IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-5, Issue-6 E-ISSN: 2347-2693

Cyber security in Developing World towards Excellency by 2026 – Opportunities, Policies

N. Satheesh Kumar[1*], Zelalem Mihret[2]

[1*]Dept. Of Computing, Adama Science and Technology, Adama, Ethiopia
[2]Dept. Of Computing, Adama Science and Technology, Adama, Ethiopia

Corresponding Author: satish4info@gmail.com, Tel: +91 9866028620

Available online at: www.ijcseonline.org

Received: 25/May/2017, Revised: 02/Jun/2017, Accepted: 20/Jun/2017, Published: 30/Jun/2017

***Abstract* -** *I*nformation and communication technology (ICT) is playing a major role in the development of socio economic related issues. Some countries in the globe have taken advantage with the effectiveness of ICT, Cyberspace and are in the process of transforming their economies into knowledge and information based economies. These benefits are being challenged by the increasing cyber threats where there is no global conscious on how to regulate cyberspace even through several countries having their own cyber security policies but without proper measures. The current setup of the internet enables developing countries to work together as a global village. The goal of this paper are to help policy makers, businesses, and societal organizations to better prepare for the technological changes ahead and enable all stakeholders to consider how present day policy choices might influence future outcome. In our paper we propose cybersecurity 2026 model along with methodology which concentrate on the several components to form a framework for trust and online security.

Key Words: Cyberspace, ICT, Stakeholders, Cybersecurity Model 2026.

I. INTRODUCTION

Most developing countries correctly identify the internet as prevailing tool to advance social, economic and human development. At the same time criminals also access the internet to perform criminal activities globe at minimal cost. Hackers, virus producers abuse the available resources and take advantage of unsuspecting computer users. Almost 4 billion people are connected to the internet through cyberspace and this figure is growing rapidly and estimated to reach 5 billion people, using 60 billion devices by 2026. This enforced to serious discussion about the need to address the challenges posed by the ICT infrastructure and internet applications on sovereign nations. By 2026, more than 93 percent of people in developed countries and nearly 70 percent emerging economies are going to be internet users.

The individuals, societal organizations, business and governments are going to face the new challenges and opportunities with the technological change over the next decade. One of the main challenge facing by the government policy makers is how to balance the aggressive technological change and the new risks generated by cyber security.

How world community and individual countries address these issues will have a major effect on the global communication and information technology. The only industrial internet of things are expected to add around $15 trillion to the global economy by 2030[1]. Some governments have begun to initiate legislative process to enforce the government control over all the collected within the country including the mandatory storage location and recording of data transactions.

We discuss the issues of global economy, flow of data and cyber security issues in the next section. In the third section, we discussed about the challenges for optimized global solution. Rest of the paper will deals with present status of cyber security, recommendations, methodology, proposed model and conclusions.

II. GLOBAL ECONOMY, CYBERSECURITY AND DATA FLOW

The present globalization model allows fast growth in the internet based economy. The mobile technology is also increasing very rapidly, in which information is shared everywhere, containing data about exchanging of goods and services and personal businesses. In 1990, 54 percent of all goods traded internationally were exchanged among developed countries, according to McKinsey Global Institute, emerging economies accounted for 40 percent of goods traded in 2012, and 60 percent of goods went to other emerging economies[2]. The monthly volume of global

online traffic grew from 84000 terabytes in the year 2000 to more than 40 X 10^6 terabytes in 2012 and expected nearly 600 times higher in 2026. As an example, the volume of skype call minutes increased more than 700 percent between 2008 and 2016[3]. The users may access several accesses and lack of security and privacy protections by private and public organizations which collect process and store massive amounts of data.

III. CHALLENGES IN CREATING A GLOBAL SOLUTION

Cybercrime affects individuals of every nation, industry and government, hence countries often view these issues based on their own local strategies, interests and agendas. The dispersed approach and solution face many common gaps and technical challenges. The nations must seek common ground and solutions to treat the internet security as a global property and sharing common rules that govern global financial transactions and transportation storage system. The policy makers in all nations should give more priority for the benefits and the cost of these policies to ensure minimum impact to the global economy.

