Digital Security: An Enigma

Avijit Dutta

Abstract The subject security has wide coverage and it is growing with every passing day. As civilization progressed from Agrarian to semi-industrialization, advanced industrialization and finally to present ICT (Information and Communication Technology) age, concerns for security are increasingly taking in all objects from physical to digital. It augmented apprehensions from losing material wealth to most abstract entities like wealth of knowledge in digital form. Today's technology allows wired and wireless access to tangible and intangible resource-built ups (material to digital), digitally, and steal the same if need arises. The riddle is to defend our own resources from the rapacious hand of ubiquitous computing and communicating technology evolved by us. The art and science of hiding and securing precious resources from possible predators in physical or digital forms make it complex and challenging. The enigma remains in the fact that predator uses same technology and at times also makes rule that prevails over others.

Keywords Collective intelligence · IoT (Internet of Things) · Ubiquitous computing · Web square

1 Introduction

Technology integration and its standardization have put civilization on fast track. From 'agrarian' to 'semi-industrialization', 'industrialization', 'advanced industrialization' and finally to 'digital age', the journey so far has been exciting. Innovations across different subject areas cooperate amongst themselves to make ways for new novelty. Weiser [1, 2] may have closely followed advances in computing hardware, system software and programming techniques during 90s to visualize the phenomena of ubiquitous computing, which now is a reality.

A. Dutta (✉)
NIC, New Delhi, India
e-mail: dutta_avijit@yahoo.com

M. U. Bokhari et al. (eds.), *Cyber Security*, Advances in Intelligent Systems and Computing 729, https://doi.org/10.1007/978-981-10-8536-9_25

Broadly, three factors have driven computing technology to ubiquity. First to name is 'Miniaturization', which is a trend to manufacture ever smaller mechanical, optical and electronic products and devices. Second to mention is 'Standardization', which is the process of developing and implementing technical standards that helps to maximize compatibility, interoperability, safety, repeatability or quality. Third to mention is 'Digital Communication', which evolved over packet switch networking technologies, mostly adhering to TCP/IP protocol standards. This allows data exchange between computing devices over wired or wireless network. At the advent of TCP/IP-related protocol like HTTP (Hypertext Transfer Protocol), World Wide Web (WWW) became a reality leading to web 1.0 paradigm, which allowed viewing vast amount of static information on web, advancing data disseminations practices, leading to dot-com era. Initial enthusiasm died down as viewers could not participate in the process, thus followed occurrence of dot-com burst. Web 2.0, which is interactive, revived web and took it to today's state of booming activities where everyone is keen to participate. In exponentially expanding web scenario, the exemplar that may follow web 2.0 is a subject of any one's guess now! To some, it is web 3.0, simply as next version standard, with more advanced technical facilities. For others, it is 'Web Square', the name and concept popularized by Tim O'Reilly and John Battelle. Progression of events allowed Tim O'Reilly, at a later date, to talk about IoT (Internet of Things) and collective intelligence [3]. He, during early years of twenty-first century, could visualize flooding of Internet usages with sensors and devices leading all to an era of nomadic and yet interactive WEB [1, 2, 4–6].

It was expected that the number of such devices would grow exponentially to guide technology to next-generation usages. These sensors and devices singularly termed as IoT are designed to add intelligence to everything from commonplace consumer items, home appliances, private or public utility systems, industrial items, healthcare system, education, agriculture and everything in between, even to railroad ties on big or small deals. 'IoTs' collects and broadcasts data across networks, enabling the data to be analysed on it or remote servers to add values and share. This approach changed the very way life and business processes were hitherto accomplished, leading to an archetype shift from physical to digital course of functioning [7–11].

