Cyber Crime and Security, a Global Vulnerable Coercion: Obstacles and Remedies

Raja Sarath Kumar Boddu and Venkata Ramana Bendi

***Abstract*—Cyber Crime is a deliberate batter of fraudulent technological practice or psychological assault to divulge the sensible information knowingly or unknowingly, with or without authorization. At present, cyber attackers have adopted those criminal fraudulent techniques with most up-to-date technology on the internet and committing crimes. Approximately, one billion people have experienced the cyber crime in the last calendar year which costs approximately $445 billion. A concerted effort by all governments of the nations should frame policies that can protect citizens from financial and other frauds. This will result in eradicating poverty and other benefits from utilizing the recovered fraud money. Proposed blueprint would suggest amicable solutions to eliminate the cyber crime.**

***Index Terms*—Cyber security, e-commerce, preventive measures.**

I. Introduction

At present, computers play a vital role in our lives and advancements in technology will play even better role in near future. Present internet generation, with high digital connectivity would result growing number of users to World Wide Web tremendously. Despite its tremendous growth, Internet access is not distributed equally within or between countries. There is a clear gap between developed and undeveloped countries in implementing cyber security policies and practices. It is highly impossible to destroy cyber crime without serious commitment globally. This is one reason of cyber crimes explosion. On the other hand, since two decades, deceitful computer users have continued to use the computer to commit crimes. Voracious hackers commit fraud to steal sensitive data by using novel methods in intelligent way. The drastic growth in the popularity of the internet and in the use of communication between computers makes the subject of computer security very relevant. It expansion is abnormal with several direction; hence, single nation alone could not control it. All nations move forward, get close and declare rivalry against this cyber crime is the only way to control it. Technology development makes cyber security more complex. Unfortunately, the voracious hackers are always ahead and cheated many inhabitants without hindrance.

At this juncture, a well balanced technology is to be invented to prevent cyber crime and to provide cyber security with affordable solutions. The main aim of this study is to compare the cyber crime strategies in India and other major nations like, USA, Japan, China, Russia, Brazil and United Kingdom and to make necessary security recommendations to prevent the cyber crime [1]. This significance of this study is since it would compare the strategies that have been undertaken by the various countries to asses those which have been most effective, so that they could be adopted by the other. In general intercontinental alliance could be effective in checking cyber crimes.

Swindling money by cybercrime can then be channeled to eradicate entire poverty of some nations. On the other hand, the pain of the cyber crime victims could not be tolerable and sustainable. Rarely, introverted victims adverse behavior could also be an evident to this extent. Sincere efforts are essential to countenance it globally, firstly, it is highly essential to think and act by the all victim nations wholeheartedly and secondly, form a global grid with relevant experts to create an environment to fight against cyber crime and thirdly, search for feasible solutions to prevent it or at least to diminish it and finally, distribute the successful technology to the other nations outside the grid unconditionally as and when they succeeded.

A. Background

In March 1989, Sir Timothy John Berners-Lee, a British computer scientist, implemented the first successful communication between a client and server with Hypertext Transfer Protocol (HTTP). Subsequently, he developed HTML in 1990, which made a huge contribution to how to navigate and view the Internet today. Later days, he has known to this universe as the inventor of the World Wide Web (WWW) on August 6, 1991. That is what most people today consider the "Internet" or a series of sites and pages that are connected with links. The Internet as a whole had hundreds of people who helped developed the standards and technologies that make it what it is today, but without the WWW the Internet would not be as popular and useful as it is today. Berners-Lee's invention makes universe as global village. The internet has facilitated many technological changes especially in data transfer, e-commerce, online education, tremendous growth in technology, inter and intra continental knowledge transformation and other significant

Manuscript received May 23, 2017; revised September 1, 2017.

Raja Sarath Kumar Boddu is with Computer Science Department, Lenora College of Engineering, India (e-mail: iamsarathphd@gmail.com).

Venkata Ramana Bendi is with Information Technology Department, AITAM, Tekkali, India (e-mail: ramana.bendi@gmail.com).

doi: 10.18178/ijiee.2021.12.1.1

activities. Unfortunately, two decade innovative technology has been erroneously utilized by some passionate hackers by persuasive cyber crimes which are resulting billions of dollars loss only with financial pilfering. Today there are many crucial departmental/areas operations are depending on Information and Communications Technology (ICT) in an immense ways.

