Global Journal on Innovation, Opportunities and Challenges in AAI and Machine Learning
Vol. 1, Issue 1 - 2017

CLOUD COMPUTING: GLOBAL ECONOMICS AFFECTED WITH CYBER CRIME AND LEGISLATION ISSUES

BHAWESH KUMAWAT*, SANJAY CHAUDHARY**

ABSTRACT

Cyber-crime is the fastest growing crime on the planet with a huge number of individuals being affected each day. The financial losses accruing from cybercrime fraud is multiplying each year. However less than half of the cybercrime cases are reported to the authorities. This implies the situation is worse than it seems to be. This paper examines the implications of cyber-crime on the social-economic development of a country. Cyber-crime is developing as a genuine risk. Worldwide governments, police departments and intelligence units have started to react. Initiatives to curb cross border cyber threats are taking shape. Indian police has started uncommon digital cells the nation over and have begun educating the individuals. This paper is an endeavor to give a look on cyber-crime in India. This fundamental base behind writing this paper is various reports from news media and news portal crime.

KEYWORDS: Cyber-Crime, Internet Crime, Uganda Crime Statistics, Hacking, Vishing, Cyber-Squatting, Phishing.

INTRODUCTION

In the present day world, India has witnessed a huge increase in Cybercrimes whether they pertain to Salami attack, Trojan attacks, e-mail bombing,Web jacking, Denial of Service attack, DOS attacks, information theft, or the most common offence of hacking the data or system to commit large number of crime. Despite technological measures being adopted by corporate organizations and individuals, we have witnessed that the frequency of cybercrimes has increased over the last decade. The Internet is fast becoming a way of life for millions of people and also a way of living because of growing dependence and reliance of the mankind on these machines. Internet has enabled the use of website communication; email messages, online chatting, what's app message sand a lot of anytime anywhere IT solutions for the betterment of human kind. Cybercrime refers to the act of performing a criminal act using computer or cyberspace (the Internet network), as the communication vehicle. Though there is no technical definition by any statutory body for Cybercrime, it is broadly defined by the Computer Crime Research Center as - "Crimes committed on the internet using the computer either as a tool or a targeted victim." All types of cybercrimes involve both the computer and the person behind it as victims; it just depends on which of the two is the main target.

*Research Scholar, Department of CSE, Madhav University, Abu Road.
**Professor, Department of CSE, Madhav University, Abu Road.
Correspondence E-mail Id: editor@eurekajournals.com

Cybercrime could include anything as simple as downloading illegal music files to stealing millions of dollars from online bank accounts.

Crime is both a social and economic phenomenon. It is as old as human society. Many ancient books right from pre-historic days, and mythological stories, magazines, have spoken about crimes committed by individuals be it against another individual like ordinary theft and burglary or against the nation like spying, treason etc.

An important form of cybercrime is identity theft, in which criminals use the Internet to steal personal information from other users. Various types of social networking sites are used for this purpose to find the identity of interested peoples. There are two ways this is done - phishing and harming, both methods lure users to fake websites, where they are asked to enter personal information. This includes original information, such as usernames and passwords, phone numbers, addresses, credit card numbers, bank account numbers, and other information criminals can use to "steal" another person's identity.

Let us now discuss in detail, the Information Technology Act -2000 and the I.T. Amendment Act 2008 in general and with particular reference to banking and financial sector related transactions. Before going into the section-wise or chapter-wise description of various provisions of the Act, let us discuss the history behind such a legislation in India, the circumstances under which the Act was passed and the purpose or objectives in passing it.

CATEGORIES OF CYBER CRIME

CYBER CRIMES AGAINST PERSONS

There are certain offences which affect the personality of individuals can be defined as:

