Chapter 5
Role of Cyber Security in Public Services

Parag Kulkarni and K. B. Akhilesh

Abstract For a developing country like India, providing public services catering to the needs of the masses is a challenge, and to achieve an economic growth with this underlying challenge, going digital is an important step. The initiatives which are taken as a part of providing public services in India are looked in detail. The analysis of these initiatives for providing an improved and a superior quality of public services is done in the context of cyber security, analyzing the issues which arise due to the cyber-threats. The soft point analysis with respect to these services is done, and the competency of the measures taken so far for ensuring cyber security is analyzed.

Keywords Public services · Cyber threats · Cyber security

5.1 Introduction

Today in the technologically advanced world, we are knowingly or unknowingly interacting with the cyber systems in one way or the other. These cyber systems' devices such as computers, smartphones, or the cyber-physical systems are ubiquitous and are interconnected and interact either through physical wires or through wireless networks such as Bluetooth and Wi-Fi. The enhancement in their capabilities comes because of the connectivity which they can provide. This connectivity is very much desired on one hand but can also be a cause for the compromise of the security of these systems. The prevention of these systems from any action intended to malign their security calls for the notion of cyber security.

The word cyber security refers to the protection of these systems from any kind of misconduct, be it damage or the theft of their hardware or the underlying software and preventing them from the misconduct and misdirection of the services they provide.

P. Kulkarni (✉)
KPMG India, Gurgaon, India
e-mail: parag2803@gmail.com

K. B. Akhilesh
Department of Management Studies, Indian Institute of Science, Bengaluru, India
e-mail: kba@iisc.ac.in

K. B. Akhilesh and D. P. F. Möller (eds.), *Smart Technologies*,
https://doi.org/10.1007/978-981-13-7139-4_5

The word cyber security is used in a broader prospect, and it aims at preventing the damage which may come from the network access and the input of the undesirable code or data (En.wikipedia.org 2018a, b).

Public services are the services which the government provides to the people who are living within the borders of the government's jurisdiction. These services are provided directly by the means of the public sector or by providing the finances for the same. Going by the literal definition, it is defined as the services that are available to all irrespective of their income, physical, and/or mental ability. Some of the examples of public services are law enforcement through police and judiciary, paramedics, banking facility, electricity supply, water supply, etc. (En.wikipedia.org 2018c).

The technological advancement which has been talked about earlier is strongly interacting with the provision of public services today.

5.1.1 Importance of Cyber Security in India

India is becoming digitalized at various fronts at an increasing rate, bringing in the menace of cyber-threats which must be dealt with upfront by putting systems capable of tackling this in place. There has been a paradigm shift in the way public services are being delivered to the common citizen of the country because of the interlinking of the delivery of these services with the technological advancement in Information and communication technology (ICT). In India, this has been achieved by the virtue of many major initiatives which have been taken in the recent past.

5.1.2 Digital India

The Indian IT industry has witnessed tremendous growth in the last decade mainly by the advent of smartphones, broadband networks, cloud computing, and business data analytics which is expanding with each passing day. The government is aiming for the digital transformation of India to make it a digitally empowered knowledge economy. As a result, it is promoting the accessibility of the digital infrastructure as a utility to each citizen. It also aims at promoting e-governance at a strategic level.

The common reports of data breaching resulting in deep financial and privacy loss are a great cause of concern in India. There has been a 300% surge in the registered cybercrime cases in the country. This shows that the digital space is very susceptible to numerous intrusions like stealing the data of national importance, attacks on open networks which temporarily disrupts services, electronic frauds via hacking, stealth of commercially valuable computerized data, and cyber-espionage. The risk of data breaches multiplies as India is taking significant steps and measures toward becoming a cashless economy. Terrorism is not only restricted to the physical intrusion of the enemy but has found new avenues by the virtue of intrusion of the spyware and malware in the systems of national importance (Consultantsreview.com 2018).

5.1.3 Aadhaar

Aadhaar has been the most talked about initiatives taken in the direction of providing and monitoring the public services to the common man by giving them a unique ID number. It covers over ninety-nine percent of the Indian citizens by giving them a twelve-digit unique identity number. This ID is based on the biometrics and the demographics data of the person. The ID is given by the Unique Identification Authority of India (UIDAI), which has successfully enrolled 1.2 billion members, making this "the world's largest ID system." This is often referred to as "the most sophisticated ID program in the world." One of the main purposes of the Aadhaar is the prevention of the leakages of the subsidies provided by the government. As all the subsidies will be directly transferred to the bank accounts of the people, and as the bank account will be linked to a particular UID, there will be no mismatch in the provision of the subsidies to the intended person, and thus, it also eliminates the need of the multiple middlemen required to transfer the benefits to the intended person which surely eliminates the possible corruption which inherently creeps in the system meant for serving the public. In India, the tax returns, bank accounts, mobile Sims, mutual funds, etc., are being linked to the 12-digit Aadhaar number raising the concern of it becoming a soft spot of target to the cyber-attacks to steal all kinds of citizen data at one go.