Technology advances ushered era of first, second, third and fourth generations of computing. During this period, human–computer interactions shifted from 'One Machine many users' to 'One user One Machine' and finally to 'Many Machine Many User' setups. Digital computing stepped out from closed realm of scientists and academicians to arrive at the doorstep of common users. As discussed earlier technology integration, its standardization and digital communication steered us to the era of WWW and Internet. Broadly, evolutionary path of Internet can be viewed as follows—from years 1969 to 1995 it belonged to hardcore technocrats and scientists, from 1995 to 2000 it belonged to geeks, from year 2000 to 2007 it became Internet of masses, from 2007 to 2011 it turned as Internet of mobiles and from 2012 and days beyond it may evolve into the era of IoT. It may be opined that emergence of web 1.0 (static web) occurred during Internet of geeks and web 2.0

(interactive web) exemplar fructified during subsequent years of innovation and continues till date [12, 13].

In this process, our wealth perspective enlarged from physical to digital entities. Amongst all digital devices, smartphones captured imagination of most. Apart from calling facilities, it possesses seeing and listening capabilities embedded in it. With a smartphone, all life processes like socializing, shopping, banking, paying bills, acquiring medical advices, etc. are easily executable. It can also do video and static photography reasonably well. Being GPS enabled, it can collect and disseminate location information effectively. After sequential and object-oriented coding standard, mobile programming is the upcoming programming practice, which offers bigger provision for interactive programming in web 2.0 ages. The entire effort for a paradigm shift is to fulfil a very simple desire, to get and remain connected. But indiscriminate connectivity brings in the risks of security breaches. The brainteaser is to get and remain connected in a secured way. Present text dwells on this riddle and attempts to hold a collective view of entire scenario in the following section.

2 Collective Intelligence

The concept of data and the process of its collection, collation and dissemination have changed largely in the era of web 2.0 [7, 8]. Today, apart from texts, digits, audio and video, photographs too are taken to mean as data. Keyboard now is not the only means for data incorporation, interpretation and interaction with digital objects and Internet. Omnipresent smart devices can look, feel, sense, photograph objects and store them within a split second instruction at any desired location, really smartly [3, 6].

Technology miniaturization, standardization and large-scale product manufacture are bringing down the cost of computing and communicating. This has helped a wide range of computing and communicating devices in terms of size and performance like servers, desktop, laptop, palmtop, smartphones, wearable devices, etc. to be available in the market. These devices are also armed with seeing, listening, recording and storing capabilities, which cater to extensive range of data processing and disbursing needs, helping to bring most on board. These devices with an identity can be linked amongst themselves and numerous other small or large smart digital devices, termed singularly as IoT, as discussed earlier, over varied choices of connectivity options like broadband, Wi-Fi, R/F, Bluetooth, etc. [14, 15].

The depiction in Fig. 1 (IoT Scenario) attempts to present a window view of the situation arising out of the increasing presence of IoTs. This helped to enhance the mass base of smart devices usages. Digital devices are capable now to communicate intelligently amongst themselves and others in forms like M2M (Machine to Machine), M2I (Machine to Infrastructure) and M2E (Machine to Environment) in real time, process data at nodes or cloud deciding almost autonomously and present the most up-to-date information to us so that we can make the best decisions.

Benson Tao observes that present efforts towards building smart, connected, autonomous and contextually aware devices around the IoTs will prove to be catalyst for a change, leading to general betterment. As it turns out, IoT is a very broad concept, which includes all kind of wearable, carriable, attachable and implantable and everything in between devices that associates with us in our daily coir.

Interestingly, O'Reilly [3] envisaged today's Internet as a new born kid, who looks, touches and feels about the things around with the help of various sensors (being carried by us), like mobile phones and smart devices, to gather data in audio, video and text form and processes them to attain a higher state of awareness. It is increasingly getting intelligent with information gathered by sensors ubiquitously strewn around, in both static and mobile state and maturing incrementally like any living objects, though as a virtual entity. In return, it shares the collected data, information and knowledge whenever these are asked for, inform of an organized query, over digital network, establishing the concept of collective intelligence. Worldwide efforts are on to bring most on board, to enrich the process of collective intelligence and get maximum benefit out of it. Well, there is dark side of this process too, which is being discussed in following segments.

