IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-5, Issue-8 E-ISSN: 2347-2693

Ethical Aspects of Software Engineering:A wake up call for India

Juneed Iqbal[1*], Bilal Maqbool Beigh[2]

[1*]Department of Computer Science, Mewar University, Chittorgarh, India
[2]Department of Computer science, Cluster university of Kashmir, Srinagar, India

[*]*Corresponding Author juny@live.in, +919906571153*

Available online at: www.ijcseonline.org

Received: 12/Jul/2017, Revised: 23/Jul/2017, Accepted: 16/Aug/2017, Published: 30/Aug/2017

***Abstract*—** Software Engineering has a direct and vigorous effect on individuals, societies, nations and to the whole world. Ignoring or not considering social context of software development can lead to catastrophic consequences. India which has become global leader as its software industry is touching skies can't sustain it unless its software engineers do not practise better Software design and development practices. Indian government is pushing its software industry further up by its digital India program, creating an ecosystem full of technical manpower, elite technical institutes etc. With the tremendous growth of software development in India, there are also serious threats due to lack of ethics and professionalism.

***Keywords*—** Software Engineering, Ethics, professionalism, Digital India, Cybercrimes

I. INTRODUCTION

The objective of this study is to comprehend ethical aspects of software engineering and to broaden its domain. Software Engineer has to be professionally responsible and should add to its repertoire the social values and the laws. This article focuses on skills of software engineer to thinking logically and analytically about these ethical issues, so as to responsibly confront ethical issues. This article emphasises on the growing software industry of India as a world leader and its challenges pertaining to ethics and professionalism.

This article is divided into three sections. First section explores ethical aspects of software engineering in terms of harms to public, obligations, professional responsibilities, social implications of the Internet ,computer crimes etc. We also discuss here ethical issues proposed by Mason like privacy, accuracy, property and accessibility. Second sections discusses the catastrophic consequences of faulty software or software used in faulty manner which can lead to damage of life and property. This section illustrates the importance of social context of software development with the help of case study and explores bad Software design and development practices, lethal software bugs, programming glitches, software design and specification errors, dark side of internet etc. Third section discusses about the Indian software industry and its challenges regarding software engineering and its ethical issues. India has a greater

Challenge for being a software development giant. This section discusses digital India dream, growing computer crimes and lack of professionalism in Indian software engineers.

II. ETHICAL ASPECTS OF SOFTWARE ENGINEERING

Software Engineering is relatively a new engineering discipline which at every phase of professional software development applies various theories, methods and tools. Software development is so pervasive that it has become a life line of modern societies. It is software which runs all departments of our society e.g. applications used in health, defense, finance, personnel, library, education, legal, transportation and many other such systems which drive our society. Software engineering not only has a concern to build an artifact but also needs to take in its problem domain direct and critical social implications and thus has to deal with a much broader ethical responsibility [1].

Software Engineer has to concern himself of the technical aspects of software development as well as its social implications, as his work can affect seriously not only people using his software but also other people who may come under influence of his software.

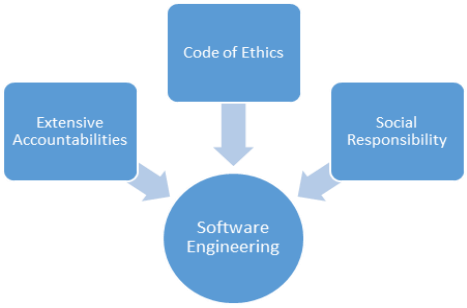

Figure 1

Software Engineer has to widen its problem domain by considering and identifying ethical issues and social context besides his technical expertise considering following [2] :

- The types of harms the public can suffer as result of this work;
- How software engineers contribute to the good life for others;
- Who exactly are the 'public' to whom the engineer is obligated;
- Why the software engineer is obligated to protect the public;
- What other ethical obligations software engineers are under;
- How software engineers can actually live up to ethical standards;
- What is the end goal of an ethical life in software engineering;
- What are the professional codes of software engineering ethics;

Mason in 1986, listed four pertinent ethical issues which are summarized by an acronym – PAPA: privacy, accuracy, property and accessibility [3].

Privacy: What information about one's self or one's associations must a person reveal to others, under what conditions and with what safeguards? What things can people keep to themselves and not be forced to reveal to others?

Accuracy: Who is responsible for the authenticity, fidelity and accuracy of information? Similarly, who is to be held accountable for errors in information and how is the injured party to be made whole?

Property: Who owns information? What are the just and fair prices for its exchange? Who owns the channels, especially the air-ways, through which information is transmitted? How should access to this scarce re-source be allocated?