5.1.4 Smart Grid

It is an information technology and communication integrated power delivery system which is enabled with monitoring, prediction, and the management of energy usages. As the present loss of energy from the grids is one of the highest in India, the establishment of these smart grids becomes extremely important. The synchronous grid in India is one of the largest in the word, covering an area of over three million square Kilometers with a capacity of 260 Gigawatt serving approximately two hundred million customers. National Smart Grid Mission was established in the year 2015 to provide an impetus to India's vision of "Access, Availability, and Affordability of Power for All" by the virtue of electricity smart grids across the country. In India, numerous smart grid projects are being implemented like the establishment of the smart meters and the intelligent power transmission and distribution equipment system by the KEPCO (Korea Electric Power Corporation) in the state of Kerala. Gujarat has already implemented modernized electricity grid with a capability of analyzing consumer behavior of usage. BESCOM (Bangalore Electricity Supply Company Ltd) has also envisioned a smart grid pilot project in this direction.

Challenges: There is always a concern with the interconnectivity of these grids, as they will be always vulnerable to the threats of the cyber-attacks. Smart grids are susceptible to a greater risk because they comprise of different types of intelligent, communication, and monitoring electrical elements being employed, enhancing the functionality of a power grid. Any security issue with the smart grids may lead to the disruption of services for a whole city. Along with this, there is always a threat of data theft be it customer usage data or the data pertaining to the service itself. Attackers and hackers can have an unauthorized access to modify load conditions for destabilizing the grid and can compromise with the smart meters to alter customers' energy usage-related data, leading to loss of revenue (The Centre for Internet and Society 2018).

5.1.5 Smart City

India is envisioning the development of cities by the initiatives such as smart city, and the very essence of the functionalities of these cities lies in the fact that the processes and services in a smart city are digitally connected. The uses of Internet of Things (IoT) devices are indispensable for the processes in these smart cities. The major concern is that the sensors used in the buildings, equipments, etc., are not secured and are not thoroughly tested, and as there is a lack of standardization for the IoT devices, they become susceptible to hacking. The connectivity of these devices also brings in the threat of the security concerns with respect to the tampering done with them, as notorious individuals can hack the sensors and feed them with false data, leading to disruption of the sophisticated processes and services such as waste management, transportation, and smart water supplies.

Thus, the influential sphere of digitalization of the public services is expanding for a developing country like India, calling for enriching our perspective towards analyzing the threats which may be there, to gain an understanding of the importance of cyber security in the delivery of public services.

5.2 How Cyber Security Can Be Achieved

5.2.1 Notions of Cyber Security, a Technical Note: There Are Four Major Areas that Are Covered Under Cyber Security

- **Application Security**: This covers the area related to the measures or the countermeasures taken for the defects that may arise during the life cycle of the development of an application, be it design, development, deployment, upgrade, or the maintenance. The major techniques to implement application security involves auditing and logging, Authentication and also the Authorization of the user and the role, validation of the input parameter, management of a session, manipulation of the parameter & exception management

- **Information Security**: Identity theft is mitigated, and privacy protection is achieved by the protection of information from unauthorized access. Some of the well-known techniques by which it is achieved are cryptography, identification of the user, authentication of the user, and the authorization of the user
- **Disaster Recovery**: The term disaster refers to the cyber-attack or the potential threat that has been materialized. In such a case, there should be a concrete plan that must be in place to ensure recovery and resumption to the normal pre-disaster state as quickly as possible. Hence, the process of disaster recovery planning which includes and is not limited to the development of the recovery strategies during a disaster, establishing priorities, and performing risk assessment
- **Network Security**: Safety, reliability, usability, and the integrity of the network are protected by the virtue of network security. Effectiveness of a network security can be gauged by knowing the degree to which it is able to target and stop the variety of threats from entering and spreading in the network. Providing an access which can be done securely by the virtual private networks (VPNs), anti-spyware and anti-virus to ensure prevention of any malicious attack, identifying fast-spreading threats like the zero-day and zero-hour attack. Firewalls which are capable of blocking unauthorized access to any network along with the intrusion prevention systems (IPS), etc., are some of the components of network security (Itgovernance.co.uk 2018).