The governments and the policy makers need to review and update the existing policies regarding the user data protection and cybersecurity enforcement mechanisms at national and international level. In addition to laws and policies, the governments have the option of adopting advanced security technologies for the data protection and national security purposes. As an example, the US adopted the electronic communications Privacy Act in 1986 and European Union drafted its data protection directive in 1990's [4]. At that stage most of the people even don't know about the internet and before smart phone and mobile devices. It is also important to make enforcement of the rules more efficient, and keep in mind that technology will continue to advance rapidly.

It is very critical to recognize that the future of the internet still depends on a highly connected, open and trusted environment where people can share information and ideas, exchange goods and services and actively participate in the global community. It is also important to find widely accepted principles to protect unauthorized internet use.

IV. RECOMMENDED SOLUTIONS

A. A new method for cyber policy and the international rule of law

There are so many technologies existing today which were not available a few years back. The complicated issues when the actual storage location is not visible to the users are, the location of data and own a cyberspace. The users need to trust the service providers to access the data when he need. The new paradigm of cyber policy must address the dynamic nature of technology and the impact on individual nations around the world. The globalization model may change to meet the demands of both economy and globally shared markets.

The international rule of law will need to evolve to reflect the various protection methods for individual nations and creating new mechanism to address international disputes without any controversy. Some organizations like "Council of Europe and G20 Cloud" policies offer best practices and lessons learned for resolving different approaches of cybercrime [5]. All the nations must collaborate each other for set of common principles in consultation with experts from various industries like Technology, trade unions, law, consumer rights.

B. Accountability and Partnership:

The public and private sectors along with individual internet users are accountable for cybersecurity and all need to be aware of methods and policies for protection from the cyberattacks. Neither the government officials nor industry leaders can solve the cyber threats nor cyber related problems on their own. This partnership will create best policies at national and international levels. The cybercrime will not stop by protecting data flow and keeping data in one common location. This will not guarantee for data security. It is the right time to map the realistic and balanced approach to safeguard cybersecurity and maintain the cyberspace as a growth engine for the world economy.

C. Transparency and Innovation:

The fundamental requirement for transparency is trust. The users must have trust on the policies made by the governments to protect the users' data. To maintain the users trust, the service providers, technology companies must offer transparency and enable proper use of internet infrastructure with the required protection of user's data. The government should concentrate or made adequate policies on private sectors for transparency in data protection and transforming the user data.

V. PRESENT STATUS OF CYBERSECURITY IN THE WORLD

The political, economic and societal forces both booster and hinder technological progress and cybersecurity. Some governments have inconsistent policies and standards with varied levels of stakeholder participation and international cooperation, while other governments form clusters of open trade and foreign direct investment (FDI). Some countries are able to leverage technology to advance economic and socioeconomic development, while other countries are left

behind technology, unable to fulfill the potential of ICT. This results uneven technological growth and advancement i.e. some countries use the technology positively transforms their societies while others struggle to overcome obstacles [6].

The Characteristics are

- Inconsistent government policies and standards.
- Cooperation in some areas but not others.
- Clusters of open trade and liberal rules for foreign direct investment, while other countries and regions remain closed.
- Varied levels of stakeholder participation and international cooperation.

Cyber security Outlook is

- Societies struggle with security challenges as responses are often limited to individual nations or sectors despite o trans-border nature of internet infrastructure.
- Government focus is often on compliance over security.

The ICT policies also vary by country. Some countries run forward towards the digital trade, whereas others reject them. The world divides into two sections, one section of countries adopt policies that enable ICT growth and development, and another section that create an uncertain business environment for technology innovations. Even through some countries use technology to advance economic and social development, their ability to continue that advancement is at risk when too many countries choose not to engage in international development positions that are inherently incompatible with the advancement of global ICT, then International efforts are weakened.

Business, economic and ICT development growth is uneven, which can be linked to disparate national policies. Free trading countries with cohesive policies promote long term economic development and good governance. Other side, the protectionist countries with disjointed policies experience volatile economic conditions. According to world economic forum, one empowered by access to ICT to improve their own livelihood to international level, the other stunned and disenfranchised by the lack of access to ICT that provides critical development opportunities by limits their innovation.