B. International Outlook on Cyber Crime

As per the statistics given by international telecommunication union, out of 7.1 billion of the population 39% are using internet. In Asia it is only 32%, population wise Asian continent contribution is very high when compared to other continents, but internet penetration is high in USA with 81% and Japan with 79.1%. A BBC report stated that cyber crime could cost 5% of their profit especially in Indian companies. Novel techniques, intellectual practice and expertise progression made hackers succeed [2]. Cyber crime not only limited to wealthy frauds, it expands cross boundaries with diversified areas like human relations damage, black mailing, forgery, cheating, stealing and so on. It enters into many areas and cracks several official and unofficial secret files, passwords, thefts related to government organization and non-government organizations of numerous inhabitants. Some intelligent hackers do the hacking to exhibit their bravery and technical competency. Resulting, 90% of the nations on the globe are the victims due to cyber crime [3]. Even though, each nation's preventive measures would rigorously try to reduce the cyber crime, the growth rate of cyber crime is increases day by day.

TABLE I: LIST OF TOP 6 COUNTRIES USING INTERNET AND ITS PENETRATION IN PERCENTILE

S.No.	Country	Internet users	Internet penetration (in %)
1	CHINA	568,192,066	42.3
2	USA	254,295,536	81.0
3	INDIA	151,598,994	12.6
4	JAPAN	100,684,474	79.1
5	BRAZIL	99,357,737	49.8
6	RUSSIA	75,926,004	53.3

II. NEED AND IMPORTANCE

Recently, Danish researchers' claims to have set a new data transfer world record by transmitting over a single optical fiber at an incredible speed of 43 terabits per second. Researchers at Technical University of Denmark (DTU) used a new type of optical fiber to claim the world data transfer record. As a matter of fact, now, a person could transfer 5375GB of data in 1 second [4]. These types of tremendous inventions could create world fastest network for excellent advancement of the technology boulevards and as well as terrible disruption actions also. At this juncture, the technocrats must think about the inventions invented and disruption abolished.

As per the survey of Norton conducted in 24 countries includes Australia, Brazil, Canada, China, France, Germany, India, Italy, Japan, New Zealand, Spain, Sweden, United Kingdom, United States; Belgium, Denmark, Holland, Hong Kong, Mexico, South Africa, Singapore, Poland, Switzerland and UAE, the Total cost of cyber crime would be US $388bn in 2012-13[5]. In India it was US$7.6bn which is less than 1% of USA. The overall opinion of the experts expressed that there would be 54% overall Computer viruses/malware and 11% of Online scams. The report stated that according to an international estimate one in 295 emails is virus infected and 3 in 100 emails carry malware. SophosLabs tracked and analyzed 95,000 malware pieces every day in 2010, which is nearly twice the number of malware pieces tracked in 2009. More than 3500 malicious websites are blocked per day and 89.4% mails are spam. The majority of the attacks (32%) are phishing followed by virus (29%) and network scanning/probing (18%)[6].This study is therefore important in to gain an insight in the strategies that are being undertaken by India and to find the effectiveness of these strategies so that each district could adopt the most effective strategy.

A. Worldwide Cyber Crimes

- Estimated $1 Trillion of intellectual property stolen each year (Gartner & McAfee, Jan 2009)
- Reported cyber attacks on U.S. government computer networks climbed 40% in 2008
- Sensitive records of 45,000 Federal Aviation Administration (FAA) workers breached (Feb 09)
- Design secrets of all U.S. nuclear weapons (Michelle Van Cleave) stolen

B. Major Threat to India

The cyber crimes in India resulted in 29.9 million people being victim of cybercrime involving direct financial losses to the tune of $4 billion, $3.6 billion in terms of time spent in resolving the crime, 4 out of every 5 online adults (80%) being victim of cybercrime and 17% of adults' online experiencing cybercrime on their mobile phones [7].

The attractive features in India are

- Rapidly growing online user base.
- Less literacy rate and high usage of E-commerce
- 121 million internet users in India
- In which,65 million active internet users,
- 50 million users use e-commerce and online shopping sites
- 46+ million Indians are using social network and

- 346 million mobile users had subscribed to data packages (Source: IAMAI; Juxt; wearesocial 2011)

Hence it is highly essential to act with suitable measures to prevent cyber crimes [8].

III. Cyber Crime Preventive Measures

The aim of this study is to minimize the drawbacks of various cyber crime scenarios and made recommendation systems and to improve the quality of various practices, which were measured by comparing the neighbor country investigations [9]. Finally, based on the observation and literature review some cyber security recommendations were proposed.

- To study the existing system being used on cyber crime and security measures and find out the ambiguity to resolve.
- To improve the quality of cyber crime prevention methodologies by adopting innovative technology with intercontinental support.
- To compare the constraint of the existing system with the derived metrics of newly proposed and then compute predictions and to establish their robustness during some uncertain conditions.
- To measure the quality of various scenarios and investigate the feasibility of the existing and proposed techniques periodically with comparison of the cyber crime intensity.
- To measure the incidents intensity of Cyber Threat globally and to share the remedy.
- To establish intercontinental cyber security Legal Framework and to observe strictly.
- Continuous and constituency intercontinental Participation to exchange new thoughts.
- To establish cyber security Education and Training universities across the nations and to recognize the talent globally.
- To establish global Emergency Response Team to share the threats and innovation.
- To establish Global Cyber Security Research and Development institutes.
- To establish Cyber Appellate Tribunal with the support of international cyber law with intercontinental prospective.

