery or from a corrupt African bureaucrat who wants to transfer his ill gotten gains out of his home country). In order to convince the victim, the suspect sends emails (some having official looking documents as attachments). Once the victim believes this story, the suspect asks for a

small fee to cover legal expenses or courier charges. If the victim pays up the money, the suspect stops all contact.

Modus Operandi -The suspect creates email accounts in fictitious names and sends out millions of fraudulent emails using powerful spam software. [13]

F. Use of Internet and Computers by terrorists

Many terrorists are using virtual as well as physical storage media for hiding information and records of their illicit business. They also use emails and chat rooms to communicate with their counterparts around the globe.

The scenario -The suspects carry laptops wherein information relating to their activities is stored in encrypted and password protected form. They also create email accounts using fictitious details. In many cases, one email account is shared by many people. E.g. one terrorist composes an email and saves it in the draft folder. Another terrorist logs into the same account from another city / country and reads the saved email. He then composes his reply and saves it in the draft folder. The emails are not actually sent. This makes email tracking and tracing almost impossible.

Modus Operandi- The terrorists purchase small storage devices with large data storage capacities. They also purchase and use encryption software. The terrorists may also use free or paid accounts with online storage providers. [13]

V. INCREASING CYBER CRIME

Over the past few years, the global cyber crime landscape has changed dramatically, with criminals employing more sophisticated technology and greater knowledge of cyber security.

In 2010, the global spam rate increased 1.4 percent year-on-year (y-o-y), to 89.1 percent, most of which involved botnets, according to a Symantec report. [1]

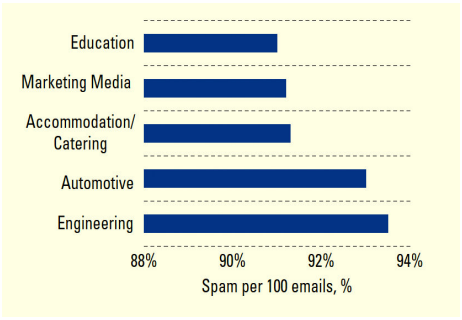

Fig 1: *Global email spam rate (as detected by MessageLabs Services, Symantec), top 5 and sectors, 2010* [1]

Figure 2 and figure 3. In 2010, the average rate of malware in email traffic was 1 in 284.2 emails, almost the same as that in 2009. However, the average rate of emails blocked as phishing attacks improved from 1 in 325.2 in 2009 to 1 in 444.5 in 2010.

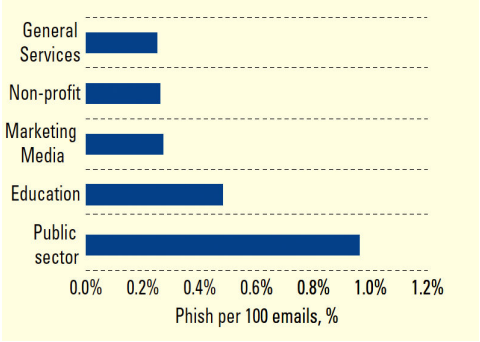

Fig2: *Global phishing rate (as detected by MessageLabs Services, Symantec), top 5 targeted sectors, 2010* [1]

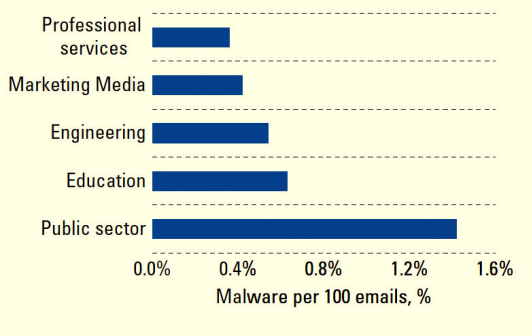

Fig3:*Global email malware rate (as detected by MessageLabs Services, Symantec), top 5 targeted sectors, 2010* [1]

VI. REAL CASES OF CYBER CRIMES IN INDIA

A. Pune Citibank Mphasis call center fraud

It is a case of sourcing engineering. US $ 3, 50,000 from City bank accounts of four US customers were dishonestly transferred to bogus accounts in Pune, through internet. Some employees of a call centre gained the confidence of the US customers and obtained their PIN numbers under the guise of helping the customers out of difficult situations. Later they used these numbers to commit fraud. Highest security prevails in the call centers in India as they know that they will lose their business. The call center employees are checked when they go in and out so they cannot copy down numbers and therefore they could not have noted these down. They must have remembered these numbers, gone out immediately to a cyber café and accessed the Citibank accounts of the customers. All accounts were opened in Pune and the customers complained that the money from their accounts was transferred to Pune accounts and that's how the criminals were traced. Police has been able to prove the honesty of the call center and has frozen the accounts where the money was transferred. [7]

B. Parliament attack case

Bureau of Police Research and Development at Hyderabad had handled some of the top cyber cases, including analyzing and retrieving information from the laptop recovered from

terrorist, who attacked Parliament. The laptop which was seized from the two terrorists, who were gunned down when Parliament was under siege on December 13 2001, was sent to Computer Forensics Division of BPRD.

