Impact of Smartphones in India – A Whitepaper

Pratik Doshi
Student, Independent Researcher
doship@protonmail.com
https://doship.wixsite.com/home

Abstract

Since the unveiling of the first-ever smartphone in 2009, Apple's iPhone, technology has remarkably penetrated into people's everyday lives in the West, an experience that came to India a little later starting around 2012. The introduction of smartphone technology to India has significant social, political, and security implications given that the county is the second most populous in the world, and that the smartphone, for many of its citizens is their first introduction to internet enabled devices. I present here various adverse effects and risks of Indians' common perceptions of smartphones based upon my research, an in-depth issue analysis, and conclude with some suggested solutions.

1 Smartphone penetration into India

The first smartphone launched in India was called HTC Magic [1], sold by Taiwanese manufacturer HTC in June 2009, just 10 months after Apple's iPhone [2], (named iPhone 3G). It had few key feature differences such as easy-to-use software, better camera and increased compatibility, supporting multiple media formats and a slightly lower price of 30,000 INR ($430 USD) [3] than that of iPhone 3G at 31,000 INR – 36,100 INR ($445 – $518 USD) [4]. To draw a contrast between the first Android run smartphone's specifications and today's Android based smartphones, we have the below table–

Aspects	HTC Magic – 2009 [5]	Today's Android Devices
Networks supported	2G, 3G	3G, 4G, LTE and VoLTE
Android Version	Donut (v1.6)	Nougat (v7), Oreo (v8), Android P (v9)
Camera (Primary)	3.15MP	13MP to 24MP
Video	320p @15fps	720p to 4k @30fps
Price	30,000 INR ($430 USD)	1,500 INR – >65,000 INR

Table 1. Contrast between HTC Magic and today's smartphones

Below table gives us the statistics of total Feature phone and smartphone users in 2009 and in 2018.

Population to Phone Ratio	In 2009	In 2018
Number of Smartphone users of total population (Includes iOS running devices)	2.5 Million mobiles for 1.2 Billion (1,214 Million [6]) = **0.21%** of total population	446 Million mobiles [7] for 1.3 Billion (1,342 Millions) = **33.23%** of total population
Number of Feature phone users	525.1 Million mobiles for 1.2 Billion (1,214 Millions) = **43.25%** of total population	1.21 Billion mobiles [7] for 1.3 Billion (1,342 Millions) = **93.08%** of total population

Table 2. Feature and Smartphone user statistics in India

Indian market witnessed the rise of Smartphones after 2012, partly because Android was free open-source [8] software. Samsung was able to sell their more feature-rich smartphones at a lower price point than Apple, establishing itself as the market leader with over 25% of total smartphone sales in India, helping to usher-in its smartphone boom. The following [9] survey graph illustrates this boom from 2012 to 2017.

