ISSN- 2350-0530(O), ISSN- 2394-3629(P)
Index Copernicus Value (ICV 2018): 86.20
DOI: https://doi.org/10.29121/granthaalayah.v7.i12.2019.294

INTERNATIONAL JOURNAL OF RESEARCH – GRANTHAALAYAH
A knowledge Repository

Science

IN SEARCH FOR CYBER DEPENDENCE

Avijit Dutta [*1]
[*1] Ex - Scientist F NIC New Delhi, India

Abstract

Civilization progressed through phases like agrarian, semi-industrialization, industrialization, advanced-industrialization and arrived at Information age. Advances in ICT (Information and Communication Technology) transformed most revered ancient concept of 'Knowledge' from abstract to measurable form with considerable economic value. Produces of knowledge exercise, in form of data, analyses and documents etc., are being digitized increasingly and stored on servers across the globe building large knowledge warehouses [1,2,3]. Some of these are shared and rests are protected. Material value of these possessions are enormous and immensely attracts attention of cyber predators, armed with aggressive ICT tools and techniques. Cyber predators can now harm both material and digital possessions with digital tools. Thus, human possessions in either form; physical and digital, demands to be defended digitally and an environment of cyber dependence needs to be established. The scope of deliberation is vast though an attempt has been made to present a kaleidoscope of the issues that deserve attention [4,5,6].

Keywords: ICT; IoT; SCADA; TCP/IP.

Cite This Article: Avijit Dutta. (2019). "IN SEARCH FOR CYBER DEPENDENCE." *International Journal of Research - Granthaalayah*, 7(12), 1-11. https://doi.org/10.29121/granthaalayah.v7.i12.2019.294.

1. Introduction

Democratization of Internet, predominantly with commercial objective, is extending its mass base at the cost of digital security measures. It is an opportunity for predators and threat for unassuming users. Present technology enables predators to gain access to physical and digital assets remotely with equal ease of fair users, using most commonly available handheld devices, say a mobile phone, which has incredible usability and gaining ubiquity status with each passing day adding to digital security risks too.

Growing flexibility to access internet, increased traffic over it. Digital wealth-houses, build across the world, are accessible to predator, defender and genuine users all alike by virtue of technologies available to one and all over internet. Nonetheless, in this set-up a balance between in and out flow of information resources needs to be established so that the painstakingly developed resource tank

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
Index Copernicus Value (ICV 2018): 86.20
DOI: 10.5281/zenodo.3595242

is not deflated completely, ever. In this text the term 'Cyber Dependence' is proposed which is related to both digital security and insecurity. Cyber dependence increases with 'Security' assurance and decreases otherwise. It may be realized that while in present scenario absolute security is not attainable and total insecurity too is not desirable which may lead to chaos. While best attempts are made by cyber/internet service providers to secure the environment sources of insecurities too are many. For stability a balance between these factors; 'security' and 'insecurity' is desirable. Cyber Dependence is proportional to this balance, which relates both security and insecurity [6,7,8].

As user participations increases, it is being realized that security consideration, in addition to micro level features involving hardware and software system configurations, consideration on macro factors like literacy rate, state of awareness, governance, cyber administration etc. are also needed, which generally reflect on of individual and societal quality engaged in the usages of the cyber system.

2. Methodology

Cyber Security issues has arrived at critical stage in present days. Frequent cyber-attacks with devastating affect touched physical and material wealth, both at individual and institutional level are not few and far between. Situation has arrived where one has to be quite careful and decisive whether to remain on or offline at a point of time with cyber world. Generally, it is advised to log-in strictly following security advices and log-off from digital resources immediately after use to avoid predator's detection and attack. It has become necessary to take precaution at different action points in the process of cyber interaction to detect and prevent intrusion to enhance trust and cyber dependence.

Present text attempts to reflect on facts like transformation of resources to digital form, evolution of ICT to nomadic and ubiquitous state leading to mass participation that eased the way of life though, infused associated risk resulting in possibility for intellectual and material losses. The text also explores necessary way out for prevention to scale down losses and finally explores association between various macro measures, available globally, to attempt a relationship between Cyber Security and Dependence.