3 Emerging Challenges

In keeping with Mark Weiser's view of 'ubiquitous computing' concepts, one may find that Computing and Communicating (C&C) emerged as profound technology in this era, which has associated with our day-to-day life processes inseparably and continuing expansion process of its presence exponentially with smart devices termed as IoTs [1–3]. These phenomena are making fast inroads in our daily

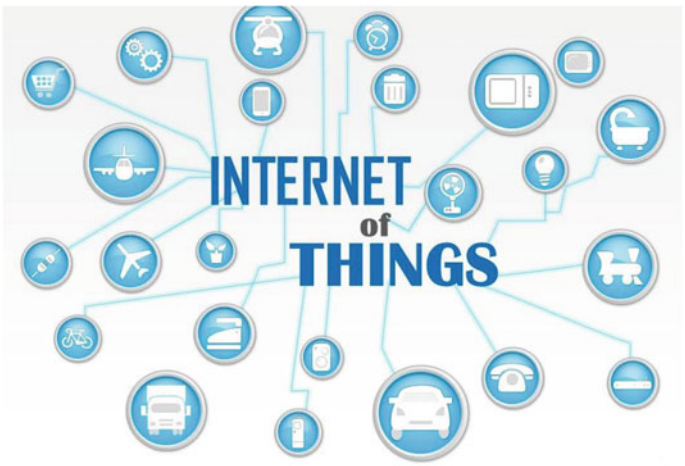

Fig. 1 IoT scenario

activities. Broadband routers offer Internet access to devices through Wi-Fi and Ethernet connections to make today's home network. Appliances like laptops, desktop computers and mobile devices, such as phones and tablets can get onto Internet through broadband router. With the IoTs finding their ways into the homes, innumerable new devices are produced that can connect to the same network. These devices are of two types; the first ones get connected through formal networking technologies as discussed earlier. Others may use different wireless technologies that suite device needs, conforming to lower energy consumption or ad hoc network coverage protocols. Nevertheless, everything is connected to the local network and can communicate freely with one another. Connections to the Internet are directed through a central router, which may (or may not) always contain basic firewall filtering functionality [9–11].

It may be known that connected version of different devices, participating in day-to-day activities, gets onto same network without essential security consideration. Despite increasing acceptance of IoTs, no standards have been planned so far for the use of these innumerable devices and sensors. They are almost on their own in the process of establishing connection, exchanging and processing information on instruction from numerous lawful or unlawful owners. Along with many goodies that computing ubiquity presents, the offered challenges lie in the fact that the 'IoT' today is an abstract collection of uses and products without common agreement or disagreement on mode of functioning. So, everyone does it their own way, often poorly, compromising security of connected devices as it greatly lacks an established concept of implementation and use. A study of security major like Symantec Corporation seems to have found that currently there is no single standard protocol in IoT and 'security' is not a word that gets strongly associated with this category of devices, leaving its consumers potentially exposed [9–11]. The 'enigma one' lies in the fact that these challenges are our own creation and we are forced to face them.

As information highway is being accessed by one and all, gradually concerns are gaining ground about the co-travellers with whom this highway is being shared! Symantec, after analysing 50 home devices, during year 2014, has observed that none of the devices used strong password, enforced mutual authentication practices or applied defence mechanism against brute-force attacks [10, 11]. It also has found mobile apps generally do not use Secure Sockets Layer (SSL) to encrypt communications to the cloud. The family of IoT devices possesses vulnerabilities, which are much in common. Potential weaknesses in authentication and traffic encryption could badly affect IoT systems. These facts though well known to the security industry, mitigation processes are not taken good care off.

It is generally felt that IoT vendors need to do more on security before marketing their product universally, leaving millions of people at risk of cyberattacks. This leads a feeling that 'IoT security is still a pipe dream' [9–11, 15]. The 'Enigma Second' lies in the fact that IoTs are being produced in large numbers with comprehensive knowledge about associated security hazards.

The digital security challenge mitigation begins with stopping innumerable entities approaching digital resources over data communication network, to verify their credentials and allowing passage, if found acceptable, denying it otherwise.