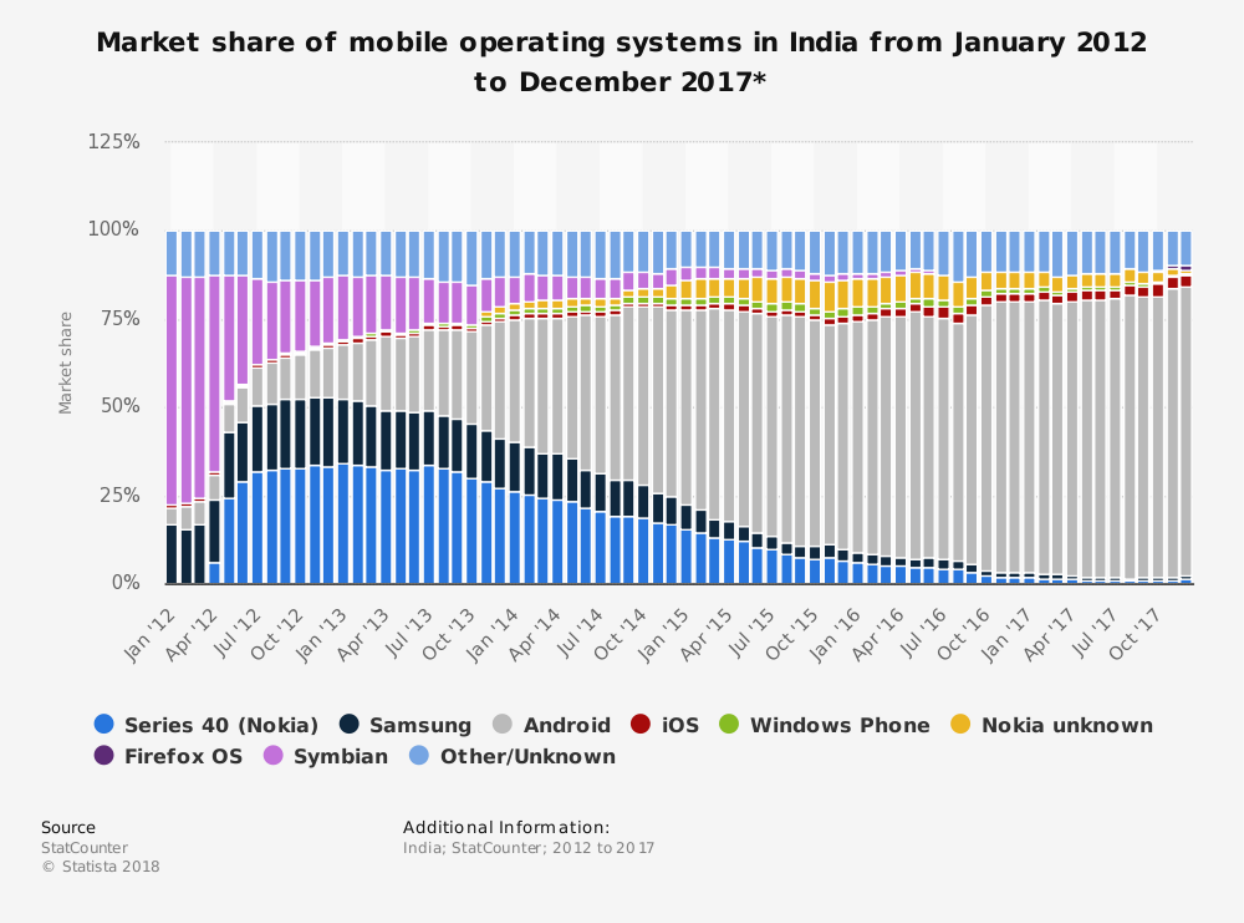

Fig 1. [9] Different Mobile OS used in India from 2012 to 2017

We can clearly see from Fig 1 that at the beginning of 2012 Android held approximately 5% of total smartphone market and that at the end of 2017 had reached 80% with all non-Android OS based smartphones falling in less than 20%. It is worth mentioning that Apple's iOS, the origin of the smartphone industry in America, and still a dominant market player at 22.4% [10], has struggled to find a foothold in India, as the graph indicates, due to its considerably higher cost.

A more recent data point in Fig 2 [10] below shows the smartphone OS used by Indians from June 2017 to June 2018, with android standing first (having maximum devices) at a whopping 89%, putting all other popular OSs out of competition.