A. Intercontinental Web Server Interfaces Are to Be Established to Authenticate Each As Follows

- Route and IP address the user is accessing the web site;
- number of prior visits to the web site made with details;
- URL of the page that contained the link to get the user to the web site;
- user's browser type and operating system and version;
- scripting languages enabling on the user's computer and its functioning;
- how many web pages the user has visited in the current session;
- File Transfer Protocol details.

The information would be saved at CentralIntercontinental Web Server to analyze as and when required. It is highly useful to prevent cyber crimes by alerting and swap over information.

IV. Conclusions

Cyber crime is an emergent and severe menace to individuals, organization government and non-government sectors. Cyber crime with its complexities has proven tricky to combat due to its nature. Extending the rule of law is a crucial step towards creating a trustworthy environment. Make it accountable for each citizen, government, non-government organizations. Educate citizens on cyber security for their systems. Make provision for strict laws to effectively frighten cybercrime. As mentioned, an intercontinental cyber crime agreement along the lines of that under consideration could help reduce and battle cyber crimes. It avoids many of the obstacles that would defeat an accord that attempted to restrict the scattering of cyber crime. Organization should provide security for their networks voluntarily with the intimation to the central intercontinental as mentioned earlier so that it becomes possible to make obligatory laws and punishment for whoever gets in the way with their property. Finally, there should be a vigorous association between the organizations, government and non-government sectors to strengthen cyber legal frameworks for cyber security unanimously.

References

[1] R. P. Kaur, "Statistics of cyber crime in India: An overview," *International Journal Of Engineering And Computer Science*, ISSN: 2319-7242, vol. 2, issue 8, August, 2013, pp. 2555-2559.

[2] A. K. Shrivastav and Ekata, "ICT penetration and cybercrime in India: A review," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, issue 7, July 2013.

[3] Delhicourts. [Online]. Available: http://delhicourts.nic.in/ejournals/CYBER%20LAW.pdf

[4] R. Anderson, C. Barton *et al*., "Measuring the cost of cybercrime," UK Ministry of Defence, 2012.

[5] B. Muthukumaran, "Cyber crime scenario in India," *Criminal Investigation Department Review*, January 2008.

[6] MCAFEE Report, "Net losses: Estimating the global cost of cybercrime," Economic Impact of Cybercrime- II in MCAFEE, Center for Strategic and International Studies, June 2014.

[7] Norton. [Online]. Available: http://norton.com/cybercrimereport

[8] Goutham Kacheru, "The Future of Cyber Defence: Predictive Security with Artificial Intelligence", International Journal Of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST), VOLUME 7,ISSUE 12 - DECEMBER 2021, pp.46–55.

[9] Kacheru, G. (2020). The role of AI-Powered Telemedicine software in healthcare during the COVID-19 Pandemic. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 11(3).

Raja Sarath Kumar Boddu received his B.E, M. Tech and Ph.D. degrees from the Andhra University College of Engineering, Andhra University, Visakhapatnam, India. Currently he is working as a professor in the Faculty of Computer Science Engineering and principal at Lenora College of Engineering (http://www.lce.ac.in), affiliated to JNT University, Kakinada, AP, India. Dr. Raja Boddu highly motivated, self-driven,moderate educator and administrator with 17 years experience in Engineering Education. So far, 19 PG dissertations supervised, 25 peer-reviewed publications published and 3 International Conferences have been addressed. Dr. Raja Boddu taught Diploma, B. Tech and M. Tech students in the areas of Artificial Intelligence, Web Technologies, Network Security, Data Mining and Nano Technology. He has been a Faculty member and course Director for Computer Science for number of courses. Dr. Raja Boddu has participated/delivered, lectures/chaired technical sessions/ seminars organized by various academic bodies and professional societies. Dr. Raja Boddu has several memberships of high profile program committees, review boards, as a Fellow of IEI, as a Life Member of IETE, ISCA and CSI, as a Senior Member of IEEE and ACM and as a Reviewer for IEI-Springer Series-B Journals, SAI Organization journals and Springer's Journal of supercomputing.

Bendi Venkata Ramana received his doctor's degree from Andhra University, the M.Tech from Jawaharlal Nehru Technological University, Kakinada and the B.Tech from Nagarjuna University, Guntur, India. He is currently working as professor and head of the Department, Information Technology, Aditya Institute of Technology and Management, India. He has published 18 papers in international Journals and conferences. He has 95 Google scholar citations.