Accessibility: What information does a person or an organization have a right or a privilege to obtain, under what conditions and with what safeguards? [3]

Software Engineering has specific ethical concerns which were emphasized in ACM-IEEE Joint Task Force on Computing Curricula which include [4]:

- Social context of Computing
- Methods and tools of analysis of ethical argument
- Professional and ethical responsibilities
- Risks and liabilities of safety-critical systems
- Intellectual property
- Privacy and civil liberties
- Social implications of the Internet
- Computer crime
- Philosophical foundations of Ethics

Social context of computing:
Social implications and repercussions of computing is a major concern for software engineer, which has become worse by the uncontrolled growth of internet and networked communication. Social context of computing also has concerns like gender discrimination, international issues and ecological issues, which a software engineer has to be aware of.

Methods and tools of analysis:
Software Engineer has to make ethical decisions after evaluation of ethical arguments and ethical choices. Methods and tools is required to acknowledge the social context of design.

Professional and ethical responsibilities:
Software Engineer has to be professionally responsible and should adhere by the Social values and the laws. Software Engineer has to responsibly confront ethical issues by his skill of thinking logically and analytically about these ethical issues. We believe to make software engineering a profession is the best way to apply ethics to software engineering and huge amount of work is needed to make software engineering a profession in India.

Risks and liabilities of computer-based systems:
Software engineer should be aware of implications of software complexity and risks, so software engineer has to be skilled enough to assess and manage risk.

Intellectual property:
Software engineers should be aware of foundations of intellectual property. The laws governing the use of intellectual property should also be known like, copyrights, patents, trade secrets etc. There are many other concerns of intellectual property like software piracy, international issues, software patents, etc. software engineer should be fully aware of all such concerns pertaining to intellectual property.

Privacy and civil liberties:
Software engineer should be aware of ethical and legal foundations for privacy protection. Huge database systems have privacy repercussions which a software engineer should be aware of and also should be acquainted with technological strategies for privacy protection. Software built by engineers has no boundary so international and intercultural issues also need to be dealt with. There are also issues which need to be considered like freedom of expression in cyberspace.

Computer crime:
Software engineer should be able to prevent computer crimes by applying crime prevention strategies. If not prevented

computer crimes should be detected and then recovery mechanism need to be applied. Computers or computer network can be used multiple ways as a tool to commit a crime. In 2001 Convention on Cybercrime[5] lists following:

- Article 2 Illegal access
- Article 3 Illegal interception
- Article 4 Data interference
- Article 5 System interference
- Article 6 Misuse of devices
- Article 7 Computer-related forgery
- Article 8 Computer-related fraud
- Article 9 Offenses related to child pornography
- Article 10 Infringements of copyright and related rights
- Article 11 Attempt and aiding or abetting

India has so far not signed the Budapest convention, we strongly suggest that India should sign the convention to give a space for a common criminal policy and international cooperation to combat computer related crimes.

Economic issues in computing:
Software Engineer must be aware of many economic issues and there implications like monopolies, effect of skilled labor supply and demand on the quality of computing products, pricing strategies in the computing domain, differences in access to computing resources and the possible effects thereof[6].

Philosophical frameworks:
Software Engineer should be aware of philosophical frameworks like Traditional ethical theories, problems of ethical relativism, scientific ethics in historical perspective and differences in scientific and philosophical approaches[6]

III. DARK SIDE OF SOFTWARE ENGINEERING

Software is extensively used in almost all areas, especially which are safety critical and extremely sensitive to errors. The flaws in software can lead to a catastrophic consequences in terms of damage to life and property. Faulty Software or software used in faulty manner can have serious ethical and social consequences, skipping social context from software development can have dire consequences. History is replete with such examples:

Lethal Software Bug:
September 26th, 1983, a software bug in Soviet Union's ballistic missile early warning system nearly triggered WWIII, The soviet early warning software system warned that five ballistic missiles are launched by US[7].The fault was due to software system that falsely detected missile launch due to satellite picking reflections off cloud-tops[7]. It was Stanislav Petrov, a lieutenant-colonel in the military intelligence section of the Soviet Union's secret service who literally saved the world[8].

Bad Software design and development practices:
A computerized radiation therapy machine, Therac-25, between June 1985 and January 1987, due to errors in the Therac-25's software, massively overdosed patients at least six times. Several patients died and many were severely injured[9]. Therac-25 is a classic example which illustrates that besides coding errors it is software engineering principles, the software design and development practices which are deciding factors for a software to be safe.

HMS Sheffield:
The British destroyer H.M.S. Sheffield was hit by Exocet missile and was sunk in the Falkland Islands war. British arsenal includes the Exocet's homing device thus ship's radar warning systems were programmed to deem the Exocet missile as "friendly" [10][11] .

Wrong Input Data:
On 28th November, 1979, an Air New Zealand airliner crashed into an Antarctic mountain killing all 237 passengers and 20 crew on board. The accident known as the Mount Erebus disaster happened due to the incorrect co-ordinates of the flight path to its navigational computer leading to wrong path of Mount Erebus[12].