The process gets multifaceted as advancing objects grows in number and form, which taxes time and computing resources of approached entity. More often than not objects seeking access to resources are large, interactive and at times deceptive. Objects approaching resources constantly change form and advancing tactics to match the defence mechanism with the intent to crack the same. Real-time detection of specifics on attack vector is difficult and this leads to security breach. Authentication and authorization become important at such instances. Digital resources can be protected with cryptographic techniques and establishment of PKI (Public Key Cryptographic Infrastructure) system. Steganographic techniques allowing enveloped exchange of document also come handy for secured data exchange. Cryptography and steganography putting together can provide robust defence mechanism against predators during digital document exchange. Enigma Third' lies in the fact that for the defence of our ever evolving resources, eternally new mechanism needs to be explored. In the following section, collective effect of enigmas around 'Digital Security' is further discussed.

4 Enigma

Collectively, the digital security enigma lies in the fact that we are defensive against our own creation and in a way we are creating our own space for both security and insecurity. Adding to woes are the facts that lessons on computer hacking are included officially in course curriculum of many national and international universities. Today, the attacker and defender use same or equivalent technologies and at times they appear like either side of the same coin. Like for cryptography there is cryptanalysis, for steganography there is steganalysis and so on. Moving on one may even find that the perception of cybercrime is relative to geographical or political jurisdiction. The inherent view that hacking others network is fair, getting hacked is not, is scaring [8].

Financial sites of many institutions and well-offs are recurrently hacked by less fortunate for instant monetary gains using advanced C&C technologies. Scientific and Defence research sites of many advanced countries are being routinely intruded these days for a fast track course to new knowledge, while gainers appreciate the act, losers strongly denounce it. This has compelled many original equipment manufacturing countries to embed cyber sniffing tools, in both hardware and software systems, which are difficult to shake off, so as to pre-empt movement of cyber predators [9–11]. It ensures (!) security breach even with best defence mechanism up front as the attack can be initiated from either side of the system.

Fact remains that resourceful and militarily powerful countries cyber-snoops friends and foes including close allies, all alike. IoTs have made the process even simpler. These devices have made even our residential places vulnerable. Gartner research predicts that there will be more than 2.9 billion connected IoT devices in consumer smart home environments in 2015. These connected devices could provide a much larger surface for attackers to target home networks. IoTs are wearable,

Table 1 Scope for security lapses

1	Insufficient authentication/authorization	6	Insecure cloud interface
2	Insecure web interface	7	Insecure mobile interface
3	Insecure network services	8	Insufficient security configurability
4	Lack of transport encryption	9	Insecure software/firmware
5	Privacy concerns	10	Poor physical security

implantable, transferable and easily accessible, turning away complex defence technicalities. So these objects can be accessed and used by both predators and defenders with reasonable ease [10, 11].

It has been observed that most IoTs have very weak password management. This apart from some of these devices which are without keyboard, passwords are managed remotely. More often than not users continue to use default password making them vulnerable to cyberattack.

Proof of concept for most IoT attacks already exists, like remotely accessing onboard computer of an aircraft to alter scheduled flying course, a home network for permanent anchoring and to create unwarranted surprises, a pacemaker to affect health of person and the count goes on. Possibilities to derive financial objectives from such attacks are not very remote. Symantec list of Top Ten IoT Vulnerabilities is indicated by Open Web Application Security Project's (OWASP), which sums up most of the concerns and attack vectors surrounding this category of devices. These are given in Table 1 [8, 10, 11].

Enigma remains in the fact that at this backdrop demands for secured access to Internet, its usages are encouraged and number of people accessing digital network is growing with every passing day. To encourage it, further issues related to net neutrality is debated. Institutions controlling critical business operations are increasingly encouraging access to its functionalities over digital network shunning personal presence and activities in their premises. As Internet opens up rapidly to make more resources accessible, concerns grow for identifying the intention of the objects approaching resources. The paradigm shift makes life processes simple, though at times at the cost of individual and collective security, creating a dichotomy between security and accessibility that leads to a puzzle.