Differing approaches to ICT lead to contrasting social conditions. Many countries start planning for their aging future populations early. Other countries are not as proactive. This model illustrates the tremendous impact of the failure to address aging populations; the population aged 65 and up is the leading indicator of public by very large margin.

VI. METHODOLOGY

The Cyber security 2026 model provides a baseline for potential scenarios that could result from policy choices. The various layers are delivered by the model like well settled economic models of countries, historical fluctuations deviations and the key indicators contribute to the development of the model. To get the analysis, additional research was done to validate the status of economic conditions, to derive the scenarios and explain the key factors influencing the scenarios to explore quantitative dimensions of the world in 2026.

The adoption of new technology is occurring at faster rate and having a more impact than ever before, while cyber security laws, policies and even social norms struggle to keep up with new developments. In particular the developing countries are likely to an increase in cyber security incidents as their technology adoption grows.

The basic indicator categories are Economic development, Business environment, purchasing power of customer, government strategy, Education, labor market and political stability and among them the selected indicators for this model are

Table 1 : Indicators chosen for the model

Indicators	Description
Technology	• Internet, Broadband subscriptions • Percentage of people using Internet • Network readiness index
Economy	• Annual disposable income • Expenditure on research and development • Capital investment in telecommunication
Government	• Public debt as a percentage of GDP • Regulatory quality index
Education	• Graduates in major fields like technology, engineering and mathematics

In the year 2007, the smartphone adoption has grown from less than 1 percent in the world population and in 2012 its growth is almost 10 percent, a 10 times increase in just 5 years. If this continues like this 80 percent of internet connections could originate from mobile devices by the year 2026 [7]. The quick adoption of smartphones reflects movement towards an internet based security including the internet of things. Not only laptops and mobile phones connected to the internet, but also many other physical devices like cars, medical devices. Over 50 billion objects are expected to be connected to the internet by 2020[8].

Table 2: Growth Rate in Internet Users

COUNTRY	PERCENTAGE
PAKISTAN	987%
GUATEMALA	519%
ALGERIA	385%

The number of internet users in the year 2026 are expected to reach 5 billion, among them approximately 76 percent from emerging economies. Some countries expected to see the greatest increase in internet users from the year 2012[9].

Table 4 : INTERNET USAGE STATISTICS

WORLD INTERNET USERS AND 2016 POPULATION STATS AS ON JUNE 30, 2016

REGIONS	POPULATION	% WORLD POPULATION	INTERNET USERS	PENETRATION (%POPULATION)	GROWTH (2000 -2016)	USERS %
Africa	1,185,529,578	16.20%	339,283,342	28.60%	7415.60%	9.40%
Asia	4,052,652,889	55.20%	1,792,163,654	44.20%	1467.90%	49.60%
Europe	832,073,224	11.30%	614,979,903	73.90%	485.20%	17%
Latin America	626,054,392	8.50%	384,751,302	61.50%	2029.40%	10.70%
Middle East	246,700,900	3.40%	132,589,765	53.70%	3936.50%	3.70%
North America	359,492,293	4.90%	320,067,193	89%	196.10%	8.90%
Australia	37,590,704	0.50%	27,540,654	73.30%	261.40%	0.80%
World Total	7,340,093,980	100%	3,611,375,813	49.20%	900.40%	100%

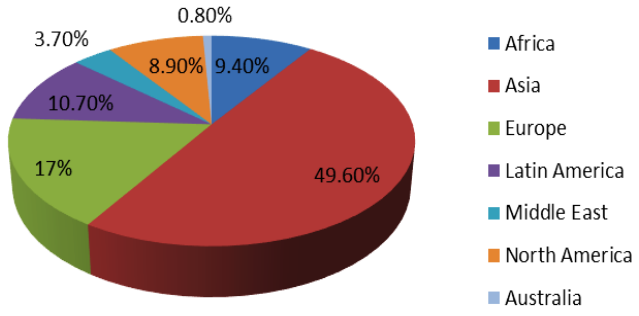


Fig 1: PERCENTAGE OF INTERNET USERS REGION WISE AS ON JUNE 30, 2016

The cybersecurity 2026 model predicts that by the year 2026, developing countries will have overtaken developed countries as the larger market. By 2026 business will lead the adoption of cloud technology in order to remain competitive and efficient.