Programing Glitch:

- Gemini V, NASA'S manned spaceflight in its Gemini program missed its landing point by 100 miles because its guidance program ignored the motion of the earth around the sun[12].
- A program testing resistance of nuclear reactors to earthquakes used an arithmetic sum of variables instead of the square root of the sum of the squares of the variables which shut down five nuclear reactors[12].
- The Soviet Phobos I Mars probe was lost, due to a faulty software update, at a cost of 300 million rubles. Its disorientation broke the radio link and the solar batteries discharged before reacquisition[13].
- On February 25, 1991, during the Gulf War, Iraqi Scud missile pierced an American Patriot Missile battery in Dharan, Saudi Arabia killing 28 soldiers. A report of the General Accounting office, GAO/IMTEC-92-26, entitled "Patriot Missile Defense: Software Problem Led to System Failure at Dhahran, Saudi Arabia" reported on the cause of the failure: "The range gate's prediction of where the Scud will next appear is a function of the Scud's known velocity and the time of the last radar detection. Velocity is a real number that can be expressed as a whole number and a decimal (e.g., 3750.2563...miles per hour). Time is kept continuously by the system's internal clock in tenths of seconds but is expressed as an integer or whole number (e.g., 32, 33, 34...). The longer the system has been running, the larger

the number representing time. To predict where the Scud will next appear, both time and velocity must be expressed as real numbers. Because of the way the Patriot computer performs its calculations and the fact that its registers are only 24 bits long, the conversion of time from an integer to a real number cannot be any more precise than 24 bits. This conversion results in a loss of precision causing a less accurate time calculation. The effect of this inaccuracy on the range gate's calculation is directly proportional to the target's velocity and the length of the system has been running. Consequently, performing the conversion after the Patriot has been running continuously for extended periods causes the range gate to shift away from the center of the target, making it less likely that the target, in this case a Scud, will be successfully intercepted"[14].

- The Mars Climate Orbiter (MCO) crashed in September 23, 1999. The mishap happened due to the failure to use metric units in the coding of a ground software file, "Small Forces," used in trajectory models, which lead to incorrect trajectory by a factor of 4.45, which is the required conversion factor from force in pounds to Newtons [18].

Software Design and Specification Errors:

On 4 June 1996, the maiden flight of the Ariane 5 Europe's newest and unmanned satellite-launching rocket launcher ended in a failure just few seconds after taking off, at an altitude of about 3700 m, the launcher deviated from its flight path and exploded. The failure was due to design and specification errors in the software of the inertial reference system[15]." This shutdown occurred 36.7 seconds after launch, when the guidance system's own computer tried to convert one piece of data -- the sideways velocity of the rocket -- from a 64-bit format to a 16-bit format. The number was too big, and an overflow error resulted. When the guidance system shut down, it passed control to an identical, redundant unit, which was there to provide backup in case of just such a failure. But the second unit had failed in the identical manner a few milliseconds before. And why not? It was running the same software,"[16].

Y2K problem:

Millennium bug also known as Y2K problem, or year 2000 problem, is one such example which has immense social and ethical concerns. It was like a software time bomb. Earlier programmers used two digits for representing year. "According to the scenario of the crisis when the date goes from 1999 to 2000 many old computer software that has not been fixed will register the date - because of their two-digits year-representation - not 2000 but 1900 which will induce an escalation of technical problems in the infrastructure of the highly computerized society. This process will very probably produce a complete chaos leading to finally at a global corruption of the modern civilization"[17]. Y2K is a typical example of short-sightedness and failure to perceive long term consequences, which can lead to catastrophic and devastating consequences.

Suicide Game:

An internet game called The Blue Whale Game in which participants are invited to complete many tasks within a 50 day period. The tasks are like self-harming, having lesser sleep, watching scary movies etc. The game targets teen and to win the game one has to committing suicide. This game has killed many children in Russia and UK. On 30 July 2017, a 14-year-old boy allegedly committed suicide by jumping from the fifth floor of an Andheri (East) building in the city of Mumbai[18].

WannaCry Ransomware Attack:

This Game took a huge toll of an estimated 300,000 users in 150 countries. Mike Hinchey, President of IFIP (International Federation for Information Processing) warned that "While we don't yet know who is responsible for the WannaCry attacks, we do know that the ransomware was developed out of exploits leaked or stolen earlier this year from America's National Security Agency (NSA), which had been stockpiling them for use in surveillance,"

Dark side of internet

Computers with the advent of Internet has occupied a huge space called "Cyberspace", upon which human race is totally dependent and thus has created alarming social and ethical concerns. Cyber criminals possess a huge threat as they use cyberspace to harm from single individual to a global enterprise. Internet which has become a life line of modern economy, education, communication, healthcare and almost all aspects of human activities also has a dark side in terms of crime opportunities of global proportion, which transcends not only physical boundaries but also human imaginations. These crimes called "Cybercrimes" committed using cyberspace i.e. computers and a network like Internet are of huge concern at global level[19]. Cybercrimes are done to target computer network or devices like Viruses, malicious code or malware, denial of service attack etc. Cybercrimes also include crimes facilitated by computer devices or networks like child pornography, terrorism, phishing scams, identity theft, cyber stalking, spam etc. Cybercrime is increasing at an alarming rate as it is now done in an organized fashion by highly skilled computer professionals creating a much greater threat on societies, nations and for the whole world. On October 5, 2016 during 71st Session of the General Assembly First Committee The United Nations Institute for Disarmament Research (UNIDIR) held a side event on cyberspace and international peace and security "discussed the important details of cybersecurity in the modern world and how Information and Communications

Technologies (ICT) are increasingly influential on economic, scientific, social, and political developments"[20].