- **HARASSMENT BY MEANS OF E-MAILS:** It is exceptionally regular kind of provocation through sending letters, offer letter, individual letter, connections of records and organizers i.e. through messages, Whatsapp. At exhibit badgering is regular as utilization of social destinations i.e. Facebook, Twitter, Instragram, Whatsapp and so forth expanding step by step.
- **CYBER-STALKING:** Cyber stalking is the utilization of the Internet or other electronic intends to stalk somebody which might be a PC wrongdoing or badgering. This term is utilized conversely with online provocation and online mishandle. A digital stalker does not present a direct physical risk to a casualty, however takes after the casualty's online action to accumulate data and make dangers or different types of verbal terrorizing. The obscurity of online cooperation diminishes the possibility of recognizable proof and makes digital stalking more typical than physical stalking. Despite the fact that digital stalking may appear to be moderately safe, it can cause casualties mental and passionate damage, and it might once in a while prompt genuine stalking. Digital stalkers target and hassle their casualties by means of sites, visit rooms, discourse gatherings, open distributing sites (e.g. web journals and Indy media) and emai.
- **DISSEMINATION OF OBSCENE MATERIAL:** It incorporates Indecent introduction/ Pornography (essentially kid explicit entertainment), facilitating of site containing these precluded materials. These disgusting issues may make hurt the brain of the juvenile and have a tendency to debase or degenerate their psyche.
- **DEFAMATION:** It is a demonstration of ascribing any individual with expectation to drop down the pride of the individual by hacking his mail account and online networking record and sending a few sends

and messages with utilizing revolting dialect to obscure people mail account**.**

- **HACKING:** It implies unapproved control/ access over PC framework and demonstration of hacking totally annihilates the entire information and in addition PC programs. Programmers for the most part hacks media transmission and portable system and furthermore hack individual ledger, and hack client platinum card, Visa, savvy card number and use for change from one financial balance to various financial balance.
- **CRACKING:** It is among the gravest digital wrongdoings known till date. It is a repulsive inclination to realize that an outsider has broken into your PC frameworks without your insight and assent and has messed with valuable secret information and data.
- **E-MAIL SPOOFING:** A mock email might be said to be one, which distorts its starting point. It demonstrates its beginning to be not the same as which really it starts.
- **SMS SPOOFING:** Spoofing is a hindering through spam which implies the undesirable uninvited messages. Here a guilty party takes personality of another as cell phone number and sending SMS through web and beneficiary gets the SMS from the cell phone number of the casualty. It is intense digital wrongdoing against any person.
- **CARDING:** It implies false ATM cards i.e. Charge and Credit cards utilized by hoodlums for their financial advantages through pulling back cash from the casualty's ledger mala-fidely. There is constantly unapproved utilization of ATM cards in this sort of digital wrongdoings.
- **CHEATING AND FRAUD:** It implies the individual who is doing the demonstration of digital wrongdoing i.e. taking secret key and information stockpiling has done it with having blameworthy personality which prompts extortion and duping.
- **CHILD PORNOGRAPHY:** It includes the utilization of PC systems to make, disseminate, or get to materials that sexually misuse underage kids.
- **ASSAULT BY THREAT:** Alludes to debilitating a man with fear for their lives or lives of their families using a PC organize i.e. Email, recordings or telephones
- **CHEATING AND FRAUD:** It implies the individual who is doing the demonstration of digital wrongdoing i.e. taking secret word and information stockpiling has done it with having blameworthy personality which prompts misrepresentation and duping.
- **CHILD PORNOGRAPHY:** It includes the utilization of PC systems to make, disperse, or get to materials that sexually abuse underage youngsters.
- **ASSAULT BY THREAT:** Alludes to debilitating a man with fear for their lives or lives of their families using a PC organize i.e. Email, recordings or telephones.

CRIMES AGAINST PERSONS PROPERTY

Cybercrimes against all types of property incorporate unapproved PC trespassing through the internet, PC vandalism, transmission of unsafe projects, and unapproved ownership of modernized data. There are sure offenses which influences individual's properties which are as per the following:

- **INTELLECTUAL PROPERTY CRIMES:** The robbery or falsifying of merchandise, for example, computerized media, extravagance designs, pharmaceuticals, electronic products, and other fabricated merchandise. For sorted out hoodlums, the wrongdoing can be exceptionally productive and just a little venture is vital as a rule. The regular type of IPR infringement might be said to be programming robbery, encroachment of copyright, trademark, licenses, plans and

administration check infringement, burglary of PC source code, and so on.