5 Analysis

The journey over Internet for knowledge and wisdom at this moment is open to all, which is expected to lead humanity to freedom from dogma, biases, short-sightedness, etc., the factors that slow down the process to become a superior entity. Plethora of web applications and mobile apps are being developed to ease the use of Internet; wherein, required technical knowledge of computing and communicating are minimal. Of late it is being observed that this freedom is being

Table 2 Cyber safety equation

Cyber safety	=	Cybersecurity/cyber insecurity
where		$0 \leq$ Security $\leq \infty$; $0 \leq$ Insecurity $\leq \infty$

used differently by a different stratum of humanity. The rulers, ruled, privileged, marginalized, scientists, technocrats, statesman, bureaucrats, etc., on right or wrong side of righteousness are using the priceless resource in line with their own agenda. As it is being deliberated that both 'security' and 'insecurity' scenarios are our own creation and since International Telecommunication Union (ITU) is producing measures of security one more measure 'Cyber Safety' may find place in present text in the following way (Table 2).

As strategic retreat, instead of attempting for an absolute secured environment in this milieu, effort could be made to make it safe, where security be more prevalent than insecurity. Increased security will enhance safety, and increased insecurity will reduce it. This is indicative of the fact that far from being deterministic, safety and security factors get probabilistic as technology advances in time, allowing **enigma** to seeps in. This in turn compels one to conceive a model on safety, leaving aside the path for absolute considerations. The analysis in this context follows next.

Deliberations so far underline the fact that advances in technology expected to associate increasingly more factors, both technical and non-technical, affecting digital safety and security, which may spice up existing enigma. Amongst these factors, data or digital communication expected to play a dominating role now and in near future as escalating indiscriminate digital connectivity presumed to dilute security considerations. Since computer network connects all and sundry across the globe, it will be quite interesting to assess broadly the association between 'Network Readiness' and 'Cybersecurity Preparedness Index'. Though both are abstract terms, in our journey to isolate factors affecting safety and security aspects the most, this text expected to open a small window view of challenges ahead.

ITU has produced security index as GCI (Global Cybersecurity Index) and cyber wellness measures for the year 2014. Global Information Technology Report (GITR) also has produced network readiness index for the same year. These are shown in 'Table 3' below in column **'A' and 'B'**. The analysis is done with limited scope presently, considering '**Network Readiness Index**' of top ten countries and their associated '**Cybersecurity Index**' as presented in **Table** 3. Values listed under column 'B' calculated to 10-point scale and listed under column **'B10'** to bring it at par with values listed under column **'A'** for comparison. The calculated value of **Correlation Coefficient** between these two parameters is presented next.

Correlation Coefficient: 0.9994697150416415. This indicates that there is high correlation between network readiness index and cybersecurity preparedness index. Thus, at this moment, to begin with, 'Network Readiness' may get maximum attention to be secured. It may be presumed that an enigmatic component has been identified.

Table 3 Network readiness and cyber security status of top 10 countries in the world

S. No.	Country Name	GITR Network Readiness Index (A)	ITU Cybersecurity Preparedness Index (B)	ITU Cybersecurity Preparedness Index on 10 Point Scale (B10)
1	Finland	6.04	0.618	6.18
2	Singapore	5.97	0.676	6.76
3	Sweden	5.93	0.647	6.47
4	Netherland	5.79	0.676	6.76
5	Norway	5.70	0.735	7.35
6	Switzerland	5.62	0.353	3.53
7	United States	5.61	0.824	8.24
8	Hong Kong SAR	5.60	0.618	6.18
9	United Kingdom	5.54	0.706	7.06
10	Korea Rep	5.54	0.706	7.06

Source [16, 17]

6 Conclusion

With a limited scope, deliberations so far have indicated that there is high correlation between 'Network Readiness Index' and 'Cybersecurity Preparedness Index'. Though absolute security is not achievable in today's scenario, mainly because of the fact that same technology and related standards are being used by both attackers and defenders, remaining oblivion to security issue may be catastrophic. Digital networks have been opening up precious resources to one and all at the backdrop of the debate on 'Net Neutrality'; thus, combinations of security options, with focus on digital network, may help in making a strong security module to enhance safety.