Faulty Aadhaar app developed by NIC:

National Informatics Centre (NIC) is a government body of India that links central and state governments every department and ministry by a digital networks which it builds and maintains. It also extends Aadhaar-enabled services for numerous welfare programmes. The eHospital app developed by NIC has a serious security loophole, the app did not encrypt its communication with NIC's servers and password was hardcoded in the eHospital application. which gave unauthorized access to the Aadhaar data requested from "Mygov", a free android app created by Bengaluru-based software developer, Abhinav Srivastava. He was arrested on 26 July 2017, till then his app had already been downloaded 50,000 times putting to risk Aadhaar numbers and personal details of thousands of citizens, revealing how digitizing government services at the cost of cybersecurity can put the personal data of citizens at risk. Dr Sandeep Shukla, head of the Computer Science department at IIT Kanpur said "NIC is the biggest government implementer of e-governance, it is an unpardonable offence that they have made such a huge mistake," he further claimed "NIC is incompetent but unfortunately all government activities happen through NIC"[21].

IV. WAKE UP CALL FOR INDIA

In present age software is a major entity as it has become an integral part of every component of human activities. The exploration of above cases pertaining to software failures in terms of a programming bug, software design and specification errors, programming glitches etc., depicts that software failure can be catastrophic leading to the loss of life, triggering wars, disrupting peace and also it can lead to severe financial losses. Cybercrime is also evolving as a serious threat. Indian software industry in last 20 years has grown dramatically at the rate of more than 30 percent a year. India has a serious challenge regarding software engineering and its ethical issues.

India as a software development giant

According to the report of Electronic and Computer Software Export Promotion Council (ESC) during the period April 2015 to March 2016, export of software is estimated to have reached to a level of US$ 107 billion and during the period April to September 2016, export of Software has reached to an estimated value of US$ 57.1 billion[22]. The Indian software industry has from about $50 million in exports in the late 1980s, in 1993 it reached to $200 million, in 2001 software exports grew 50–60 percent annually, reaching $6 billion. It has grown tremendously to go beyond 100 billion. Indian IT-ITES industry revenue recording an increase of around 8.8% is estimated at USD 141.0 billion in FY2016-17 as compared to USD 129.5 billion in FY2015-16,. The overall industry's growth of this sector over the last five years is given in the Figure 1 [23].

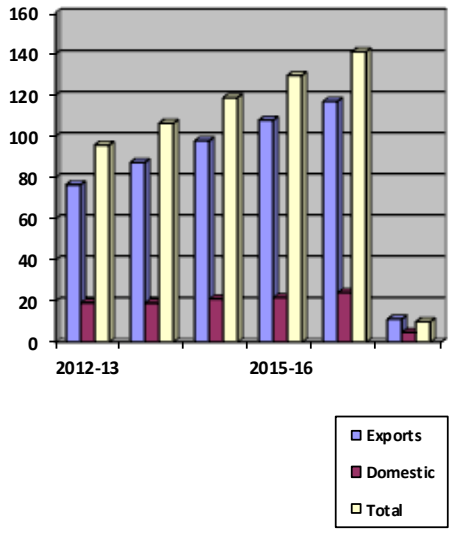

Figure 2

Evans Data Corp. in its latest Global Developer Population and Demographic Study 2017 reports that India is projected to have the largest software developer population by 2021. As per Evans Data projects there are about 18.2 million software developers worldwide, which will increase by 45% and it will rise to 26.4 million by 2019. Report further suggests that presently, the U.S. has about 3.6 million software developers while India has about 2.75 million. Report emphasized on the fact that India has a huge population of 1.2 billion and 50% of India population is under 25 years thus by 2018, India will overtake U.S by having 5.2 million developers, a nearly 90% increase, versus 4.5 million in the U.S., a 25% increase though that period. A T Kearney's 2016 Global Services Location Index(GSLI) based on an assessment of 38 metrics, rated India as the number one countries with the strongest underlying fundamentals to potentially deliver information technology (IT), business process outsourcing (BPO), and voice services[24]. Tremendous increase in software developer population is due to following reasons:

- Low wages of Indian developers attract companies all over world to hire developers and engineers from India.
- Lower infrastructure buildup and maintenance cost saves huge money.

- India is positioned on the other side of globe, thus giving opportunity for companies to work for a 24 hour.