3. Digital Resources

It is important to note at this stage that engagement and use of resource perception is shifting from physical to digital form with varying risks, which brings in digital security issue on the center stage along with physical one [6,7]. Standardization of ICT and Knowledge exercises allowed technologies of different domains to converge, leading to present information age, wherein IoTs occupies center stage. Progression of computing and communicating technology advanced through first to fourth generation and continuing its march to fifth generation model, involving artificial intelligence notion. This brought changes in designing and coding patterns from sequential to object-oriented methods. On the other hand, as data communication technique improved, TCP/IP based internet technology gained popularity leading to Web1.0 and Web2.0 paradigm, which may lead to Web 3.0 or Web Squared in future, as envisaged by Tim O'Reilly and John Battelle [8,18].

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
Index Copernicus Value (ICV 2018): 86.20
DOI: 10.5281/zenodo.3595242

The process, as discussed, enhanced human-computer relation from one-to-many (Mainframe System) to many-to-many (IoT System) affiliation, where many clients talk to many servers and vice versa over internet simultaneously. This ushered ubiquitous computing concept as visualized by Mark D. Weiser, scientist at Xerox PARC in the United States. He is widely considered to be the father of 'ubiquitous computing', the term he coined in 1988 and deliberated about the same in his seminal paper 'The Computer for the 21st Century'. In his paper he went on to elaborate how ICT would be evolving as a profound technology, weaving itself into our day-to-day life inseparably, smearing its own distinct existence, progressively [20,21]. World experienced this progression in reality, leading to the age of sensors. Technology advances, its miniaturization, standardization and integration evolved tiny computing devices which senses all sorts of changes in their environment, like location, temperature, pressure, movement, frequency etc. This allowed them to find their places in all kind of engineering, medical and general utility devices, making them digitally controlled. These devices collectively come under banner 'Internet of Things', IoTs. Though these devises eased life complexity in many ways, their remote accessibility over digital network exposes them to security risks. Researchers have shown implanted medical devices, devices on automobiles, home appliances and even digital components of aircraft can be accessed from external devices with adverse notion [14,15,16].

4. ICT Ubiquity Through IOT

ICT evolution, necessitates its application base be enlarged to make the process financially viable. This requires abstraction and encapsulation of technicalities as complex detailing beyond a point to a user makes a product unpopular. Progression of Digital Computation and Communication ushered era of World Wide Web (WWW) and INTERNET. This led to Web 1.0 (static web), which popularized computing and communicating technology to some extent though failed to sustain it long, leading to dotcom burst as general populous had very little chance to participate interactively with the process.

Technical exercises attending the issues related to failure of Web 1.0 led to Web 2.0, which is present form of participative web activities that enjoys wide acceptability [7,8]. This web application form has become extensively popular as it provides scope for wide range of user interactions having various problem-solving abilities. An end user with minimum technical understanding can enjoy today's computing prowess with tiny, mobile yet power packed devices, in various forms, so much so that ICT attained a state of ubiquity. These computing systems occurs in different shapes, sizes and processing capabilities, generally identified as IoTs "Internet of Things", which forms backbone of today's Computing System [2,11,13,14,18].

The process of technology encapsulation and abstraction simplified its use leading to mass adoption as one need not to know much about the background technical grinds. Today's handheld smart mobile phone, an instance of class IoT, showcases the scenario in perfect frame, where in, technology related to telephony, photography videography, messaging, data processing, reporting and everything in between, are integrated, so much so that it almost replaced the need for Personal Computers, Laptops, Camera, Audio-Video Recorder, Pager etc. It is envisaged Smart Phones may integrate more device utilities in future to make individual existence of those devices redundant. Evolutionary path of Computing and INTERNET, from years 1969 to 1995, belonged to hard core technocrats and scientists, from 1995 to 2000 it belonged to technical geeks, from year 2000 to

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
Index Copernicus Value (ICV 2018): 86.20
DOI: 10.5281/zenodo.3595242