The cybersecurity 2026 model shows that the developed countries face rapidly aging populations and falling birthrates, while emerging countries can expect more working age adults because of rising birthrates. These changes will have effect on resource needs and long term economic stability. This model forecasts that the developed countries have a ratio of the population younger than 14 years and older than 65 years is one to one in the year 2012 and expected to three to two ratio in the year 2026.

Table 3 :TOP 20 COUNTRIES WITH HIGHEST NUMBER OF INTERNET USERS - JUNE 30, 2016

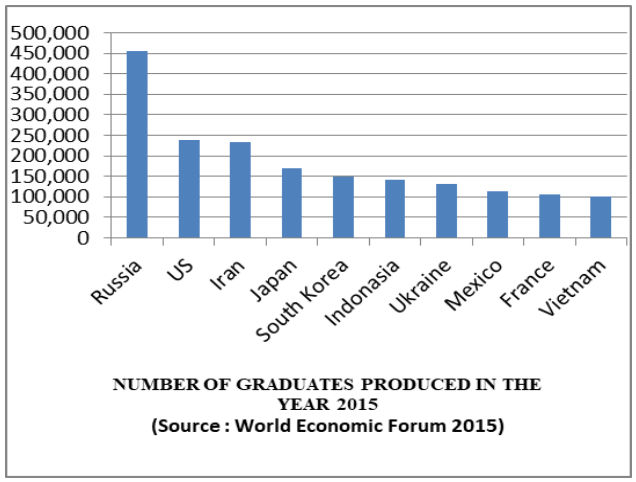
SL. NO	COUNTRY	POPULATION 2016	INTERNET USERS	INTERNET PENETRATION	GROWTH% (2000 - 2016)
1	China	1,378,561,591	721,434,547	52.30%	3106.40%
2	India	1,266,883,593	462,124,989	36.50%	9142.50%
3	US	323,995,528	286,942,362	88.60%	200.90%
4	Brazil	206,050,242	139,111,185	6705%	2682.20%
5	Japan	126,464,583	115,111,595	91.00%	144.50%
6	Russia	146,358,055	103,147,691	70.50%	3227.30%
7	Nigeria	186,879,760	97,210,000	52.00%	48505.00%
8	Indonasia	258,316,051	88,000,000	34.10%	4300.00%
9	Germany	80,722,792	71,727,551	88.90%	198.90%
10	Maxico	123,166,749	69,000,000	56.00%	2443.90%
11	UK	64,430,428	60,273,385	93.50%	291.40%
12	France	66,836,154	55,860,330	83.60%	557.20%
13	Phillippines	102,624,209	54,000,000	52.60%	2600.00%
14	Bangladesh	162,855,651	53,941,000	33.10%	53841.00%
15	Vietnam	95,261,021	49,063,762	51.50%	24431.90%
16	Iran	82,801,633	47,800,000	57.70%	19020.00%
17	Turkey	80,274,604	46,196,720	57.50%	2209.80%
18	South Korea	49,180,776	45,314,248	92.10%	138.00%
19	Thailand	68,200,824	41,000,000	60.10%	1682.60%
20	Egypt	90,067,793	333,000,000	37.00%	7300.00%
21	**Top 20 Countries**	**4,959,932,042**	**2,640,559,365**	**53.20%**	**926.70%**
22	Rest of the World	2,380,161,938	970,816,448	40.80%	835.30%
23	**Total World Users**	**7,340,093,980**	**3,611,375,813**	**49.20%**	**900.40%**

Source : International Telecommunications Union

The skill gap is that rising education levels alone is not enough to address the problem. The US bureau of labor

statistics projects an annual addition of more than 122,000 jobs in the computing occupations that require a bachelor's degree in computer science, yet only 51,000 of these degrees are awarded each year. Emerging economies like china, India and Brazil demonstrate a different pattern. For example only 4 percent of bachelor's degrees in the United States are in engineering, compared to 31 percent in china [10].