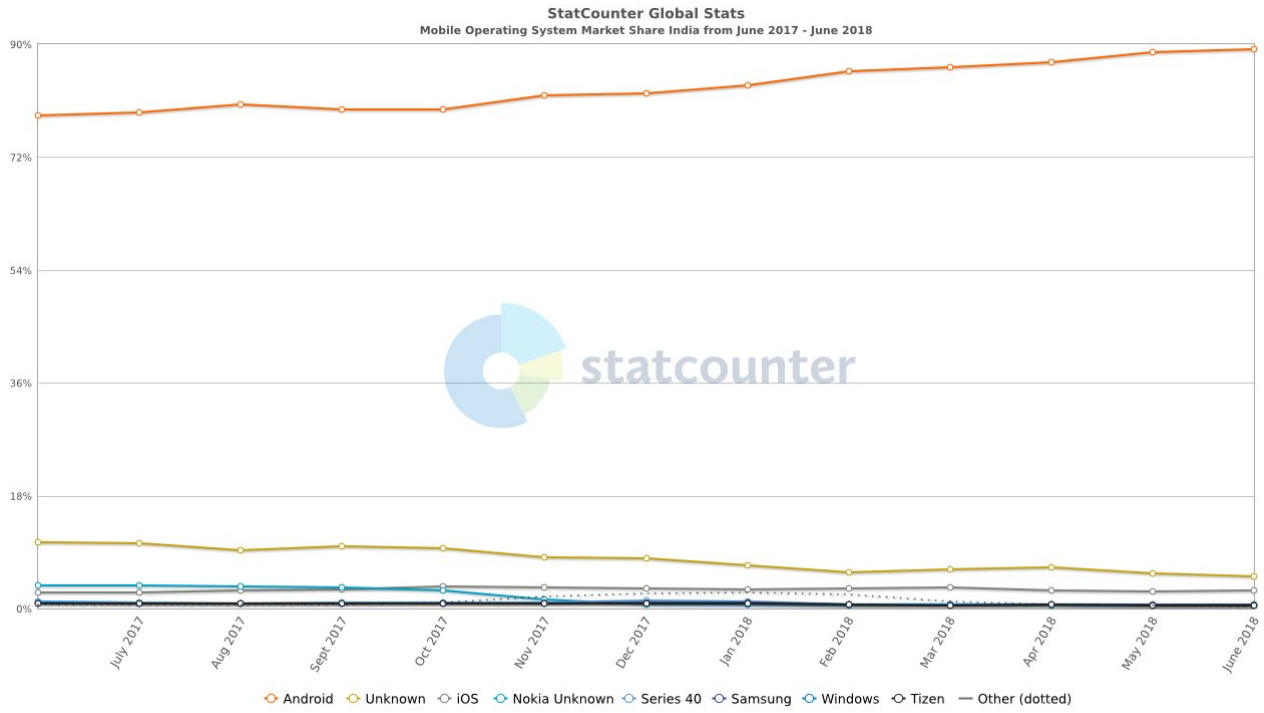

Fig 2. [10] Different Mobile OS used in India from June 2017 to June 2018

The fact that all non-Android based devices comprise somewhere between 11-18% of the Indian market in 2018 strongly suggests that a security analysis of Android devices is paramount in the Indian context.

Legend for Fig 1 and 2:

Series 40 (Nokia) [11]: A feature phone User Interface (UI) by Nokia
Samsung UI: A feature phone UI by Samsung
Android [12]: Mobile OS developed by Android Inc., then acquired by Google LLC
iOS [13]: OS developed by Apple Inc. exclusively for its handheld devices
Symbian [14]: Discontinued OS for Personal Digital Assistants (PDAs) and smartphones.
Windows Phone [15]: A discontinued OS for Windows phone developed by Microsoft
Firefox OS [16]: Discontinued OS for smartphones, tablets and smart TVs designed by Mozilla
Tizen [17]: Mobile OS developed by Linux Foundation that runs on many Samsung devices including smartphones, smart TVs, tablets and in-vehicle infotainments (IVIs).

2 Three Factors for India's Smartphone Revolution

There are many factors why smartphones are becoming mainstream in India. Presented here are three main factors: affordability, usability, and youth trends. These factors are relevant

to a security analyses insofar as they correlate to particular software and usage patterns unique to the country.

2.1. Affordability:

India is a *price sensitive market* [18] which means that the price (cost) of a commodity heavily influences its sales. As mentioned, Android based smartphones can be considerably cheaper than iOS-based smartphones, giving it the edge in affordability and sales that has led to its considerable market lead. And unlike iOS, Android is free and open-source, meaning that any manufacturer can participate in that market by further developing it or customizing it for its own range of devices. Because of this, the country has around a hundred Android based smartphone brands, of which 20 are the most common. These brands focus on making affordable devices to sustain growth against competitors, giving preference to devices retailing between 4,000 to 15,000 INR (~$60 – $250 USD), a price range that appeals to the less wealthy majority in India. The affordability of smartphones has ushered-in an internet revolution in India which did not take place with expensive desktop and laptop computers, as it did in the West from the mid-1990s.