5.3 What Is Being Done to Achieve It in India: Initiatives and Policies?

5.3.1 Indian Computer Emergency Response Team (CERT-in)

To provide on-time security warnings and effective response to the incident for the enhancement of the security of the Indian communication and information infrastructure, CERT-in was established in 2004. Early warnings and advisories are being provided by its 24/7 operations and engagement with the users. It caters to the e-governance project owners, critical sectors, the law enforcement, and judiciary. It is designated as a national agency to perform the following functions:

- Collecting, analyzing, and disseminating the information related to cyber-incidents
- Forecasting the cyber security-related incidents
- Taking emergency measures
- Coordinating the activities pertaining to the response of cyber-incident

- Issuing the vulnerability notes, guidelines, and advisories related to prevention, response, and procedures for the information security practices.

A computer forensic facility for the investigation of the cybercrimes has been established by the CERT-in, and the network is being augmented for the inclusion of the investigation related to network and mobile forensics. It also provides training and support for the investigation of cybercrime to the government officials in defense, banks, law enforcement agencies, and the judiciary.

5.3.2 Cyber Security R&D

With the aim to provide impetus to the R&D activities, academic institutions and autonomous research & development organizations are provided grant in aid for undertaking the timebound R&D projects for Security Architectures, Surveillance Monitoring & Forensics, Network & Systems Security, Cryptography and Cryptanalysis, Assurance Technologies, Vulnerability Detection and Analysis.

5.3.3 Controller of Certifying Authorities

There is an importance and a priority to provide sanctity to the digital signatures because they are being widely used now for the authorization like the handwritten signatures. Authentication of the users is done by the digital signature certificate issued by the certifying authorities (CAs) for the digitally signed documents under the Indian IT Act, 2000. The controller of certifying authorities (CCA) verifies if a given certificate is being issued by a licensed certifying authority (CA) by certifying the public keys of CA's by its private keys. For the mentioned purpose, Root Certifying Authority of India (RCAI) operates. NRDC—National repository for digital certificates is a repository of all digital certificates which are issued by the certifying authorities in India and is maintained by the CCA.

5.4 Shortcomings with Respect to Cyber Security in India

- Majority of the hardware and software technology along with the cyber security tools in India are being imported, and there is a skill gap in India for inspecting them with hidden Trojans, malware, backdoors, and flaws, making them susceptible to cyber-attacks. Publicly available sources and vendor communication are the only source of knowledge of these weaknesses and vulnerabilities.
- At present, there is non-availability of top-level experts for high-end jobs in the field of cyber security, this urgently emphasizes the need to build skills in these

very sophisticated areas for building the high technology products indigenously or at least gaining the expertise to critically examine them before deployment in the critical industry and infrastructure sector.

- There is a need of skilled hands-on cyber security experts in the five major functional areas of cyber security as presently there are only 62,000 trained cyber security experts and the requirements will shoot up to 1 million by the end of 2025(NASSCOM's Cyber security Task Force).
- Lack of formal graduate-level courses on cyber security in India and there are no training concepts like virtual laboratories and cyber ranges.
- Without the knowledge of the owner, a smartphone can be used as a master-spying device which can be controlled remotely. This fact is not known by a majority of the one billion mobile phone users. Thus, this lack of awareness is to be mitigated (Firstpost 2018).

5.5 Case Studies from the Indian Context

5.5.1 Ransomware Attacks Disrupting Public Services

Ransomware is a malware which is usually sent through the emails, it encrypts the data in the target system, and the access to the data gets blocked till the ransom is paid in bitcoins which is the virtual currency.

5.5.1.1 WannaCry Ransomware

This ransomware attack which began on 12th May 2017 impacted many public and private organizations in India, disrupting their services. Among the public services, there were many cases of the attack like (1) The computer systems of 18 police units in the state of Andhra Pradesh got compromised; (2) Customer care centers of Electricity Distribution Company in West Bengal; (3) Gujarat State Wide Area Network. **Cerber ransomware**: In Jan 2017, three servers of the Quality Council of India in Delhi were attacked by this ransomware. The experts took 36 hours to bring back the systems to the normalcy without the payment of any ransoms. **Locky ransomware**: computer systems of the revenue and public works department in Maharashtra got infected in May 2016 by this ransomware.

Tackling these attacks in the future: (1) there should be an urgent enactment of the cyber security laws in India, along with the amendment of the IT Act 2000 making these cyber-attacks a criminal offense and fixing responsibilities, liabilities, and accountabilities of the intermediary agencies and the Internet service providers in the future occurrences of such offenses. (2) An NGO named Cyber Peace Foundation from the state of Jharkhand has deliberately set up vulnerable networks in ten states, to analyze the nature of the attacks and determining the appropriate responses, more such initiative needs to be promoted (Dey and Dey 2018).