The education sector is also growing rapidly. By 2026, the emerging economies will produce nearly 17 million graduates in science, technology, engineering and mathematics fields annually which will be nearly 5 times greater than 3.3 million per year from the developed countries.



NUMBER OF GRADUATES PRODUCED IN THE YEAR 2015
(Source : World Economic Forum 2015)

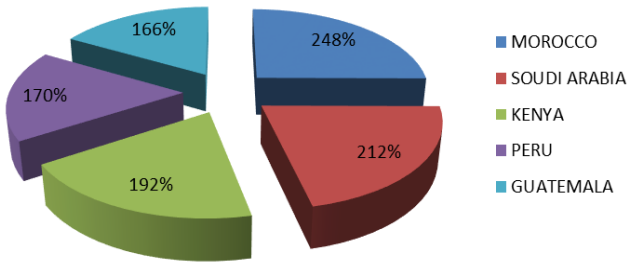


Fig 3 : COUNTRIES WITH STONGEST GROWTH IN STEM GRADUATES FROM 2013

The R & D investment is developed countries grows only 25 percent between 2015 and 2026, while the R & D investment of developing countries more than double during the same period. By 2026, developing countries experience a six fold increase in broadband penetration rates, but still lag behind the penetration rate in developed countries. The annual disposable income grows 65 percent in developing countries, but even these impressive gains are approximately 10 percent less than in the outcome.

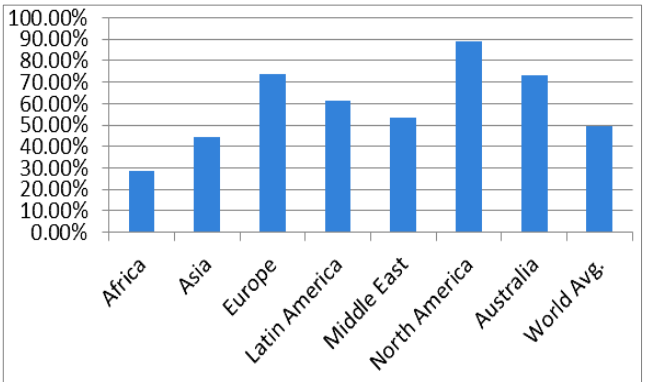


Table 4 : Internet World Penetration Rates by Regions - June 2016

VII. CYBERSECURITY 2026 MODEL

The key to success is preparation and balance. By taking the advantage of ICT advancements to address the concerns and enable all stakeholders to thoughtfully consider how present day policies might influence the future outcomes. The objectives and actions of governments, business and societal organizations today will shape the process of technology in the future. As an example, the business can invest in research and development to create new technologies, or simply use the technology to reduce the costs. They can proactively support the development of technology to increase productivity or they can restrict technology change. According to cybersecurity 2026 model, there will be 900 million people over age 65 in the year 2026, a 60 percent increase over the year 2015.

The major attribute of this model is innovation, in which clear and effective government policies and standards across economies, and strong collaboration between governments to support open trade and promote FDI. The actions of governments, business and societal organizations foster the widespread and rapid adoption of technology. If the government policies are not clear then the economic and technology growth is slower with limited adoption of ICT and deep failures in cybersecurity.

In this model of scenario strong cooperation among the national governments as well as between governments and their stakeholders make this outcome possible. The countries accelerate and deepen their transition towards knowledge based economies with an educated workforce.

The key characteristics of this scenario are

- Clear, effective government policies and standards.
- Strong international and cross sector relationships.

- Open trade and promotion of foreign direct investment.
- Multi stakeholder and intergovernmental collaboration.
- Ability to attract and retain skilled workers to grow the economy.

Impact on technology and economic development is

- Accelerated economic and technology growth
- Political, economic and social support of ICT development

Cyber security outlook is

- Society experiences the benefits of ICT with improved cybersecurity as a result of continual innovation and collaboration across industrial sectors and international borders.