2.2. Usability:

Smartphones have developed to such an extent that they have displaced other technologies that were once common such as clocks and watches, cameras, calculators, compasses, telephones (both landlines and the formerly common VoIP devices), and has led to the decreased use of newspapers, television, music players, and gaming consoles. Many common daily tasks have migrated to the smartphone including socializing, exchanging documents and media, banking, booking tickets, entertainment, looking up information, fitness tracking, etc. Smartphones are also incredibly easy to use, appealing to both young and old, and even overcoming issues of literacy to

a considerable extent --an issue in India where literacy ranges more widely than in the West. Thus, usability has enabled the smartphone to become a central hub of the daily activity of many Indians who can afford one.

The graph below [19] shows what the general Indian population uses smartphones for.

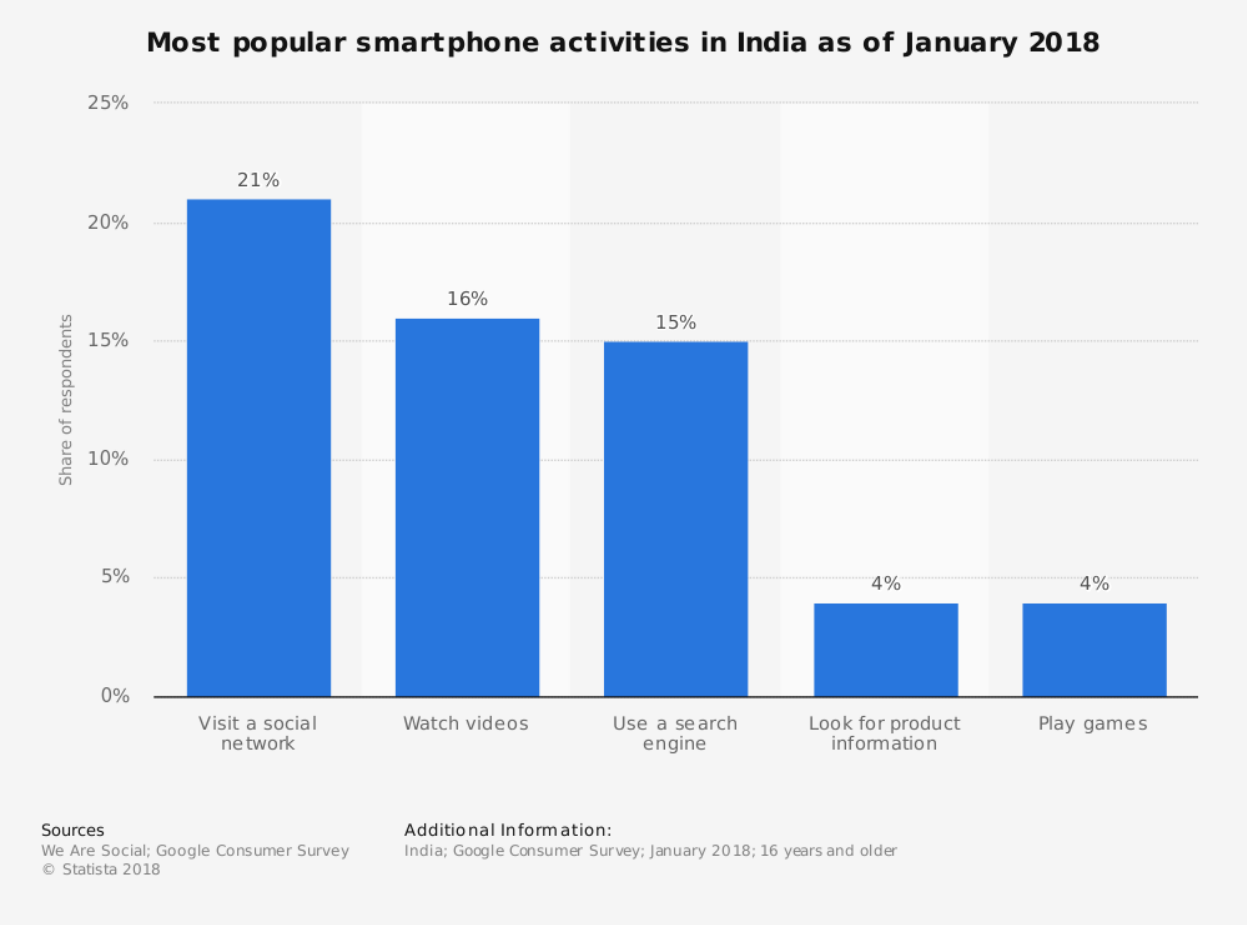

Fig 3. [19] Popular smartphone activities in India as of Jan-2018 across all age groups