2007 it became tools of masses, from 2007 to 2011 it moved to domain of mobiles, from 2012 and days beyond it may progress into the era of Internet of Thing (IoT) [14,15,16].
Mark Weiser, in his seminal paper talked about ubiquitous computing concept and profound technologies, that assimilate with our day-to-day activities in an inseparable way [20,21]. These technologies mostly work on the strength of data communication, storage and retrieval mechanism which are provided through severs (web and database), located at geographically distributed places which are connected amongst themselves and client systems (IoTs) with communication network of different technology options (broadband, wi-fi, Bluetooth etc.) having different protocol standards. However, the process of abstraction and encapsulation of technologies keeps users off from inherent technicalities comfort and ease of use. Today's Smart Phones present a case in point which meet almost every digital need of a common man without much knowledge of computing. The process democratized internet and associated technologies in a way that anybody in possession with a smart phone having valid connectivity through an ISP (Internet Service Provider), can latch onto internet to link anything or anyone anywhere in the world [10,11,13,19].

5. Collective Intelligence

Tim O'Reilly and John Battelle envisioned exponential growth of IoT and internet users and talked about collective intelligence that may develop out of knowledge exercise getting executed over internet platform. In this setup present internet sphere is envisioned as a budding virtual entity, embryonic like a new born baby, continuously maturing with viewing, sensing and processing the accumulated knowledge to attain wisdom and intelligence. Innumerable devices and cameras carried by IoT users, works as sensory organs of the stated virtual entity [11,15,16,18].

However, it needs to be considered that not all join the internet bandwagon with pure intention. In other words, not all its organs are engaged in noble act of pure knowledge creation. The wrong doers with an intention to disrupt the most precious system possessed by humanity, at this moment, the INTERNET, raises the obvious question 'Who is on the other side of the wire?". More associated concerns in this context, gain ground, since virtual possession of Knowledge asset has a black market. This makes us to take measures beyond pure technical alternatives, which works with mathematical precision.

It cannot be denied that the human understanding, attitude and penchant for wrong doing failed the established system time and again. Edward Snowden's episode established this fact. He was an American Computer Professional, CIA employee and contractor for US government, gained access to classified information inappropriately and leaked it to storm the world with debate on security issues. However, with this incident (leak) people across the world could know about various surveillance programs planned behind the scene. This may make one to believe that anyone, whosoever is connected to internet stands vulnerable to cyber-attack. As most security issues are connectivity driven a very brief description of digital communication system is presented in the following segment to provide further insight [11,12,19].

6. Internet and Data Connectivity

Data communication over digital network/internet can be explained through OSI or with TCP/IP model. OSI is outcome of standardization effort of International Organization for Standardization

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
Index Copernicus Value (ICV 2018): 86.20
DOI: 10.5281/zenodo.3595242

(ISO) and erstwhile International Telegraph and Telephone Consultative Committee (CCIT/CCITT), during 1970s. Later in 1980s their individual efforts were merged and published by ISO as 'ISO 7498' and by CCITT as 'X.200'. CCITT is now the Telecommunications Standardization Sector of the International Telecommunication Union (ITU-T). The Open Systems Interconnection (OSI) model is a conceptual model that characterizes and standardizes the communication functions of a telecommunication or computing system without reference to its underlying internal structure and technology. It conceives seven layers as depicted of activities in data communication.