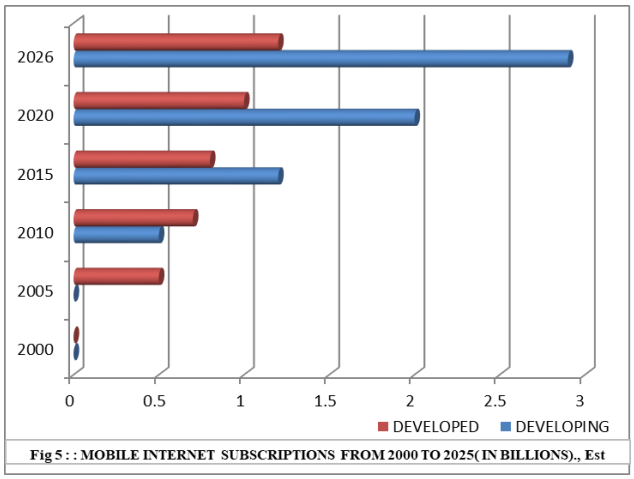


Fig 5 : : MOBILE INTERNET SUBSCRIPTIONS FROM 2000 TO 2025(IN BILLIONS)., Est

The national policies provide favorable business conditions needed to promote economic and technological growth. Countries enable growth in the ICT industry through clear policies that are based on global standards and that are reviewed regularly for new developments. The success of technology and infrastructure in developing countries greatly depends on government action. Most governments keep up with the rapidly evolving technology environment by regularly clarifying their roles in the cyber system, reviewing their policies to ensure relevance and effectiveness and upgrading their own ICT system. The governments need to adopt quickly the ICT developments because they work closely with business and societal organizations when they develop policies and standards.

Individual countries need work to harmonize their efforts and to develop the international agreements and global standards that create an environment friendly to the growth of ICT. The countries achieving the high growth depends on whether the governments to use global ICT standards and to cooperate in regularly updating them. Removing the costs and hurdles associated with nation specific standards dramatically increases innovation by providing a global platform on which to build. The countries need to identify jointly their ICT security requirements and develop processes to verify that those needs are met. For example the cloud security alliance has developed a security, trust and assurance registry (STAR) that aims to provide transparency into the security controls that cloud service providers use.

One of the most important features is the extensive use and deep market penetration of mobile computing. The mobile internet subscriptions increase by 60 percent in developed countries and by a 400 percent in developing countries. The strong economic conditions will create favorable environments for investment in research and development, which drive further economic growth by creating business opportunities and increasing productivity.

The cybersecurity 2026 model suggests that the aging population in developed countries and younger population in developing countries can pose significant challenges. The countries respond effectively to these challenges by leveraging ICT to enable improvement in major areas of concern such as health care. The policy makers set educational priorities that expand access to education, improve educational quality and skill development to market needs. The governments need to work closely with business and societal organizations to address the gap between the skills needed to drive economic growth and existing workforce talent.

The cyber security 2026 model characteristics are

- Technology foundations
- Threat environments
- Global cooperation
- Education
- Talent mobility
- Trade

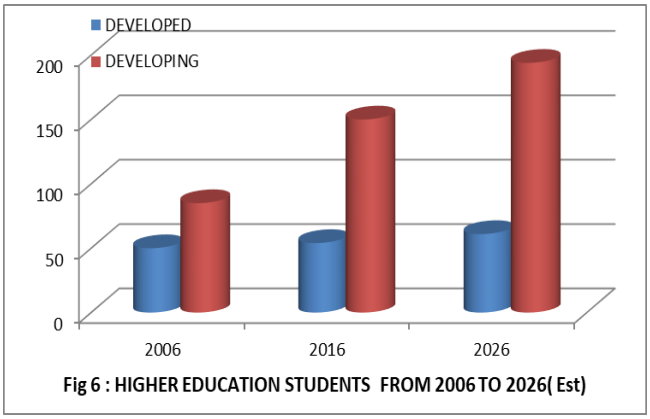


Fig 6 : HIGHER EDUCATION STUDENTS FROM 2006 TO 2026(Est)

VIII. CONCLUSION

The focusing areas of this paper are social, economic, Government, Population and Education sectors. The developing countries will need to deal with the existing challenges in all types of activities which are related to cybersecurity. The people from various categories are always expecting the change in the technology. Whatever the policies governed by the various organizations today are going to produce better and efficient results in the next decade in the form of Cybersecurity Model 2026. The policy makers are in reality more and more connected to highly secured world. Cybersecurity is one of the most challenging aspects of risk management.