2.3. Youth Trends:

Youth aged 14-24 years [20] are a considerable driver of smartphone usage and sales. Although smartphone use remains a minority experience in India with only 446 million [7] devices in a country of 1.3 billion people, youth have more exposure to smartphones than the general

population. They are more inclined to notice and play with the devices borrowed from those around them. Seeing smartphones as the trendy technology, youngsters beg their parents to buy them one. They are also very interested in participating on social media especially on *WhatsApp* [21], *Facebook* [22] and *Messenger* [23], *Snapchat* [24], on video sites like *YouTube* [25] and *Hotstar* [26], and on the latest trending apps like *TikTok* [27] (formerly *Musical.ly*); and for the young adults, dating and hookup apps like *Tinder* [28] and *Grindr* [29]. As in the West, socialization is increasingly taking place through apps like these, and Indian youth feel that more intensely than the older generations. Smartphone video games are also a special temptation for youth, especially boys, who play games like *Subway Surfer* [30], *Candy Crush Saga* [31] to *PUBG* [32] and *Asphalt 8 – Airborne* [33], *Asphalt 9: Legends* [34] etc. Although only 11% [35] (updated April 2019) of smartphone use is dedicated to video games for the general population, for youth (<24 years) the percentage is considerably higher at 55% and 66% of casual gamers and heavy gamers respectively [36].

These factors – affordability, usability, and youth trends – also paint a preliminary picture of the emerging information security trends in India. For example, cheaper phones tend to be loaded with older, less up to date software which could be vulnerable to hackers. Because the affordability and usability of smartphones leapfrogged the desktop revolution of the West, many Indian users will be less aware of the security implications of their technology use and of security practices that are more commonly known in the West. These include protection practices like encryption and secure wiping, software updating and upgrading, and simply being less inclined to hand over one's information to these devices, apps, and websites – although that may be a contested point given the universality of Facebook and other such socializing sites. Although, youth are better positioned to learn the technical and security aspects of their device use, most will not. And

so, the general emerging security picture is unfortunately one of more vulnerable devices in the hands of a more vulnerable population.

3 Public Perception of Smartphone Technology Risks

The common public perception in India towards the smartphone is that it's a magical device which gives its users access to anything they want: a plethora of multimedia (audio & video), the power and pleasures of surfing the internet, social media, games, and all the features of feature phones. Very few Indian smartphone users have a deeper insight into the hardware or software functions of their devices.

Many believe that internet is comprised of only WhatsApp, Facebook, YouTube, Google, and a few other apps and websites. They are generally much less aware of a wider internet and what it offers, much as *AOL* [37] Online users in the mid-late 1990s could not see what was beyond their digital walled garden. In general, Indian users lack a broader perspective about their activities online, and its consequences. Indian smartphone users have increased their monthly internet usage from 0.062GB (62MB) [38] in 2014 to 7.4GB [39] in 2017, with 1.3 billion GB alone being wireless internet used by smartphones (in 2017) [40].

The social media obsession leads smartphone users to update everything they do in their day-to-day life on their social media profiles. This activity leaves more and more information about these users exposed on the internet where it can be accessed and used by others, not only by friends and family as users naively think, but also by personal enemies, political opponents, nefarious corporate interests, hackers, organized crime, a censorious government, and even foreign agencies. From cyber-bullying to catfishing, from ransomware to kidnapping plots, from cyber-stalking to cyber-espionage, social media users expose themselves to many information-based threats that are

further exacerbated by the ever-renewing flood of technical vulnerabilities of these apps and websites.

Few Indian smartphone users are sophisticated enough to manage these risks, and most who fall into trouble will do so unwittingly. These risks become more significant as Indians use more networked devices like smartphones, they become more vulnerable to information-based attacks.