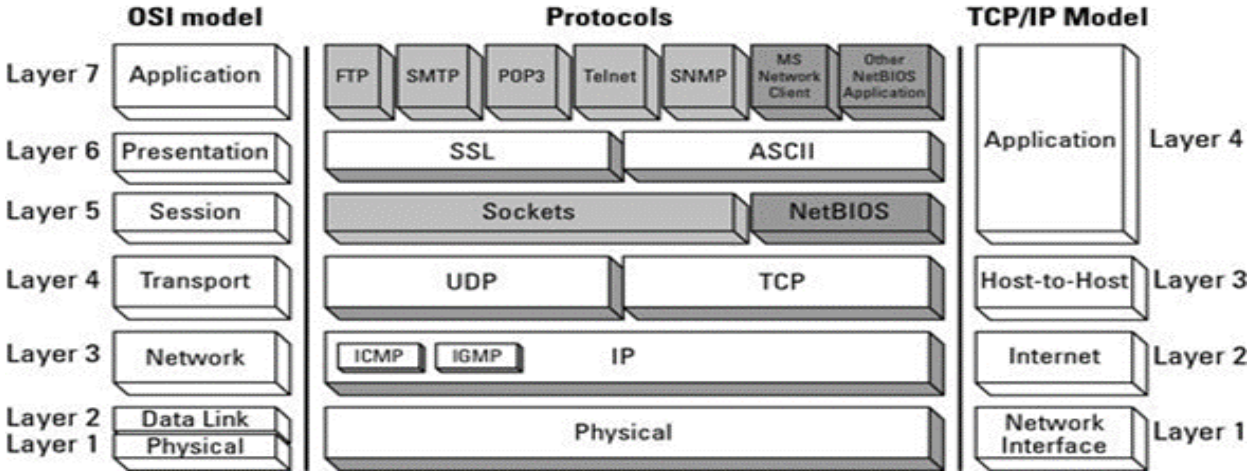

Figure 1:

The research branch of the U.S. Department of defense, Defense Advanced Research Projects Agency (DARPA), created the TCP/IP model in the 1970s for use in Advanced Research Projects Agency Network (ARPANET), a wide area packet switching network that preceded today's internet and continued to be foundation stone of data communication network. TCP/IP was originally designed for the Unix operating system, and subsequently it integrated with all operating systems that came after it. It conceives four action layers [23].

The two main protocols in the internet protocol suite serves specific functions. TCP (Transmission Control Protocol) defines how applications can create channels of communication across a network. It also manages how a message is assembled into smaller packets and then transmitted over the internet and reassembled in the right order at the destination address where IP (Internet Protocol) defines how to address and route each packet to make sure it reaches the right destination. Each gateway computer on the network checks this IP address to determine where to forward the message.

A broad comparison of OSI and TCP/IP model is attempted in Fig -1. It may be mentioned here that a cellular network or mobile network, which is network for today's IoTs, is a communication network, where the last link is wireless. The network is distributed over land areas called cells; each cell is served by at least one fixed-location transceiver. These base stations provide the cell with the network coverage which can be used for transmission of voice, data, and other types of content. [13,19,23]. It may be indicated here that cyber security risks exist in each layer.

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
Index Copernicus Value (ICV 2018): 86.20
DOI: 10.5281/zenodo.3595242

Today's computing paradigm works in three tire architectures having client, web and data sources at each tire as depicted in Fig-2. The data exchange between these tires if mapped on OSI or TCP/IP model, one may visualize technically the scope for security lapses exists at each layer of every objects in three tire architecture; client, web and data source. Technicalities apart it may be expected that security risk also emanates from the way systems at these layers are used or abused or misused. Assessing reasons behind pure technical flaws are easier to detect and rectify than those that arises out of human errors/activities, some of which may be obsessive.