Digital India

Government of India launched a flagship Programme on 1 July 2015 called Digital India with a vision to transform India into a digitally empowered society and knowledge economy. Digital India is an umbrella programme blending together whole lot of concepts, thoughts, initiatives and ideas into a one larger goal i.e. to make India a knowledge economy run by digitally empowered society. Digital India programme has nine initiatives or pillars of growth areas[25]:

1. Broadband Highways :

This project is about deploying high speed broadband connectivity to all rural areas, urban areas and at national level. The project aimed laying optical fibre under the National Optical fibre Network (NOFN) in all 2.5 lakh gram panchayats by 2016. In urban areas Virtual Network Operators would be leveraged for service delivery and communication infrastructure and at national level National Information Infrastructure (NII) will integrate State Wide Area Network (SWAN), National Knowledge Network (NKN), National Optical Fibre Network (NOFN), Government User Network (GUN) and the MeghRaj Cloud to make one platform to various government departments up to the panchayat level.

2. Universal access to Mobile Connectivity:

This project is about mobile coverage of around 55,619 uncovered villages in a phased manner during 2014-18.

3. Public Internet Access Programme :

This project is about providing internet services to 2.5 lakh villages which comprises of one in every panchayat by March 2017 and 1.5 lakh post offices which will become Multi service centers.

4. e-Governance – Reforming Government through Technology:

This project is about reforming government through technology by providing online application submission, online storage of documents and Integration of services and platforms" e.g. Aadhaar platform of Unique Identity authority of India (UIDAI), Mobile Seva platform, payment gateway sharing of data through open Application Programming Interfaces (API) and middleware such as National and State Service Delivery Gateways (NSDG/SSDG) should be mandated to facilitate integrated and interoperable service delivery to citizens and businesses"[26].

5. E-Kranti - Electronic delivery of services

On 25 march 2015 Union Cabinet approved E-Kranti with the vision of "Transforming e-Governance for Transforming Governance" based on following key principles[27]:

1. Transformation and not Translation - All project proposals in e-Kranti must involve substantial transformation in the quality, quantity and manner of delivery of services and significant enhancement in productivity and competitiveness.
2. Integrated Services and not Individual Services - A common middleware and integration of the back end processes and processing systems is required to facilitate integrated service delivery to citizens.
3. Government Process Reengineering (GPR) to be mandatory in every MMP - To mandate GPR as the essential first step in all new MMPs without which a project may not be sanctioned. The degree of GPR should be assessed and enhanced for the existing MMPs.
4. ICT Infrastructure on Demand – Government departments should be provided with ICT infrastructure, such as connectivity, cloud and mobile platform on demand. In this regard, National Information Infrastructure (NII), which is at an advanced stage of project formulation, would be fast-tracked by DeitY.
5. Cloud by Default – The flexibility, agility and cost effectiveness offered by cloud technologies would be fully leveraged while designing and hosting applications. Government Cloud shall be the default cloud for Government Departments. All sensitive information of Government Departments shall be stored in a Government Cloud only. Any Government Department may use a private cloud only after obtaining permission from Department of Electronics and Information Technology which shall do so after assessing the security and privacy aspects of the proposed cloud.
6. Mobile First - All applications are designed/ redesigned to enable delivery of services through mobile.
7. Fast Tracking Approvals – To establish a fast-track approval mechanism for MMPs, once the Detailed Project Report (DPR) of a project is approved by the Competent Authority, Empowered Committees may be constituted with delegated powers to take all subsequent decisions.
8. Mandating Standards and Protocols – Use of e-Governance standards and protocols as notified by DeitY be mandated in all e-governance projects.
9. Language Localization - It is imperative that all information and services in e-Governance projects are available in Indian languages as well.
10. National GIS (Geo-Spatial Information System) - NGIS to be leveraged as a platform and as a service in e-Governance projects.
11. Security and Electronic Data Preservation - All online applications and e-services to adhere to prescribed security measures including cyber security. The National

Cyber Security Policy 2013 notified by DeitY must be followed.[27]

6. *Information for All*

This project is about government to engage with citizens pro-actively through social media, web based platforms, emails and SMS services.

7. *Electronics Manufacturing*

This project is about NET ZERO imports by 2020 by promoting electronics manufacturing in the country by better taxation, incentives, skill development, R&D in electronics etc.