A few brief stories can give an indication of what is at stake for Indians. Some of these risks are more common in Indian than in the West. For example:

3.1. Posting way too much information:

Giving away information on online portals, blogs, social media pages and giving more than necessary information when requested, especially on social media sites. It is commonly observed that many Indians post their personal phone numbers, pictures with geotagging [41] and many such private data on public comments without knowing its security implications and unknown to the risk that it can be used by anyone who comes across it for their various means.

3.2. Posting all your whereabouts on social platform:

Posting timely personal whereabouts commonly called as live status, where people post streaks of pictures which automatically will be unavailable on their timeline in the next 24 hours. This is a personal story of a friend's neighbor, where the couple was living with their kid who was just enrolled in primary school. On the first day of school, mother took a picture of the kid with details regarding school's name and address (geotag) and posted it on her Facebook wall. Later realizing that the kid was missing post school hours and soon they got threatening calls asking for ransom

to bail out the kid. The cost of their post on Facebook was both the danger to the child's life and the ransom they paid.

3.3. Political and religious strife conducted online:

People with political/religious affiliations or views can be baited into conflict with groups having contradictory views. This might eventually result in online harassment, that can lead to real world violence between real world communities.

4 Technical Vulnerabilities

Smartphones are complicated devices. Technical flaws in software and hardware design and implementation cannot be avoided. These technical vulnerabilities can lead to data breaches, some of them large scale, and potentially disastrous.

In recent years the world has seen many cyber-attacks targeting people's data on the internet, including the 2015 Target credit card leak, the 2017 Equifax data breach, the WannaCry and Petya/Non-Petya ransomware in 2017. In the last decade these types of attacks have been increasing in India as well. A report from Indian Computer Emergency Response Team (CERT-In) [42] has confirmed that by the mid-June of 2017, India has witnessed over 27000 different cyber-attacks and taking a toll at 0.7 million [43] within the first half of 2018. Here are other relevant details:

- India ranked *5th most vulnerable* country to cyber security breaches [44].
- Indian companies, both large and mid-sized, on an average *lose $10.3 Million USD (71.5 crores INR) to $0.011 Million USD (0.76 crores INR)* respectively to cyber-attacks annually [45].

- Most (~70%) [46] mobile *banking apps and* 49 out of 50 top *Indian e-commerce apps are vulnerable* to breaches/attacks [47].
- India accounts for *30-35% of total global mobile malware attacks* annually [48].

Some well-known Indian data breaches affecting or involving smartphones are the Aadhaar PII (Personally Identifiable Information) and biometrics breach (2017-2018), Paytm's root access breach (2017) [49], the Zomato Hack (2017) [50], the Indigo Twitter hack (2017) [51], the multiple hacks of Indian Railways (IRCTC) (2014-2017).

Attacks on banking apps may also involve smartphone vulnerabilities. In 2016 Indian banks were attacked by malware injection through debit cards, compromising 3.2 million debit cards [52] from most major banks of India. More recently in 2018, a bank in Pune – Cosmos Bank – was targeted by an organized criminal attack using cloned debit cards, causing a loss of 940 million INR ($13.5 million USD) [53]. Let us examine these Indian data breaches in more detail.

4.1. Paytm requesting root access [49]

Paytm is an India-based mobile payments e-wallet app. A vulnerability discovered by Bibhas Debnath [54] and later exposed by Robert Baptiste [55] in 2017 revealed that the app requested root (superuser) access, enabling the app to access everything on a user's smartphone, such as contacts, photos, location data, and application data of other apps without a user's consent. In addition to the privacy concerns this gave rise to, Paytm's rooting of the phone created a major backdoor for malware and spyware. Paytm later addressed the complaints, stating that the National Payments Corporation of India (NPCI) asked it to request for root access in rooted phones, claiming the NPCI wanted to know if users of jailbroken smartphones were using fake credit and

debit cards to make various Paytm purchases. Paytm engineers later updated the app's configuration file so it did not ask its users to give the app root access just within 4 days.