- **CYBER SQUATTING:** Cyber hunching down alludes to illicit area name enlistment or utilize. Digital hunching down can have a couple of various varieties, however its basic role is to take or incorrectly spell an area name so as to benefit from an expansion in site visits, which generally would not be conceivable. Trademark or copyright holders may disregard to reregister their space names, and by overlooking this imperative refresh, digital squatters can without much of a stretch take area names. Digital hunching down additionally incorporates sponsors who mirror space names that are like prevalent, exceptionally trafficked sites. Digital crouching is one of a few kinds of cybercrimes. Digital hunching down is otherwise called area crouching.
- **CYBER VANDALISM**: Vandalism means deliberately destroying or damaging property of another. accounts to the act of damaging someone's data from the computer that in a way disrupts the victim's business or image due to editing the data into something invasive, embarrassing or absurd.. These acts may take the form of the theft of a computer, some part of a computer or a peripheral attached to the computer.
- **HACKING COMPUTER SYSTEM:** A hacker is any person engaged in hacking. The term hacking historically referred to constructive, clever technical work that was not necessarily related to computer systems. Today, however, hacking and hackers are most commonly associated with malicious programming attacks on networks and computers over the internet.
- **TRANSMITTING VIRUS:** The source of the infection was a single person on the airplane with influenza. Nasal secretions, which contain virus particles, are responsible for transmission by direct contact or by contaminated objects. An infected person will frequently touch their nose or conjunctiva, placing virus on the hand.
- **CYBER TRESPASS:** It intends to get to somebody's PC without the correct approval of the proprietor and does not aggravate, modify, abuse, or harm information or framework by utilizing remote web association and so forth.
- **INTERNET TIME THEFTS:** Basically, Internet time burglary goes under hacking. It is the utilization by an unapproved individual, of the Internet hours paid for by someone else. The individual who gains admittance to somebody elsea™s ISP client ID and watchword, either by hacking or by accessing it by illicit means, utilizes it to get to the Internet without alternate persona™s learning. You can recognize time burglary if your Internet time must be energized regularly, notwithstanding rare utilization

CYBERCRIMES AGAINST GOVERNMENT

Digital Terrorism is one unmistakable case of cybercrime against government. The development of Internet has demonstrated that the medium of the internet is being utilized by people and gatherings to undermine the administrations as additionally to threaten the natives of a nation. This wrongdoing shows itself into fear based oppression when an individual hacks into a legislature or military looked after site. There are sure offenses done by gathering of people meaning to debilitate the universal governments by utilizing web offices. It includes:

- **CYBER TERRORISM:** According to the U.S. Government Bureau of Investigation, digital psychological warfare is any "planned, politically inspired assault against data, PC frameworks, PC projects, and information which brings about brutality against non-warrior focuses by sub-national gatherings or secret specialists." Cyber fear based oppression exercises jeopardize the sway and uprightness of the country.

- **CYBER WARFARE:** It alludes to politically propelled hacking to lead harm and surveillance. Digital fighting is PC or system based clash including politically propelled assaults by a country state on another country state. In these kinds of assaults, country state performing artists endeavor to disturb the exercises of associations or country states, particularly for vital or military purposes and digital undercover work.
- **DISTRIBUTION OF PIRATED SOFTWARE**: It means distributing pirated software from one computer to another intending to destroy the data and official records of the government. Software piracy is the stealing of legally protected software. Under copyright law, software piracy occurs when copyright protected software is copied, distributed, modified or sold. Software piracy is considered direct copyright infringement when it denies copyright holders due compensation for use of their creative works.
- **POSSESSION OF UNAUTHORIZED INFORMATION:** It is very easy to access any information by the terrorists with the aid of internet and to possess that information for political, religious, social, ideological objectives.

CYBERCRIMES AGAINST SOCIETY AT LARGE

An unlawful act done with the intention of causing harm to the cyberspace will affect large number of persons. This offence includes:

- **CHILD PORNOGRAPHY**: It is substantial number of wrongdoing in world. It includes the utilization of PC systems to make, convey, or get to materials that sexually misuse underage kids. It likewise incorporates exercises concerning foul introduction and profanity.
- **CYBER TRAFFICKING**: It might movement in drugs, individuals, arms weapons and so forth which influences vast number of people. Trafficking in the internet is likewise a gravest wrongdoing in India.
- **ONLINE GAMBLING**: Online extortion and duping is a standout amongst the most lucrative organizations that are developing today in the internet. There are numerous cases that have become visible are those relating to Master card violations, authoritative wrongdoings, offering employments in various organizations, and so forth.
- **FINANCIAL CRIMES**: This sort of offense is normal as there is fast development in the clients of systems administration locales and telephone organizing where guilty party will endeavor to assault by sending fake sends or messages through web. Ex: Using Visas and check card by getting watchword unlawfully.
- **FORGERY**: It intends to cheat substantial number of people by sending undermining sends as on the web and sending secret information one email to another emails.

