International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 3 | ISSN : 2456-3307

Challenges and Risks of Privacy and Personal Information Security in Digital India

V Karamchand Gandhi[1], Dr M Suriakala[2]

[1]Doctoral Research Scholar, PG and Research Department of Computer Science, Dr Ambedkar Government Arts College (Autonomous), Vyasarpadi, Chennai, Tamilnadu, India

[2]Assistant Professor, Department of Computer Science, Government Arts College for Men (Autonomous), Nandanam, Chennai, Tamilnadu, India

ABSTRACT

The Digital India programme is a one of the dream programme of the Government of India with a target of transforms India into a digitally empowered society and knowledge economy. It has been required to ensure e-Governance in the country to promote inclusive growth that covers electronic services, products, devices and job opportunities. Indian organizations have not paid adequate attention towards the area of cyber security. The widespread absence of even the most routine security tools and policies has left many Indian organizations vulnerable to serious cyber-attacks. Although spying has been an accepted all the part of digital contents, digital era is termed as the golden age for spying. Moreover, electronic manufacturing in the country needs to be strengthened. In this paper, the emerging challenges in security and privacy faced by the organizations in India are analyzed. The security mechanisms used by the organizations have been identified. The security counter measures which are needed to be taken to overcome the vulnerabilities in Digital India are identified.

Keywords: Digital India, Information Security,

I. INTRODUCTION

Digital India is a vision programme of India based on technology with a target of transform India to a digitally empowered society and a knowledge economy. To realize the objectives, the programme has established an ecosystem comprised of several Ministries and government departments, initiatives which are coordinated by the Department of Electronics and Information Technology (DeitY) by the Indian Government. Bring public services to the people by the use of information technology is an important part of Digital India and it makes the initiative as a technology led enabling programme to the citizens of India. The Digital India programme was launched by Prime Minister NarendraModi on July 1st 2015.

The objective of Digital India is transforming the country into a knowledge economy and information society, the initiative needs some preparatory measures. Creation of sufficient physical infrastructure in IT, providing the vital governance services to the people on e-mode and empowering people to handle digital technologies (digital literacy to the people) are the main key areas to prepare the Nation towards Digital India *[1].* Following are steps and targets related with the key areas to attain the objectives of Digital India.

- High speed internet facility, high configuration mobile phone and e-based bank account, access to common service centre, internet identity, sharable private memory space on a public cloud and safe and secure cyberspace.

- E-Governance and E-services on demand will be available in real time in online and mobile platforms, seamlessly integrated across all departments and jurisdictions. All citizen information and documents to be made available on the public cloud platform so that physical document presentation can be minimized. Cashless electronic transactions and Geographical Information Systems (GIS) will be integrated in Digital India.
- Empower citizens, especially rural citizens, by providing digital literacy to use and utilize the services given by Digital India.

Digital technologies influence almost all aspects of the economy and society. Hence the programme covers wider areas to make India a digitally empowered country. The Government has identified the following pillars for Digital India.*[2]*

Universal Access to Phones: Mobile phone coverage will be provided to all the remaining villages in all over the country. The Department of Telecommunications will be the nodal department and project cost will be around Rs 16,000 Cr during 2014-18 to strengthen the telecommunication in India.

E-Governance – Reforming Government through technology: Digital technology will be used for the better delivery of government services to the citizens. The government aims to improve processes and delivery of services through e-Governance with UIDAI, payment gateway, EDI and mobile platforms. School certificates, voter ID cards and etc will be provided online. All databases and information should be in electronic form and not manual to eliminate the manual process.

*IT for Jobs:*This aspect is focuses on providing skill and training to the youth for availing employment opportunities in the IT/ITES sector. This is focusing on disadvantaged regions- rural areas and North East, training one crore students in IT/ITES Sector, training three lakh service delivery agents etc.The main objective of this pillor is to enlighten the knowledge of youth in IT *[3].*

*Early Harvest Programmes:*Ithis pillar, the Government will set up Wi-Fi facilities in all universities and in public spaces like Bus, Railway Stations, etc across the country, eBooks will be provided to Educational Institutions, email will be made the primary mode of communication, Aadhar Enabled Biometric Attendance System will be deployed in all central government offices etc.