8. *IT for Jobs*

This project is about training youth in towns and villages for IT sector jobs, It also focuses on setting up BPOs in each North-eastern state. It has eight components with specific scope of activities[28]:

1. IT Trainings to people in smaller towns and villages
2. The target of this component is to train one crore students from smaller towns & villages for IT sector jobs over 5 years. DeitY is the nodal department for this scheme.
3. IT/ITES in Northeastern States
4. This component focuses on setting up BPOs in every north-eastern state to facilitate ICT enabled growth in these states. DeitY is the nodal department for this scheme.
5. Training Service Delivery Agents
6. The focus is on training three lakh service delivery agents as part of skill development to run viable businesses delivering IT services. DeitY is the nodal department for this scheme.
7. Training Rural Workforce on Telecom and Telecom related services
8. This component focuses on training of five lakh rural workforce the Telecom Service Providers (TSPs) to cater to their own needs. Department of Telecommunications (DoT) is the nodal department for this scheme.[28]

9. *Early Harvest Programmes*

This project is about digitizing government institutions, schools, Universities etc, and implementing following within short timeline[29] :

- IT Platform for Messages
- Government Greetings to be e-Greetings
- Biometric attendance
- Wi-Fi in All Universities
- Secure Email within Government
- Standardize Government Email Design
- Public Wi-Fi hotspots
- School Books to be eBooks
- SMS based weather information, disaster alerts
- National Portal for Lost & Found children

The dark sides of cyberspace

Internet has become a life line for modern societies and is prerequisite for the functioning of such societies. From large enterprise and national economies to individual consumers and upstart entrepreneurs, everyone is dependent on Internet. Internet has changed every aspect of our society, it has created enormous opportunities but with it comes the greater risk to security and privacy. Internet is being used by everyone, so it brings with it predators, cyber criminals, hackers etc. who misuse internet to harm people. Asian countries are on the top of internet usage list and India has taken the second position among the top Internet users. Indian growth of Internet usage is as per its dream of "digital India", but with it we need efficient policies and law to counter any threat due to misuse of Internet.

Internet Users in the World
By Geographic Regions- 2017

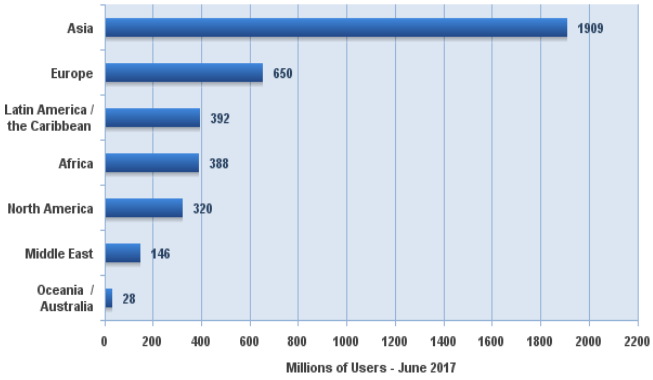

Figure 3

Source : Internet World Stats- http://www.internetworldstats.com/stats.htm

Top Ten Internet Countries in Asia
March 31, 2017

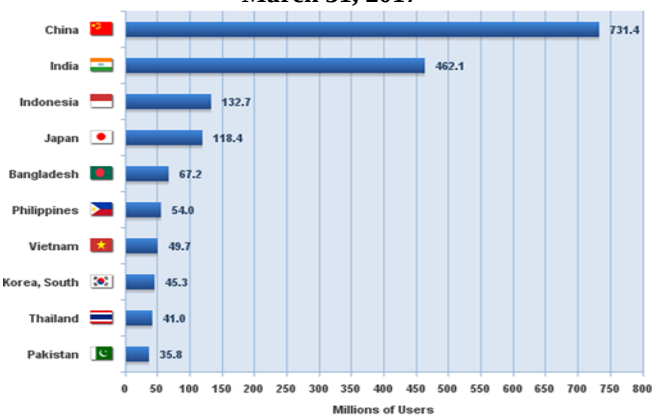

Figure 4

Source: Internet World Stats- http://www.internetworldstats.com/stats3.htm

India has a serious challenge to curb increasing cybercrimes due to lack of robust cyber law and cybercrime investigation organizations. On July 2, 2013 the National Cyber Security Policy 2013 was released with an aim for protection of information infrastructure in cyberspace, reduce vulnerabilities, build capabilities to prevent and respond to cyber threats and minimize damage from cyber incidents, but unfortunately it has not been fully implemented in India so far. India has a deficiency in terms of modern cybercrime police force, formulation of regulations and guidelines for effective investigation of cybercrimes and the formulation of effective cybercrime prevention strategy[30]. According to NASSCOM, there is extremely low rate of conviction of cybercrime in India, thus India has to work in these areas to make them robust and effective.

According to National Crime Record Bureau, India, statistical information there is unceasing growth in the cybercrimes in India. Cases of cybercrimes (IT Act + IPC sections + SLL crimes) have increased by 20.5 %(from 9,622 cases in 2014 to 11,592 cases in 2015) in 2015 as compared to 2014, as it is clear from figure 5 and Figure 6 below.