7 Future Scope

It has just been conceived that 'Digital Security' aspect increasingly getting probabilistic and security model needs to be evolved to control '**Enigma'** with an aim to establish enhanced safety. In this context, data from more countries needs to be included to make the study further accurate. Apart from factors like 'Network Readiness', associations of other factors like country-wise Knowledge Index (KI), knowledge economy index, ICT index, etc. with cybersecurity preparedness index, may be explored individually and collectively to evolve a reliable security/safety model that assures safe network usages.

Acknowledgements Contributions of theorists who can look into the future and guide science and technologies beyond horizon are deeply acknowledged.

References

1. Weiser M (1991) The computer for the 21st century. Scientific American, Sept 1991, pp 94–104
2. Weiser M, Brown JS (1996) The coming age of calm technology. Xerox PARC, 5 Oct 1996
3. O'Reilly T, Battelle J. Web squared: web 2.0 five years on; special report
4. Kleinrock L. Nomadic computing—an opportunity CCR 4/95
5. Burgin M, Eberbach E (2012) Evolutionary computation and the processes of life. ACM Publication
6. La Porta TF, Sabnani KK, Gitlin RD. Challenges for nomadic computing: mobility management and wireless communications. Bell Laboratories
7. Avijit D. Knowledge ubiquity in web 2.0 paradigm. Innovation in information system and technology. ITCDC '09 Macmillan Publications, pp 234–238
8. Avijit D. Digital security: a moving target. Int J Electr Electron Comput Sci Eng. Special issue —TeLMISR 2015. ISSN: 2348-2273
9. Barcena MB, Wueest C (2015) Insecurity in the Internet of Things. Symantec, security response, version 1.0, 12 March 2015
10. Symantec, ISTR, April 2015, vol 20
11. Symantec, Insecurity in Internet of Things, version 1.0, 12 March 2015
12. Cortada JW, Marc GAMLN How nations thrive in the information age. IBM Institute for Business Value, IBM Global Business Services
13. Kephart JO, Chess DM (2003) Autonomic computing. IBM Thomas J. Watson Research Center, IEEE Computer Society
14. https://bensontao.wordpress.com/2013/10/06/vivante-internet-of-things
15. http://securityaffairs.co/wordpress/34974/cyber-crime/iot-security-symantec.htm
16. INSEAD (2014) Global information technology report
17. ITU (2015) Global cyber security index & cyberwellness profile report
18. Lytinen K, Yoo Y. The next wave of nomadic computing: a research agenda for information systems research. Working papers on information systems, Sprouts. ISSN: 1535-6078
19. Cousins KC, Robey D. Human agency in a wireless world: patterns of technology use in nomadic computing environments. Information and Organization; Science Direct
20. Venkatasubramanian K, Gupta SKS (2006) Security solutions for pervasive healthcare. P1: Binaya Dash, 8 Dec 2006, vol 11:58, pp AU7921–AU7921˙C015
21. Kleinrock L. Nomadic computing. Computer Science Department, Los Angeles
22. Davis RM. Evolution of computers and computing. Science 195
23. Satyanarayanan M. Pervasive computing: vision and challenges. School of Computer Science, Carnegie Mellon University
24. TechTarget, Security Media Group. Information security, October 2014, vol 16, no 8
25. http://www.slideshare.net/MhaeLyn/iot-30545508

Author Biography

Avijit Dutta is an M.Sc. (Statistics), M.Phil. (Applied Mathematics/Statistics), and MBA (Finance and Marketing) graduate. He is associated with ICT for the last 34 years. During this period, he served both private and government institutions at various capacities in different projects. He retired from National Informatics Centre (NIC), New Delhi, Government of India (http://www.nic.in), as Scientist "F"/"Senior Technical Director" on December 31, 2018, after rendering 31 years and 2 months of coveted service. He continues to enjoy ICT thereafter on personal capacity.