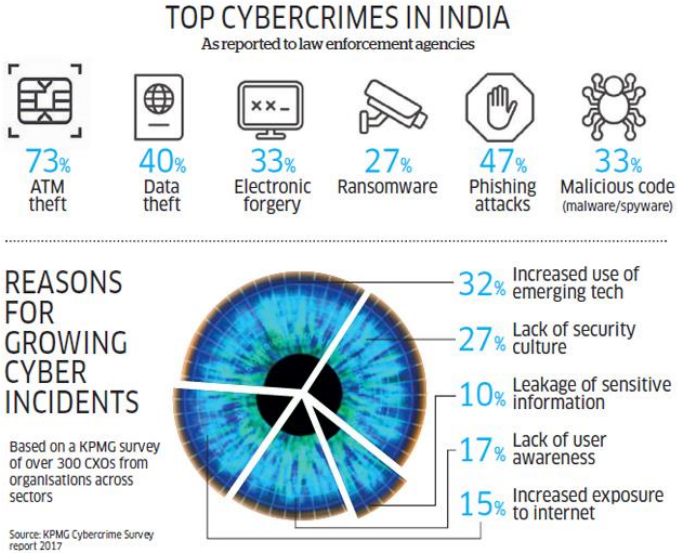

Figure 1

II. DIGITAL INDIA – HOW SAFE IT IS?

In the recent days, the government of India insists the people to link their tax returns, bank accounts, mobile SIM cards, mutual funds and more to the 12-digit Aadhaar. This has raised the billion-dollar query. In the year 2016, 3.2 million credit and debit cards details were stolen by Chinese hackers report said *[4].* A 2017 study by PwC and Assocham reported that attacks on Indian websites increased five times in the past four years. It noted that Digital India spends tiny amount of concentration on security. To reassure 1.19 billion Aadhaar users that their details cannot be accessed over platforms like WhatsApp, the Unique Identification Authority of India (UIDAI) gave an option last week to create a

virtual ID which has 16 digits to hide the real Aadhaar.

III. DATA POOLS & RISKS

In Digital IndiaApart from Digital India platform's data sources, there are equally confidential data pools with sensitive personal information about bank transactions, taxes filed, passport details, property ownership, birth certificates, photographs and so on. These data pools reside in systems of Passport Offices, e-governance portals, income tax e-filing centers offices System, UIDAI and others. The size of data on these system increase rapidly minute by minute *[5].* A millions of peoples apply for Aadhaar every month or go to its centres to update or correct information, including address, date of birth, name. The government is the biggest player in digital India, with several petabytes of data residing with various agencies. It is the whole responsible for its security related issues.

And there are multiple user agencies accessing that data pools to complete their tasks. These include banks, telecoms, insurance companies, credit card issuers, mobile wallets, ecommerce companies, hospitals, security and gas agencies. Linking Aadhaar with everything is a risk if done without adequate security wall, checks and balances. Who is the actor, who owns the information, how and why do multiple agencies have access to databases? There are good uses and bad uses of data. The trouble is we don't know about the bad user. Paytm has a 50-strong team in Toronto to secure transactions for its 200 million users in India *[6].* When every bank account is verified with Aadhaar, every transaction will be tracked. It will make it more secure as frauds will be detected. The accent is clearly on the cure.

Figure 2.*Common precautionary activities to avoid Vulnerabilities*

IV. RISKY YET UNAVOIDABLE IN DIGITAL INDIA

Back to older, paper based transactions, money order transfers in post offices, queuing up in banks or writing cheques like time-consuming practices are not the right answer for the best practices now a days. Reliance Jio's user base ran into millions within weeks by Aadhaar ID verification. Passports are now issued in two weeks with Aadhaar from six months earlier. Tax payments are filed in real time by e-filing procedures *[7].* Yet Digital India needs to build trustful and greater security countermeasures in the access of data pools. The problem with government databases is that these are live, accessed by multiple users within the government and outside agencies. That multiplies the security challenge. No one's bank

account details have been compromised because of Aadhaar data leaks.

As it is, the majority of non-biometric information that Aadhaar captures is already there in public domain and people share more voluntarily on Facebook, twitter and other social media platforms *[8].* For Aadhaar to be breached, the hacker needs biometrics as well, a near impossibility as they are securely encrypted and never shared with anyone. Biometrics-based Aadhaar has helped remove fake beneficiaries and ghost accounts in all the areas like ration card, voter Id, etc. However, despite an unbreakable 2048 bit encryption of most government databases, 100% security may never be possible *[9].* There is more financial fraud in the US than in India, yet they have not given up on Digital America. JP Morgan Chase, Visa, PayPal have all seen major cyber breaches in the past. The ratio of risk of financial fraud in the US to India is 8:1. Digital Fraud in India has been under verification and control due to the Reserve Bank of India's insistence on the tighter, two-factor authentication and other security measures and because the number of people using digital services frequently is still low. More than 50% e-shoppers still insist on cash on delivery option.