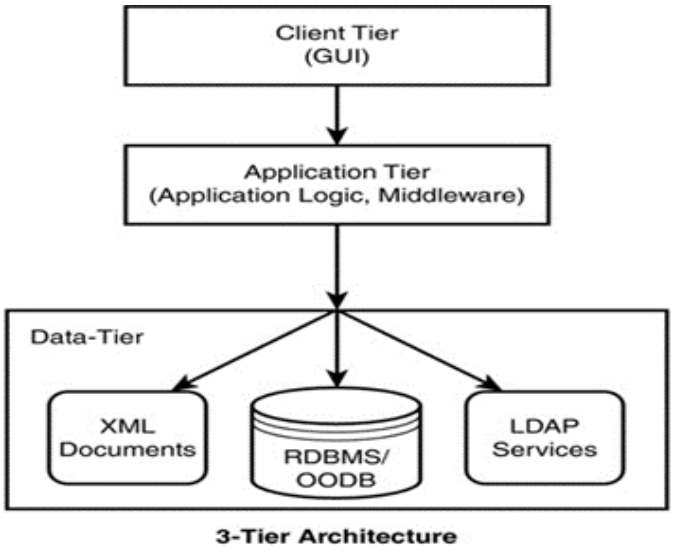

Figure: 2

Moving out of pure science and technology realm ICT made inroads in academic, medical, commercial and industrial processes. This includes industrial and infrastructure courses like power transmission, civil defense, communications, banking, space systems, transportation etc. Some of these operations are managed at facilities that are functional 24×7 mode; any disruption in there can impact human life, economy even national security. Impact of security lapses are there too in case of interconnected device distributed over wide geographical area. SCADA (Supervisory control and data acquisition) systems in this context may be taken as the case in point. SCADA, is a system of software and hardware elements that allows industries to gather and process real-time data for system administration locally or at remote locations over digital network. Like ICT, SCADA also has evolved through generations. As ICT progresses through generations so has SCADA system. It evolved through four generations and increasingly getting more and more stable over time. Earlier discussions on cyber-attack on individual or institution would have restricted affects, however attack on SCADA system can halt grind of activities in for a nation or group of nations. The risk getting real with globalization of ICT, wherein overseas participation comes in regular course [6,7].

7. Sources of Insecurity

As human computer relation shifted from one-to-many (One Computer Many User – Mainframe System) to a complex many-to-many scenario (IoT system), security contemplations too shifted from simple to complex considerations. In earlier sections attempt was made to provide a window

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
Index Copernicus Value (ICV 2018): 86.20
DOI: 10.5281/zenodo.3595242

view on digital security issues. To summaries it may be observed that apart from hardware, software, network connectivity etc. human elements active behind the machine can also become sources of insecurity. Examples are not few and far between where individuals in want of fame and fortune shared classified system information under their control, breaking standard and norms leading to large security breach. In the followings avenues of security risks are broadly elaborated.

First, technology dependence, that brings in weakness in dealing with it and associated security issues. It is learned that to deal with cyber espionage snooping software are being hardcoded in the computing and communicating system by original equipment manufacturers (OEM) under instructions from competent authority for surveillance. Mobile users may have noted that curtain apps during installations seeks permission for internal access, and if not provided, suspends installation. Few multinational TV manufacturers implants software in TV components to gather information on user's choice of channel selection to say the least, actual objectives those run behind the curtain are difficult to assess. There could be no assurance how a TV works in case it is installed at the residence of a person who is prominent in national level affairs. Such examples are many and may be associated with most IoT devices people use. This makes more ICT original hardware and software producing countries less vulnerable to cyber predators. Innovative drive in the areas concerning ICT may provide suitable answer [6,7,8].

Second, laxity in maintaining SCADA system in terms of upgradation, integration and maintenance may provide leeway to cyber predators for attack which may lead to a national disaster. Any individual or institution having access to SCADA system of a country can hold the country at ransom or affect its social fabric adversely to a great extent.

Third, in any region governance weak in cyber administration offers a happy playing field to cyber predators. Able ICT governance is the key for cyber defense in such scenario.

Fourth, last but not the least, human factors which encapsulates vices like greed, disloyalty, insincerity, opportunism, inappropriate lust for fame and wealth, resulting in breach of trust at the cost of insecurity to institution. Instances for men failing machine are many. In this context appropriate human quality in terms literacy and awareness provides solution. Right kind of people behind the machine produces desired result.

8. Open Web Application Security Project (OWASP)

At this juncture, when most applications are web based as discussed earlier, reference to OWASP becomes evocative. OWASP seeks to educate developers, designers, architects and business owners about the risks associated with the most common Web application security vulnerabilities. OWASP, which supports both open source and commercial security products, has become known as a forum in which information technology professionals can network and build expertise. The organization publishes a popular Top Ten list that explains the most dangerous Web application security flaws and provides recommendations for dealing with those flaws. The OWASP Top 10 Web Application Security Risks broadly depicted below-

1) Injection Flaws like CRLF, LDAP, SQL etc. occurs when an attacker sends untrusted data to an interpreter and that is executed without authentication.