The laptop contained several evidences that confirmed of the two terrorists' motives, namely the sticker of the Ministry of Home that they had made on the laptop and pasted on their ambassador car to gain entry into Parliament House and the fake ID card that one of the two terrorists was carrying with a Government of India emblem and seal. The emblems (of the three lions) were carefully scanned and the seal was also crafty made along with residential address of Jammu and Kashmir. But careful detection proved that it was all forged and made on the laptop. [7]

C. Andhra Pradesh tax case

The owner of a plastics firm in Andhra Pradesh was arrested and Rs. 22 crore cash was recovered from his house by the Vigilance Department. They sought an explanation from him regarding the unaccounted cash. The accused person submitted 6,000 vouchers to prove the legitimacy of trade, but after careful scrutiny of vouchers and contents of his computers it revealed that all of them were made after the raids were conducted. It was revealed that the accused was running five businesses under the guise of one company and used fake and computerized vouchers to show sales records and save tax. Thus the dubious tactics of the prominent businessman from Andhra Pradesh was exposed after officials of the department got hold of computers used by the accused person. [7]

D. The bank NSP case

The Bank NSP case is the one where a management trainee of the bank was engaged to be married. The couple exchanged many emails using the company computers. After some time the two broke up and the girl created fraudulent email ids such as "Indian bar associations" and sent emails to the boy's foreign clients. She used the banks computer to do this. The boy's company lost a large number of clients and took the bank to court. The bank was held liable for the emails sent using the bank's system. [7]

VII. EFFECTS OF COMPUTER CRIME

A. Potential economic impact

As today's consumer has become increasingly dependent on computers, networks, and the information these are used to store and preserve, the risk of being subjected to cyber-crime is high. Some of the surveys conducted in the past have indicated as many as 80% of the companies' surveyed acknowledged financial losses due to computer breaches.

As the economy increases its reliance on the internet, it is exposed to all the threats posed by cyber-criminals. Stocks are traded via internet, bank transactions are performed via internet, purchases are made using credit card via internet. All instances of fraud in such transactions impact the financial state of the affected company and hence the economy.

The disruption of international financial markets could be one of the big impacts and remains a serious concern. The modern economy spans multiple countries and time zones. Such interdependence of the world's economic system means that a disruption in one region of the world will have ripple effects in other regions. Hence any disruption of these systems would send shock waves outside of the market which is the source of the problem.

Productivity is also at risk. Attacks from worms, viruses, etc take productive time away from the user. Machines could perform more slowly; servers might be in accessible, networks might be jammed, and so on. Such instances of attacks affect the overall productivity of the user and the organization. It has customer service impacts as well, where the external customer sees it as a negative aspect of the organization. [14]

B. Impact on consumer trust

Since cyber-attackers intrude into others' space and try and break the logic of the page, the end customer visiting the concerned page will be frustrated and discouraged to use the said site on a long term basis. The site in question is termed as the fraudulent, while the criminal masterminding the hidden attack is not recognized as the root cause. This makes the customer lose confidence in the said site and in the internet and its strengths.

According to reports sponsored by the Better Business Bureau Online, over 80% of online shoppers cited security as a primary worry when conducting business over the Internet. About 75% of online shoppers terminate an online transaction when asked for the credit card information. The perception that the Internet is rife with credit card fraud and security hazards is growing. This has been a serious problem for e-commerce. [14]

C. Slows production time and add to over head cost

Computer crime reduces the productivity of a company, as a company will take measure to reduce cybercrime, by entering more password or other acts this will take time to do and therefore will affect productivity. Computer crime will increase the cost as to stop viruses and malware companies must buy strong security software to reduce the chances of attacks from such attacks. [10]

VIII. SOME COUNTER MEASURES FOR CYBER SECURITY

A. Intrusion Detection and Prevention System (IDPS)

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents.

Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators. In addition, organizations use IDPSs for other purposes, such as identifying problems with security policies, documenting existing threats, and deterring individuals from violating security policies. IDPSs have become a necessary addition to the security infrastructure of nearly every organization.