5.5.2 Case of Cyber-Attack on Indian Defense

In the year 2012, a malware-infected USB was able to transfer the classified data from the INS Arihant which is India's first nuclear submarine. The USB device covertly collected the classified files based on certain keywords from the stand-alone computers and stored it in hidden folders, when connected to an Internet-enabled system it transferred the files to a specific IP address (Theregister.co.uk 2018).

5.5.3 Global Case Studies

5.5.3.1 Impact of Ransomware on National Health Service (NHS) in UK

Scale of the NHS in England: the NHS, with its 236 trusts, serves around one million patients every day. It employs over one million people fulltime in England. The total yearly spending (2017–18) on health care in England is nearly 124 billion pounds, with nearly 110 billion pounds spent on day-to-day running of the NHS and the rest on training, education, promotion, etc., apart from this there are 1.58 million people involved in social health care and twenty thousand organization providing accommodation and personal care from nursing homes and residential care.

Impact due to the ransomware attack in 2017: around one-third of the trusts (80 out of 236) were affected by the cyber-attack, this led to a major disruption in the services provide by the NHS. The systems were locked out and the service providers were forced to use pen and paper for tasks such as record maintenance and appointment bookings. Nearly, 1.2% of the appointments had to be either rebooked or to be canceled in the first week of the outbreak of this cyber-attack. As a general practice, the patient data are stored digitally, this attack disrupted the flow of information from the primary care to the secondary care services (Smart 2018).

5.5.3.2 DNS Attack on UK Educational Services

DNS attack: Domain name system (DNS) converts the user-friendly domain name to the computer-friendly IP address. When a user-friendly domain name is typed by the user in the client system, the DNS resolver searches for the IP corresponding to the domain name in the cache, and if it is not present in the cache, it queries with the DNS server to get the mapping of the domain name to its IP. There are various forms and types of DNS attacks which take the advantage of the back and forth communication, some of them are zero-day attack, cache poisoning, denial of service,

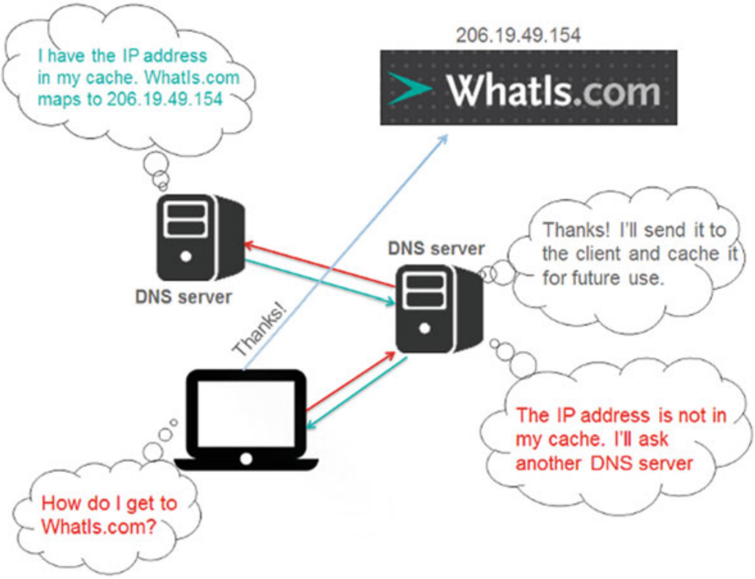
I have the IP address in my cache. WhatIs.com maps to 206.19.49.154
206.19.49.154
WhatIs.com
DNS server
DNS server
Thanks! I'll send it to the client and cache it for future use.
Thanks!
The IP address is not in my cache. I'll ask another DNS server
How do I get to WhatIs.com?

Fig. 5.1 Working of DNS. *Source* SearchSecurity (2018)

distributed denial of service, DNS amplification, and fast flux DNS (SearchSecurity 2018) (Fig. 5.1).

In 2016, the educational organizations in the UK were widely hit by the DNS attack. The UK education network Janet was badly hit by the distributed denial-of-service (DDoS) attack in April 2016 which led to a forty-eight-hour disruption in the access by the apps provided by the university to the students and the teachers. Eleven percent of the educational institutions were affected by the attack. The major reasons of the vulnerability for these types of attacks are (1) Failure in adapting security measures for protecting the DNS; (2) Response to the notifications regarding the vulnerability is not there; (3) The absence of the awareness regarding the different types of security issues which might occur (Voice-online.co.uk 2018).