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
Index Copernicus Value (ICV 2018): 86.20
DOI: 10.5281/zenodo.3595242

2) Broken Authentication results out of inaccurately configured user and session authentication, this allows predators to take control of keys, password or session token. Multifactor Authentication helps to prevent risk arising out of such scenario.
3) Sensitive Data Exposure occurs when Applications and API s do not protect data like financial information, username, password etc. allowing attackers too see them steal and commit fraud with users. Data Encryption is the way out from such problems.
4) XML External Entity issues occurs with poorly configured XML processors evaluate external entity references within XML documents. Attackers can use external entities for attacks including remote code execution, and to disclose internal files and SMB file shares. Static Application Security Testing (SAST) can discover this issue by inspecting dependencies and configuration.
5) Broken Access Control issues occur due to improperly configured or missing restrictions on authenticated users, allowing them to access unauthorized functionality or data, such as accessing other users' accounts, viewing sensitive documents, and modifying data and access rights. Penetration testing is essential for detecting unauthorized access controls, other testing methods only detect where access controls are missing.
6) Security Misconfiguration risk refers to improper implementation of controls intended to keep application data safe, such as misconfiguration of security headers, error messages containing sensitive information (information leakage), and not patching or upgrading systems, frameworks, and components. Dynamic Application Security Testing (DAST) can detect misconfigurations, such as leaky APIs.
7) Cross-Site Scripting (XSS) flaws give attackers the capability to inject client-side scripts into the application, for example, to redirect users to malicious websites.
8) Insecure deserialization flaws can enable an attacker to execute code in the application remotely, tamper or delete serialized (written to disk) objects, conduct injection attacks, and elevate privileges.
9) Developers at times may use components with known vulnerabilities which may give attackers chance to invade
10) Insufficient logging and ineffective integration with security response system allows invaders to attack and prolong threat scenario for longer time.

OWASP tools, document and code library projects are organized into three categories, tools and documents that can be used to find security-related design and implementation flaws, tools and documents that can be used to guard against security-related design and implementation flaws and tools and documents that can be used to add security-related activities into the application lifecycle management (ALM) [26].

9. Analysis

Thus far discussions penned wide scope of cyber-attack, which challenges defense mechanism so extensively that no single solution could be conceived as a way out. In fact, a composition of technical and extra-technical consideration needs to be amalgamated to evolve ethos on cyber defense. It has become essential now to assess the gravity of cyber security risk in real terms. International Telecommunication Union (ITU) took up the cudgel and came up with Global Cyber Security Index (GCI) in the year 2014, for the first time to develop a Global Cyber Security Culture and its integration to core ICT activities [22].

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
Index Copernicus Value (ICV 2018): 86.20
DOI: 10.5281/zenodo.3595242

GCI measures commitment of ITU members in line with Global Cyber Security Agenda (GCA) adopted by ITU counties and around five pillars namely legal, technical, organizational, capacity building and cooperation. The process involves preparation of questioners for each pillar with the help of experts and asking member countries to respond online on them. ITU assesses the member countries on the basis of their response and provides GCI scores. Counties which fails to respond are assessed through open source research. The related data can be found in its report published in each year and available in its web site. In the context of its report of year 2017, the correlation study between final GCI score and score of related five pillars of top ten GCI scoring countries, reveals interesting observations.

The analysis here is taken bit ahead by taking E-governance development index (EGDI) scores of the associated countries of the same year in consideration. The calculated values are tabled in 'Table 1'. The study yields positive correlation between all variables and GCI, though the highest value is reflected in case of cooperation. The lowest correlation value, though positive, is found in case of legal and technical factors. This may indicate that cooperation between various entities are most essential for a healthy GCI score which implies strong commitment towards cybersecurity, thereby increasing cyber dependence [22].

Table 1:

Correlation Data for Year 2017	
GCI vs Legal	0.28992
GCI vs Technical	0.265465
GCI vs Organisation	0.598578
GCI vs Capacity Building	0.593021
GCI vs Cooperation	0.687543
GCI vs Egov	0.265296

GCI score assumed to reflects on Cyber dependence. Higher the score cyber environment is more dependable and lower score speaks otherwise. Technicalities apart digital security also depends significantly on factors associated with use and abuse of internet, which in turn mostly depends on human factors.

It is already been discussed earlier that Cyber Dependence is proportional to the balance between both security and insecurity. To define it more precisely followings relations are proposed [6].

1) Cyber Dependence ∞ Security,
2) Cyber Dependence ∞ 1/ Insecurity
3) Cyber Dependence = K*Security/Insecurity, where K is constant

10. Future Scope

As it is the man behind the machine that matters the most, affect of human quality on GCI score, in other words commitment towards cyber security needs to be studied more extensively.