THE IMPACT OF COMPUTER CRIME ON BUSINESS

- Computer criminals cost billions in damages to businesses and individuals across the globe each year. Regardless of business efforts, there appears to be no end in sight to the growing threat of computer crime.
- The FBI has reported that computer criminals costs U.S. businesses about $67 billion a year according to Silicon.com. In a survey cited by President Obama, Americans have lost $8 billion in the past two years to computer crimes.
- Security Costs is defined as Silicon.com reports that businesses annually spend billions of dollars battling computer crimes.
- Growing Problem- Cyber-attacks have been around since the Internet was created,

according to "Time", and computer crime is growing more frequent. In that same article, it was reported that the Pentagon said there were 360 million attempts to break into computer networks in 2008.

- Tech-Savvy Criminals- Cyber criminals are getting smarter, learning new methods of attacking computers. A Canadian teen, for example, caused an estimated $1.7 billion in damages in a 2000 "denial-of-service" attack on eBay and Amazon.com, the "Time" article reported.
- Cyber Warfare- Criminals from China and Russia have infiltrated the U.S. electrical grid and planted software aimed at damaging the system, according to "Time." In turn, the Defense Department plans to create a command unit aimed at battling computer warfare. Business transactions are becoming the habitual need of today's life style.

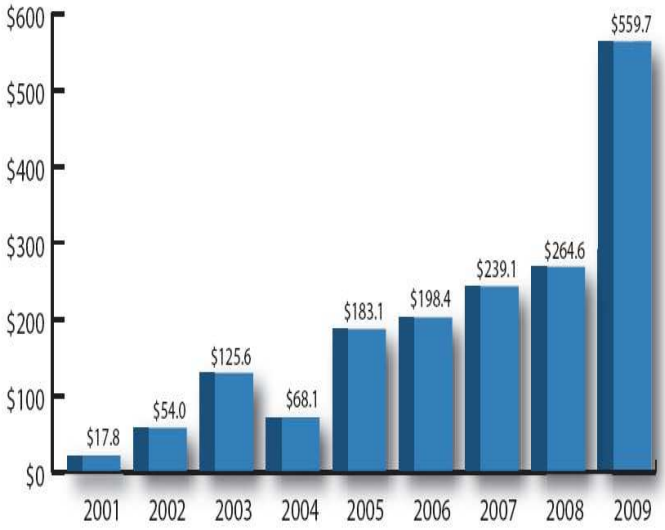
IMPACT OF CYBERCRIME ON PRIVATE INDUSTRY

Using three credits to portray cybercrime I would utilize the words meddling, quiet and unsafe. Simply the noiseless method of this sort of violations is a noteworthy issue in battling the danger, truth be told, regularly the organizations understand that they have been casualties of fakes or assaults until the point when long after the occasion happened. The outcomes are incapacitating and recover the circumstance is now and again incomprehensible, absolutely the time hole between the criminal occasion and its revelation gives favorable position to the individuals who carry out violations frequently unbridgeable that makes unthinkable any activity of abuse. In any case, we are accepting that the occasion is found by the casualties and this isn't generally valid, numerous organizations are in truth finished the years are casualties of cybercrime, yet they don't know, a disease that wrecks from inside.

Concurring the report "Second Annual Cost of Cyber Crime Study – Benchmark Study of U.S. Organizations" distributed by the Ponemon Institute, an examination depends on an agent test of 50 bigger measured associations in different industry segments, in spite of the abnormal state of consciousness of the digital risk the effect of cybercrime has genuine monetary results for organizations and government foundations. The report demonstrates that the middle annualized cost of cybercrime for 50 associations is $5.9 million every year, with a scope of $1.5 million to $36.5 million every year for each organization. The aggregate cost is expanded if contrasted with the principal investigation of the earlier year.

The lion's share digital assaults by and large allude to criminal action directed through the Internet that incorporate digital reconnaissance, reallocating on the web financial balances, making and dispersing infections to taint the casualties, posting classified business data on the Internet and disturbing a nation's basic national framework.

The accompanying outline 1 show that basically all organizations experienced assaults moved utilizing malware, exceptionally intriguing likewise the information identified with the activity made by the insider and the harms caused by social building assaults. The conclusion is that enterprises succumb to cybercrime, yet to various degrees and with various monetary effects.