The current cyber models are not working and we need to consider security secure, vigilant and resilient cyber models that can manage risks and drive innovation in the cyber world. The cybersecurity model 2026 provides a method for evaluating the changes in the literacy, education, immigration, and connectivity over time, so that all the countries can overcome the problem of Cybersecurity with better interaction than the existing method. The presented cyber security model is the best choice to overcome the challenges globally and also help to make common policies for the better coordination among the countries. Such models could minimize emerging cyber threats globally and increase trust on cyberspace and especially in emerging economies where ICT plays an important part in the future economy, and where cyber security is at early stages.

IX. REFERENCES

[1]. James Manyika, Michael Chui, Jacques Bughin, "*Disruptive Technologies: Advances that will transform life, Business and Global Economy, McKinsey"*, Global Institute, May 2013.

[2]. R. E. Crossler, A. C. Johnston, P. B. Lowry, Q. Hu, M. Warkentin, and R. Baskerville, "*Future directions for behavioral information security research*," Computers & Security, vol. 32, pp. 90–101, Feb. 2013.

[3]. Greenwald G, MacAskill E., *"Boundless Informant: the NSA's secret tool to track global surveillance data*", The Guardian. 2013 Jun 11;11.

[1]. Cavely, M.D.(2014) Breaking the Cyber Security Dilemma: Aligning Security needs nad Removing Vulnerabilities(Springer Science)

[2]. Laukka, M(2010). "Criteria for privacy support system". Proceedings of the 5th Nordic Workshop on secure IT systems, Raykjavik, Iceland, Oct 12-13.

[3]. DeGusta, Michael. "*Are smart phones spreading faster than any technology in human history*." Massachusetts Institute of Technology Review (2012). APA

[4]. Manyika J, Bughin J, Lund S, Nottebohm O, Poulter D, Jauch S, Ramaswamy S., "*Global flows in a digital age: How trade, finance, people, and data connect the world economy*". McKinsey Global Institute; 2014.

[5]. S.Jayasri, D.Karthika, "*Microcontroller Based Traffic and Road Condition Monitoring Alert System Using Internet of Things*", International Journal of Computer Sciences and Engineering, Vol.4, Issue.4, pp.272-279, 2016.

[6]. United States. "*White House Office, and Barack Obama. International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked Worldr*". White House, 2011. APA

[7]. Gwartney, James, Robert Lawson, and Seth Norton. "*Economic freedom of the world 2008 annual report"*. The Fraser Institute, 2008. APA

[8]. *Organisation for Economic Co-operation and Development (OECD). Better skills, better jobs, better lives: a strategic approach to skills policies*. OECD, 2012. APA

[9]. The UK Cyber Security Strategy, 2011, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-agency-prism-outline-lyrics#lyric

Authors Profile

Dr. N. Satheesh Kumar pursed Bachelor of Science from Kakatiya University in 1997, Master of Science in year 2001 and Ph.D. in 2013, and currently working as Associate Professor in Department of Computer Science and Engineering, Adama Science and Technology University since 2015. He is a member of IEEE & IEEE computer society since 2013, a life member of the ISTE since 2009. He is the initiator and leader of Network Science Research group in currently working organization. He has published more than 30 research papers in reputed international journals including Thomson Reuters (SCI & Web of Science) and conferences including IEEE and it's also available online. His main research work focuses on Mobile Adhoc Networks, Network Security, Light Fidility IoT and Computational Intelligence based education. He has 18 years of teaching experience and 4 years of Research Experience.

Mr. Zelalem Mihret pursed Masters Degree in Computer Science from University of Trento, Italy in 2014, and currently working as Senior Lecturer and Program Chair, Computer Science and Engineering program, Adama Science and Technology University. He is the active member in Network Science Research group in currently working organization. He has published more than 10 research papers in reputed international journals including Thomson Reuters and conferences including IEEE and it's also available online. His main research work focuses on Networks and Security, Light Fidility IoT, Cloud Computing and Software Engieering. He has 3 years of Research Experience apart from the teaching experience.