Cyber Crimes/Cases Registered and Persons Arrested under IPC during 2013-2015

Sl. No	Crime Heads under IPC Crimes	Cases Registered			% Var.	Persons Arrested			% Var.
		2013	2014	2015		2013	2014	2015	
1	Offences by Public Servant	1	0	0	-	2	0	0	-
2	Fabrication/Destruction of Electronic Records for Evidence	12	1	4	300.0	11	1	2	50.0
3	Cheating@	-	1,115	2,255	102.2	-	335	754	55.6
4	Forgery	747	63	45	-28.6	626	58	72	19.4
5	Data Theft@	-	55	84	52.7	-	11	135	91.9
6	Criminal Breach of Trust	518	54	42	-22.2	471	39	1,292	97
7	Counterfeiting *	59	10	12	20.0	93	8	14	42.9
8	Others	-	974	980	0.6	-	772	598	-29.1
Total Offences under IPC		**1,337**	**2,272**	**3,422**	**50.6**	**1,203**	**1,224**	**2,867**	**57.3**

Figure 5

Source : National Crime record bureau

Patterns of Cases Reported and Persons Arrested under IT Act during 2013 – 2015 and Percentage Variation during 2015 over 2014

SL	Crime heads under IT Act	Cases Registered			% Var.	Persons Arrested			% Var.
		2013	2014	2015		2013	2014	2015	
1	Tampering Computer Source Documents (Sec. 65 of IT Act)	137	89	88	-1.1	59	64	62	-3.1
2	Computer Related Offences(Sec. 66 to 66E of IT Act)	2,516	5,548	6,567	18.4	1,011	3,131	4,217	34.7
3	Cyber Terrorism@(Sec. 66F of IT Act)	-	5	13	160.0	-	0	3	-
4	Publication/Transmission of Obscene/Sexually Explicit Content(Sec. 67 to 67C of IT Act)	1203	758	816	7.7	737	491	555	13
5	Intentionally not Complying with the Order of Controller(Sec. 68 of IT Act)	13	3	2	-33.3	3	4	3	-25
6	Failure to Provide or Monitor or Intercept or Decrypt Information(Sec. 69 of IT Act)	6	2	0	-100	7	0	0	-
7	Failure to Block Access any Information Hosted etc.@ (Sec. 69A of IT Act)	-	1	0	-100	-	0	0	-
8	Not Providing Technical Assistance to Govt. to Enable Online Access@(Sec. 69B of IT Act)	-	0	3	-	-	0	0	-

9	Un-authorized Access/Attempt to Access to Protected Computer System(Sec. 70 of IT Act)	27	0	8	-	17	0	4	-
10	Misrepresentation/Suppression of Fact for Obtaining License etc. (Sec. 71 of IT Act)	12	5	4	-20	14	13	2	-84.6
11	Breach of Confidentiality/Privacy(Sec. 72 of IT Act)	93	16	20	25	30	13	6	-53.8
12	Disclosure of Information in Breach of Lawful Contract@(Sec. 72A of IT Act)	-	2	4	100	-	5	2	-60
13	Publishing/Making Available False Elect. Signature Certificate (Sec. 73 of IT Act)	4	0	3	-	8	0	0	-
14	Create/Publish/Make Available Electronic Signature Certificate for Unlawful Purpose(Sec. 74 of IT Act)	71	3	3	0	51	5	3	-40
15	Others	274	769	514	-33.2	161	520	245	-52.9
Total Offences under IT Act		**4,356**	**7,201**	**8,045**	**11.7**	**2,098**	**4,246**	**5,102**	**20.2**

Figure 6

Source : National Crime record bureau

Number of Cyber Crime Cases in India

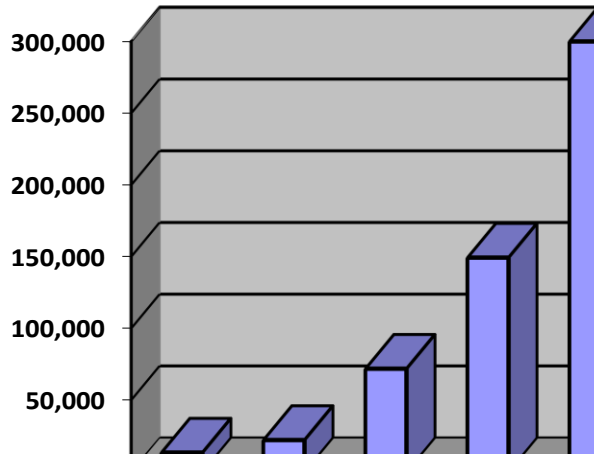

Figure 4

Source: ASSOCHAM-Mahindra SSG Report, Jan 2015

V. CONCLUSION

Software Engineers are expected to produce quality work, which can be improved by technical as well as ethical paradigms. Software Engineer has to make ethical decisions after evaluation of ethical arguments and ethical choices. Methods and tools is required to acknowledge the social context of design. Skipping social context from software engineering can create serious threats to privacy, accuracy, property and accessibility. Unprofessional Software engineering principles, the software design and development practices can lead to failures in terms of a programming bug, software design and specification errors, programming glitches etc., which can be catastrophic leading to the loss of life, triggering wars, disrupting peace and also it can lead to severe financial losses. Indian software industry is growing with young software engineers shaping India to become global leader. Indian government is pushing it further up by its digital India program creating an ecosystem full of technical manpower, elite technical institutes etc. With the tremendous growth of software development in India, there are also serious threats due to lack of ethics and professionalism. India has to take concreate steps to abide by a code of ethics, monitor its practice, get professionalism in its software engineers by redesigning and integrating ethics into curriculum, reform and make better laws and create efficient policies to cut of risks and endure its progress as a global leader.