PREVENTION OF CYBER CRIME

Counteractive action is constantly superior to cure. It is constantly better to avoid potential risk while working the net. One should make them his piece of digital life. A resident should remember the accompanying things – precautionary measure, counteractive action, insurance, Perseverance and protection. The accompanying can be dealt with:

- To avert digital stalking abstain from uncovering any data relating to one self. This is comparable to unveiling your personality to outsiders out in the open place.
- Always abstain from sending any photo online especially to outsiders and talk companions as there have been occurrences of abuse of the photos.
- Always utilize most recent and refresh antivirus programming to make preparations for infection assaults.
- Always keep move down volumes with the goal that one may not endure information misfortune in the event of infection tainting.
- Never send your Visa number to any site that isn't secured, to prepare for fakes.
- Always keep a watch on the locales that your youngsters are getting to keep any sort of badgering or depravation in kids.
- It is smarter to utilize a security program that gives control over the treats and send data back to the site as leaving the treats unguarded may demonstrate lethal.
- Websites proprietors should watch activity and check any abnormality on the webpage. Putting host construct interruption location gadgets with respect to servers may do this.
- Use of firewalls might be valuable.
- Web servers running open locales must be physically separate shielded from inner corporate system.

GOVERNMENT RULES

As of late, the Central Government made the tenets in the activity of the forces presented by sec 87(2) (CA), read with sec 6A (2) of the Information Technology Act, 2000. Such principles are known as the Information Technology (Electronic Service Delivery) Rules, 2011. These standards are intended to help or expound the arrangements of the IT Act. For bringing data security, rules are joined to legitimately convey open administrations through electronically by the proper Government or by its organization. It is given that the suitable Government may indicate the shape and way of Electronic Service Delivery and decide the way of scrambling delicate electronic records requiring

classification, while they electronically marked. Likewise all experts that issue any permit, allow, endorsement, authorize or endorsement electronically, might make, accomplish and keep up a store of electronically marked electronic records. The suitable Government determines the security methodology in regard of the electronic information, data, applications, and vault of carefully marked electronic records. The appropriate Government may direct every service provider and authorized agent to keep an updated and accurate account of the transactions, receipts, vouchers and specify the formats for maintaining accounts of transactions and receipt of payment in respect of the electronic services deliver and the said records shall be produced for inspection and audit before an agency or person nominated by the appropriate Government. Sensitive personal data or information of a person means such personal information which consists of information relating to:

- Password
- Financial information such as Bank account or credit card or debit card or other payment instrument details
- Physical, physiological and mental health condition
- Sexual orientation
- Medical records and history;
- Biometric information;
- Any detail relating to the above clauses as provided to body corporate for providing service; and
- Any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

CONCLUSION

This work discusses the implications of cyber-crime on the economy. Cyber-crime negatively affects the country's economy and is the fastest growing crime in the world. It has been a catalyst for the recent 'credit crunch' and will continue causing more financial' meltdowns' if more serious measures are not taken. There is an urgent need for education of the masses, starting from the children, teenagers, the business community and professionals etc. Judges, prosecutors and law enforcement officers need to be sensitized about how to prevent and prosecute cyber-crime. Secondly, an investment in technology and innovations is critical in the fight against cyber-crime. More attention should be paid to the next generation Internet and the development of security products

REFERENCES

[1]. Halder, D., & Jaishankar, K. (2011): Cyber-crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9.

[2]. Saul Hansell (2007): Social network launches worldwide spam campaign New York Times [3] Guillaume Lovet Fortinet, (2009): Fighting Cybercrime: Technical, Juridical and Ethical Challenges.

[3]. Mbaskei Martin Obono (2008): Cybercrimes: Effect on Youth Development http://www.i-genius.orgaccessed 26 the April 2012. [5] Parker D (1983): Fighting Computer Crimes, U.S. Charles Scribner's Sons.

[4]. An article "Urbanization and Cyber Crime in Nigeria: Causes and Consequences". VOL. 2, NO. 7, August 2012 ISSN 2225-7217.

[5]. Laura Ani (2011): "Cyber Crime and National Security: The Role of the Penal and Procedural Law.

[6]. Mbaskei Martin Obono (2008): Cybercrimes: Effect on Youth Development.