5.6 Conclusion

The need of providing a good quality of public services is of utmost importance for a developing country like India. Along with this, the cost at which it is provided must be analyzed because a country like India always suffers with a dilemma of providing good services but at a lower cost to ensure economic growth and staying competent among other economies. Going digital provides a framework by which these two things can be matched. The word digital inherently brings along with it the additional concerns related to security. It is because of the ever-evolving threats from the cyber-attackers and hackers who are always on a lookout for breaching the security for monetary benefits or for the purposes relating to destabilizing the existing norms in a civilization. The era of cyber-terrorism has dawned upon due to the evolution of the digital world and dependency on the processes and services arriving due to this, which has opened new avenues of threats. As observed, the digitalization of the Indian public services is leading us to be prone to the cyber security attackers, both within and outside the country. A host of digital initiatives are being taken in India for the provision of public services, these digital initiatives aims at ensuring a superior quality delivery of the service and reduction of the losses which prevails in the existing methods and processes. These developments should always be scrutinized and debated to measure and gauge their preparedness related to the security concerns hovering over them because of the scale and scope at which they operate. The existing state of the public services has been analyzed and the soft spots prevailing there are identified. A further analysis of the existing security practices has been done, which highlights the present measures and mechanisms in place. Examining the preparedness with regard to the existing policies and strategies points that, there are some measures which have a good potential as far as mitigating cyber risk is concerned, but to generalize there is a lot which needs to be done in India to strengthen the very fundamentals of cyber security for keeping the cyber-threats at bay. Further to this, analyzing the previous cyber-attacks both in the Indian and global context provides the pointers onto which stress needs to be given on a priority basis to ensure avoiding their occurence in the future.

5.7 Limitations and Further Research

This study deals with the analysis of the cyber-threats which includes analysis of their causes, their impacts, and the domains in which they can affect. The study is scoped to the analysis of the role of cyber security in "public services" which corresponds only to core public services. The intersections of these services with the services in other domains should be analyzed in order to get a micro-level analysis pertaining to the cause, effect, and prevention of cyber-threats. This will further supplement the enhancement of understanding the role of cyber security.

References

Consultantsreview.com. (2018). *Digital India can't do without the protective wall of cyber security*. [online] Available at https://www.consultantsreview.com/cxoinsights/digital-india-can-t-do-without-the-protective-wall-of-cyber-security-vid-858.html. Accessed February 13, 2018.

Dey, A., & Dey, A. (2018). WannaCry hasn't hurt India's government, but there have been dangerous, unreported attacks before. [online] Scroll.in. Available at https://scroll.in/article/837783/wannacry-what-indias-government-agencies-should-learn-from-the-global-ransomeware-attack. Accessed February 25, 2018.

En.wikipedia.org. (2018a). *Computer security*. [online] Available at https://en.wikipedia.org/wiki/Computer_security. Accessed February 8, 2018.

En.wikipedia.org. (2018b). *Computer security*. [online] Available at https://en.wikipedia.org/wiki/Computer_security. Accessed February 16, 2018.

En.wikipedia.org. (2018c). *Public service*. [online] Available at https://en.wikipedia.org/wiki/Public_service. Accessed February 15, 2018.

Firstpost. (2018). *Why cyber security is important for digital India—Firstpost*. [online] Available at http://www.firstpost.com/business/why-cyber-security-is-important-for-digital-india-2424380.html. Accessed February 23, 2018.

Itgovernance.co.uk. (2018). What is cyber security? *IT Governance.* [online] Available at https://www.itgovernance.co.uk/what-is-cybersecurity. Accessed February 21, 2018.

SearchSecurity. (2018). What is DNS attack? *Definition from WhatIs.com*. [online] Available at http://searchsecurity.techtarget.com/definition/DNS-attack. Accessed March 1, 2018.

Smart, W. (2018). *Lessons learned review of the WannaCry Ransomware cyber attack*. [online] London: Department of Health and Social care. Available at: https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf. Accessed February 22, 2018.

The Centre for Internet and Society. (2018). Cyber security of smart grids in India. [online] Available at https://cis-india.org/internet-governance/blog/dataquest-april-25-2016-vanya-rakesh-and-elonnai-hickok-cyber-security-of-smart-grids-in-india. Accessed Februaary 23, 2018.

Theregister.co.uk. (2018). Indian navy computers stormed by malware-ridden USBs. [online] Available at http://www.theregister.co.uk/2012/07/03/indian_navy_hacked_usbs. Accessed February 25, 2018.

Voice-online.co.uk. (2018). The growing cyber security threat to the UK education sector. [online] Available at http://www.voice-online.co.uk/article/growing-cyber-security-threat-uk-education-sector. Accessed February 22, 2018.