References

[1] J. Iqbal and B. Maqbool, "*Computer Ethics: Job of Computer Scientist*," Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 7, no. 6, Jun. 2017.

[2] Nidhin Thomas, Atharva Joshi, Rishikesh Misal and Manjula R, "*Data Mining Techniques used in Software Engineering: A Survey*", International Journal of Computer Sciences and Engineering, Vol.4, Issue.3, pp.28-34, 2016.

[3] R. O. Mason, "*Four Ethical Issues of the Information Age*," MIS Q, vol. 10, no. 1, pp. 5–12, Mar. 1986.

[4] Shackelford R, McGettrick A, Sloan R, Topi H, Davies G, Kamali R, Cross J, Impagliazzo J, LeBlanc R, Lunt B., "*Computing curricula 2005: The overview report*", InACM SIGCSE Bulletin, Vol. 38, No. 1, pp. 456-457, 2006.

[5] Weber AM. The Council of Europe's Convention on Cybercrime. Berkeley Technology Law Journal, Vol.18, Issue.1, pp.425-46, 2003.

[6] H. T. Tavani, "*Ethics and technology: controversies, questions, and strategies for ethical computing*", Fourth edition. Hoboken, NJ: Wiley, 2013.

[7] "*September 26th, 1983: The day the world almost died*," Mail Online, 1983.

[8] "*The Man Who Saved the World*," Wikipedia. 09-May-2017.

[9] "*OEC - An Investigation of the Therac-25 Accidents* http://www.onlineethics.org/cms/4661.aspx. [Accessed: 26-Jul-2017].

[10] ColdWarWarriors, HMS Sheffield Hit by Exocet Missile. .

[11] "Loss of sheffield -board of Enquiry." 28-May-1982.

[12] H. Lin, "The Development of Software for Ballistic-missile Defense," Sci Am, vol. 253, no. 6, pp. 46–53, Dec. 1985.

[13] A. Boydston and W. Lewis, "Qualification and reliability of complex electronic rotorcraft systems," in Army Helicopter Society System Engineering Meeting, 2009.
[14] D. 20548 R. N. G.-92-26 Or Publisher: US General Accounting Office, "Patriot Missile Defense: Software Problem Led to System Failure at Dhahran, Saudi Arabia," 1992.
[15] "*ARIANE 5 Failure - Full Report*," Paris, Jul. 1996.
[16] Gleick, "A Bug and a Crash by James Gleick," New York Times Magazine, Dec-1996.
[17] L. Ropolyi, "S*ocial and ethical aspects of the Y2K problem*," in Proceedings of the Fifth International Conference on the Social and Ethical Impacts of Information and Communication Technologies: Ethicomp, 2001, pp. 18–20.
[18] "*Mumbai teen jumps to death, cops suspect links to Blue Whale challenge*,"www.hindustantimes.com/, 31-Jul-2017.
[19] R. Moore, "*Cybercrime: Investigating High-Technology Computer Crime"*, Routledge, 2014.
[20] "The UN, "*Cyberspace and International Peace & Security-Side Event-October 5th – UNODA*." .
[21] "*Latest Aadhaar leak exposes security flaws in app developed by NIC*," hwww.hindustantimes.com/, 17-Aug-2017.
[22] "*Towards sustainable and lasting GrowthANNUAL REPORT 2016-17 Government of India Ministry of Commerce & Industry Department of Commerce*.," 2017.
[23] "*Performance & Contribution towards Exports by IT-ITES Industry | Ministry of Electronics and Information Technology, Government of India*." meity.gov.in/content/performance-contribution-towards-exports-it-ites-industry#tab1. [Accessed: 09-Aug-2017].
[24] "*2016 Global Services Location Index*.", 2016
[25] "*Programme Pillars | Digital India Programme.*" digitalindia.gov.in/content/programme-pillars. [Accessed: 12-Aug-2017].
[26] "*e-Governance – Reforming Government through Technology | Digital India Programme*.", digitalindia.gov.in [Accessed: 12-Aug-2017].
[27] "*eKranti | Digital India Programme.*", digitalindia.gov.in/content/ekranti. [Accessed: 12-Aug-2017].
[28] "*IT for Jobs | Digital India Programme*.", digitalindia.gov.in/content/it-jobs. [Accessed: 14-Aug-2017].
[29] "*Early Harvest Programmes | Digital India Programme.*" http://digitalindia.gov.in/content/early-harvest-programmes. [Accessed: 14-Aug-2017].
[30] K. Sridharan and Saktheeswari, "*A Case Study on Cyber Crime In India*," Int. J. Power Control Signal Comput., vol. 4, no. 2,2013, 2013.