V. HUMAN FACTOR IN DATA SECURITY

Technology has increased in complexity day by day. People don't depend on one technology partner in their day today life but an ecosystem of partners who supply different software. People dependence on others is a security risk in all the way. Often users store personal information on their smartphones*[10].* They download free apps like WhatsApp or TrueCaller. These apps want to make the people's life easier, but at the cost of sharing their address book. An app could seek permission in its long list of conditions which nobody cares to read to copy every word people key in, compromising security. Social medias have user's name and birth dates, besides all frequent updates. Amazon, Flipkart and other ecommerce companies know addresses, mobile numbers and credit card numbers, etc. Over the next few years, if users are able to do banking via links, say, on Facebook, it will multiply risks. Users need to be careful before connecting to public Wi-Fi *[11].* Also, using the corner photocopy shop or even printers and copiers in offices to get Aadhaar or passport copies is not without risks.

VI. NOT ENOUGH SECURITY SPEND

Most Indian companies still don't spend the much of money that securing digital assets needs. The US government spent $19 billion in 2017 to secure IT assets. In India, the Ministry of Electronics and Information Technology mandated all government departments in September 2017 to spend 10% of their technology budgets on security. This was after attacks like WannaCry. The 2017 Global Cyber security Index by the UN ranked India 23rd among 165 countries in commitment to cyber security *[12].* India scored better in security than in ease of doing business, but is not entirely risk-free. It need to enrich the higher security infrastructure.

VII. GET READY FOR QUANTUM ERA

In the security world, it's a never-ending cat-and-mouse game, with hackers trying to breach networks each and every minute. The greatest threat to Digital India could arise from hackers residing anywhere in the world. About 20 years back, 40-bit encryption was considered high-technology. Today it can be breakthrough in minutes and companies have moved to 128-bit and 256-bit encryption. Databases like Aadhaarare secured with 2048-bit encryption. That could take thousands of man hours or several years to break the fence. However, what appears impregnable today could succumb to quantum computing (QC) in just a few years. Today's encryption methods could be brought down with QC in minutes. It could become main stream in 8-10 years.

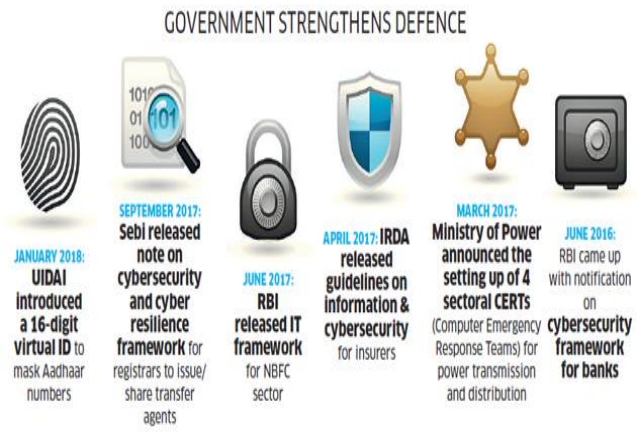

Figure 3

In today's computing world, information is stored in binary 0s and 1s. QC increases the ability of computers to store information in multiple bits or states. This allows them to perform incredibly complex calculations at speeds unimaginable today. There is a need of Governments and companies will have to migrate to quantum era much like how they adjusted to Y2K and is being called Y2Q. Even in pre-QC era, the need for quantum based safe encryption is real. QC can help in enhancing response to attacks and detection capability *[13].* Now a day, companies are think about to strengthen security as data resides in multiple places. However, Cent percentage of security is a mythical target because of the variety of attack methods, number of known and unknown hardware and software vulnerabilities, limitations in detection and response technologies, etc.

VIII. WANTED SECURITY GEEKS

There are not enough geeks to protect digital data and digital assets in IT era. Digital India needs top professionals who can build hack proof systems and are blockchain and quantum computing era ready and ensure 24x7 protections against threats. All the way, India is trying to bridge the gap between demand for cyber security professionals and the talent pool of available skilled professionals in this domain of Digital data Security *[14].* Lack of security professionals is a worldwide problem as well an area that Indian engineers can explore. Even the US is expected to have half-a-million or more unfilled cyber security jobs by 2021. Every IT worker needs to be involved themselves in protecting and defending digital data from hacking and vulnerabilities. Cyber security, a complex domain with constant flux and rapid changes, wants skilled Security professionals having expertise in mathematics, statistics, data science and computation in order to keep up with the latest challenges. Giving shoulder with the Digital India army of security geeks could be the next hot spot for engineers.