IDPSs typically record information related to observed events, notify security administrators of important observed events, and produce reports. Many IDPSs can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment (e.g., reconfiguring a firewall), or changing the attack's content. [15]

B. Agent Based Distributed Intrusion Detection System (ABDIDS)

Agent based distributed Intrusion detection system is an important component of defensive measures protecting computer systems and networks from abuse. ABDIDS automates security management tasks such as the interpretation and correct diagnosis of IDSes output. ABDIDS is a fully distributed system made by set of nodes with three types of agents: Monitoring Registry Agents (MoRA), Monitoring Agents (MoA) and managing agents (MA). [16]. ABDIDS is fully distributed and provides two capabilities in addition to other functionalities of IDS:

(a) Early warning when pre-attack activities are detected,

(b) Detecting and isolating compromised nodes by trust mechanisms and voting-based peer-level protocols. [17]

B. 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 against unauthorized access, and

b) To protect the privacy of users. It includes the following components:

- Subscriber Identity Module (SIM)
- Subscriber identity confidentiality
- Subscriber identity authentication

User data and signaling confidentiality between the MS and the SGSN GPRS backbone security. [18]

REFERENCES

[1] KPMG INTERNATIONAL Issues Monitor "Cyber Crime – A Growing Challenge for Governments July 2011", Volume Eight

[2] "It is time for countries to start talking about arms control on the internet", Economist, July 1, 2010. Retrieved June 23,2011, Available http://www.economist.com/node/16481504

[3] Dr.B.Muthukumaran, Chief Consultant, Gemini Communication Ltd., "Cyber crime scenario in India", Criminal Investigation Department Review-January2008

[4] "Common Cyber Crimes and Government Laws and Rules in Information Security" Unit 3, Information Technology Act

[5] Kulwant Malik , "Emergence of Cyber Crime in India" , International Referred Research Journal,July,2011,ISSN-0975-3486, RNI: RAJBIL 2009/30097, VOL-II *ISSUE 22

[6] V.Shiva Kumar, Asst.Director A.P.Police Academy, "Cyber Crime Prevention And Detection",.

[7] Dr. A. Prasanna, Associate Fellow IMG,Thiruvananthapuram.,"Cyber Crimes: Laws And Practice"

[8] Mohit Goyal, "Ethics And Cyber Crime In India", International Journal of Engineering and Management Research, Vol. 2, Issue-1, Jan 2012

[9] Brett Pladna, "The Lack of Attention in the Prevention of Cyber Crime and How to improve it", ICTN6883, East Carolina University

[10] Anah Bijik Hassan, Funmi David Lass, Julius Makinde, "Cybercrime in Nigeria: Causes, Effects and the Way Out", ARPN Journal of Science and Technology, ISSN 2225-7217, VOL. 2, NO. 7, August 2012

[11] Ali Peiravi, Mehdi Peiravi, "Internet security - cyber crime Paradox", Journal of American Science 2010;6(1):15-24 (ISSN: 1545-1003).

[12] Gerard Sylvester, "Cyber Crime", SAMACHAR *July-August 2007 Page 40, 43*

[13] Rohas Nagpal ,"Cyber Crime & Digital Evidence –Indian Perspective" , "Real world cyber crime cases"

[14] Hemraj Saini, Yerra Shankar Rao, T.C.Panda, "Cyber-Crimes and their Impacts: A Review", International Journal of Engineering Research and Applications(IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 2,Mar-Apr 2012, pp.202-209

[15] Karen Scarfone ,Peter Mell "Guide to Intrusion Detection and Prevention Systems (IDPS)", National Institute of Standards and Technology Special Publication 800-94 Natl. Inst. Stand. Technol. Spec. Publ. 800-94, 127 pages (February 2007)

[16] Yu Lasheng , and Mutimukwe Chantal "Agent Based Distributed Intrusion Detection System (ABDIDS)" ISBN 978-952-5726-07-7 (Print), 978-952-5726-08-4 (CD-ROM) Proceedings of the Second Symposium International Computer Science and Computational Technology(ISCSCT '09) Huangshan, P. R. China, 26-28,Dec. 2009, pp. 134-138

[17] Arjita Ghosh and Sandip Sen ,"Agent-Based Distributed Intrusion Alert System" ,University of Tulsa, Tulsa OK 74104, USA

[18] Anju P Rajan Mathew, A. AJilaylwin, Shaileshwari M U"Cyber security solutions for DLMS meters using GSM/GPRS technology"