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
Index Copernicus Value (ICV 2018): 86.20
DOI: 10.5281/zenodo.3595242

Acknowledgement

I acknowledge contribution from all cyber experts who have made their knowledge available in various forms on different platforms for common awareness.

References

[1] James W. Cortada, Ashish M. Gupta and Marc Le Noir; How the most advanced nations can remain competitive in the Information Age, IBM Institute for Business Value, IBM Global Business Services,
[2] Dutta Avijit; Knowledge Ubiquity in WEB 2.0 Paradigm; Innovation in Information System and Technology, ITCDC '09 Macmillan Publications; Page 234-238,
[3] Dutta Avijit; Collaborative Knowledge with Cloud Computing, Proceedings of the 4th National Conference, INDIACom – 2010,
[4] Dutta Avijit; Digital Communication and Knowledge Society; BIJIT – 2012 Issue 8: (July - December, 2012 Vol.4 No.2)
[5] Dutta Avijit; Agile Social Interaction on Virtual Plane; Proceedings of the 7th National Conference; INDIACom-2013,
[6] Dutta A. (2018) Digital Security: An Enigma. In: Bokhari M., Agrawal N., Saini D. (eds) Cyber Security. Advances in Intelligent Systems and Computing, vol 729. Springer, Singapore
[7] Dutta Avijit, Vinay Kumar; Managing Information Security in Digital Age, IJMSS, January 1, 2012
[8] Dutta Avijit, Vinay Kumar; Evolution and Adoption of Social IT, Volume 8 Issue 2 2013, IMS Manthan
[9] Jeffrey O. Kephart, David M. Chess, Autonomic Computing, IBM Thomas J. Watson Research Center, IEEE Computer Society 2003,
[10] Kalle Lyytinen, Youngjin Yoo, The Next Wave of Nomadic Computing: A Research Agenda for Information Systems Research, Working Papers on Information Systems, Sprouts, ISSN 1535-6078
[11] Karlene C. Cousins, Daniel Robey; Human agency in a wireless world: Patterns of technology use in nomadic computing environments; Information and Organization; Science Direct.
[12] Krishna Venkata Subramanian and Sandeep K.S. Gupta, Security Solutions for Pervasive Healthcare P1: BINAYA DASH, December 8, 2006 11:58 AU7921 AU7921˙C015
[13] Koroma J., Vartiainen M. (2018) From Presence to Multipresence: Mobile Knowledge Workers' Densified Hours. In: Taylor S., Luckman S. (eds) The New Normal of Working Lives. Dynamics of Virtual Work. Palgrave Macmillan, Cham
[14] L. Kleinrock; Nomadic Computing; Computer Science Department Los Angeles, California, USA
[15] Mark Burgin and Eugene Eberbach, Evolutionary Computation and the Processes of Life; an ACM publication August, 2012;
[16] Satyanarayanan M, Pervasive Computing: Vision and Challenges; School of Computer Science Carnegie Mellon University
[17] TechTarget, Security Media Group, Information Security, October 2014, Vol 16, No 8.
[18] Tim O'Reilly and John Battelle; Web Squared: Web 2.0 Five Years On; Special Report
[19] Thomas F. La Porta, Krishan K. Sabnani, Richard D. Gitlin; Challenges for Nomadic Computing: Mobility Management and Wireless Communications; Bell Laboratories
[20] Weiser, M. The, The Computer for the 21st Century, Scientific American, September 1991, Pages 94-104
[21] Weiser, M, Brown, J.S.The Coming Age of Calm Technology, TECHNOLOGY1 Xerox PARC October 5, 1996
[22] https://www.itu.int/dms_pub/itu-d/opb/str/d-str-gci.01-2017-pdf-e.pdf
[23] http://en.wikipedia.org/wiki/Transmission_Control_Protocol

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
Index Copernicus Value (ICV 2018): 86.20
DOI: 10.5281/zenodo.3595242

[24] http://en.wikipedia.org/wiki/Public_key_infrastructure
[25] https://en.wikipedia.org/wiki/Cellular_network,
[26] https://www.owasp.org/index.php/Main_Page

*Corresponding author.
E-mail address: dutta_avijit@yahoo.com