IX. CONCLUSION

Digital India will create new economic and social opportunities to the society. At the same time that will also be creating an increasingly large attack surface for criminals to exploit data from well-protected IT environments. The government initiative that seeks to transform the country into a connected economy can be successful only when security of the connected devices is assured. The increasing synchronization and interpretation of existing digital data and processes within government departments will require maximizing security posture while keeping critical data flowing in such a daunting threat environment. Due to these all the cyber security risks, the movement towards Digital India is inevitable. The government and enterprises realize this and efforts are on for developing better systems for maintaining security while also taking advantage of the plethora of technological applications that have exploded during the last few years.

X. REFERENCES

[1]. http://www.digitalindia.gov.in/content/about-programme

[2]. https://economictimes.indiatimes.com/news/economy/policy/how-safe-is-digital-india-indias-vast-data-pools-need-to-be-secured-

with-tighter-de-risking-tools/articleshow/62489823.cms

[3]. http://www.academia.edu/16201285/Cyber_Security_of_Digital_India

[4]. V Karamchand Gandhi "An Overview Study on Cyber crimes in Internet" International Journal of Information Engineering and Applications from IISTE, Volume 2, Number 1, pages 1-5, February 2012. ISSN 2224-5782 (Paper) ISSN 2225-0506 (Online).

[5]. Digital India, Government of India Press Release, August 2014. See: http://pib.nic.in/newsite/PrintRelease.aspx?relid=108926

[6]. Digital India Programme : Importance and Impact .Retrieved from http://iasscore.in/national-issues/digital-indiaprogramme-importance-and-impact

[7]. Digital India. Unlocking the trillion Dollar Opportunity: ASSOCHAM –Deloitte report, November 2016.Retrieved from www.assocham.org.

[8]. Kadam Avinash (2015). Why cyber security is important for digital India. Retrieved from http://www.firstpost.com/business/why-cyber-security-is-important-for-digital-india-2424380.html.

[9]. V Karamchand Gandhi, "An Overview Study on Cyber crimes in Internet" International Journal of Information Engineering and Applications from IISTE, Volume 2, Number 1, pages 1-5, February 2012. ISSN 2224-5782 (Paper) ISSN 2225-0506 (Online).

[10]. Midha Rahul (2016). Digital India: Barriers and Remedies . International Conference on Recent Innovations in Sciences, Management , Education and Technology. Retrieved from http:// data. Conference world .in/ICISMET/P256-261. Pdf.

[11]. V Karamchand Gandhi, "A Study on Phishing: Preventions and Anti-Phishing Solutions" International Journal of Scientific Research, Volume 1, Issue 2, July 2012, pages 68-69. ISSN 2277-8179. (UGC Approved Journal)

[12]. Rani Suman(2016) .Digital India: Unleashing Prosperity . Indian Journal of Applied Research, volume-6, Issue 4, pp187-189 Retrieved from https://www.worldwidejournals.com/indian-journal-of-applied...

[13]. Digital India Programme : Importance and Impact .Retrieved from http://iasscore.in/national-issues/digital-indiaprogramme-importance-and-impact

[14]. http://www.nextgenias.com/2015/09/essay-on-digital-india-programme-for-upsc-ias-preparation

With the security and privacy of 1.2 billion citizens at risk, a serious, focused and apolitical discussion on the subject is required. What are the rights of those whose data is held with companies and government departments?Â The current Information Technology Act, with its limited data protection and privacy-related provisions, does not provide for an all-encompassing, comprehensive legal framework for privacy and data security. There are glaring gaps that must be plugged through such measures: Expansion of the definition of sensitive personal data under Rule 3 of the Sensitive Personal Data Rules: The categories of sensitive personal information (passwords, financial information, sexual orientation among others) are inadequate. Safety and security on the Internet: challenges and advances in Member States: based on the findings of the second global survey on eHealth.(Global Observatory for eHealth Series, v. 4). 1.Internet - utilization. 2.Computer security.Â Internet security, in the form of spam, is another persistent challenge. Crime follows opportunity and the first spam actually appeared in 1978, shortly after the Internet itself had been opened to the public. Spam itself poses a risk for individuals and institutions, but its greater threat may be as a vehicle for fraud, viruses, malware, and spyware.Â The capacity for digital literacy is intertwined with accessibility to and quality of online health information. It is anticipated that the importance of these issues will become even more prominent in the coming years.