4.2. Zomato data breach [50]

In 2017, Zomato, one of India's largest food delivery companies, faced a major data breach, a hack claimed by an individual known as *nclay*. The reports stated that data of around 17 million users was stolen, including emails and passwords which could then be used to access user's Zomato profile containing further personal information like phone number, GPS location, payment options including debit and credit card details etc.

4.3. Indian Railways (IRCTC) hacks

The Indian Railways IRCTC website, run by the Indian government, is the largest Indian e-commerce website used for the booking of train tickets and facilitates the booking of bus and plane tickets, hotels, and other travel-related services. Over the past few years, this website has been in the news due to the many breaches and hacks that effected it. In 2016 it was hacked by a group of hackers and the target was the consumer data [56]. Another event included a hacker generating fake tickets [57]. In the first incident, personal data of around 1 crore users was breached. In the second case a hacker's cover was blown up by CBI, revealing that he used the IRCTC website to generate fake tickets and make money off people he was scamming with those fake tickets. These ongoing security breaches prove that the security of government services is no less vulnerable than that of private companies.

4.4. Aadhaar breach:

Aadhaar is the Indian national biometric database implemented in 2009 notable for being pushed by government edict as a requirement for nearly every aspect of Indian daily life, including

the purchase of mobile SIM cards, opening a bank account, taking privileges of government subsidiaries and even admission into schools, making it as the most common ID proof at an international scale. However, some of these requirements were lifted by the Indian Supreme Court in late 2018 [58]. As the world's largest public biometric collection program, Aadhaar has been highly controversial due to its security mismanagement and has been receiving negative attention since last couple years.

In 2017 Robert Baptiste [59] revealed a vulnerability in the mAadhaar app [60] which enabled ordinary smartphone users to gain access to a developer's database that leaked Aadhaar personal details, contradicting government claims that the Aadhaar project was secure. Baptiste also revealed that the Aadhaar password system was flawed because the password is generally a random string of numbers as a seed and a hardcoded string, which is very easy to guess or break in. These flaws at the time gave easy access to sensitive personal Aadhaar data including encoded biometric details, "know your customer" (KYC) details required for banking and other sensitive financial transactions, user passwords, and app configuration details including address, GPS locations from where they are accessing the app, and IP address.

In January 2018 [61], there were allegations encompassing that a billion Aadhaar account details were breached and easily available. Reports even say that the hackers produced fake Aadhaar cards and sold them on WhatsApp for 500 INR ($7.18 USD). These cards were used to open fake bank accounts, obtain PAN (personal account number, similar to a social insurance number in the United States) cards and SIM cards for mobile phones. Whereas critics and public focused on potentially negative privacy outcomes, in these cases government officials continued to defend Aadhaar as being the most secure database and denied [62] all claims of such hacks or breaches.

This leaves an open question: If the – so called – "most secure" information initiative by the Indian government exhibits so many flaws, what can we expect for the nation's security as a whole? Are there really any consequences in India for allowing insecure software involving personally sensitive information to be used by the public?

The list below [63] shows many other cyber-attacks which targeted India's government portals and some private companies, their impacts, attack types and reason behind those hacks.

Sector	Impact	Attack type	Reason behind the hack
Telecom Regulatory Authority of India (TRAI) [64]	Website hacked. 1 million email IDs	DDOS attack	Net-neutrality movement
Indian Army's - Principal Comptroller of Defence Accounts (Officers) portal [65]	Website hacked	Unknown/Not shared	Army officials' financial details stolen
Jawaharlal Nehru University Library [66]	Website hacked and defaced	Unknown	To create political conflicts
Orissa University of Agriculture and Technology [67]	Website hacked	Unknown/Not shared	Unknown
Indian Space Research Organization (ISRO) [68]	Website of ISRO's commercial arm "Antrix" was hacked	Confidential	Confidential
Kerala Government website [69]	Website hacked	Unknown	To threaten
Central Bureau of Investigation (CBI) - considered as one of	Website hacked	Confidential	To threaten

the most secure websites of India [70]			
Indian Embassy website (of 7 countries) [71]	Website hacked	SQL Injection	Details of Indians living abroad were leaked
Aadhaar Website and mobile app (mAadhaar) [60]	Data breach	Unknown	Personal details, biometric data was sold and to generate revenue using advertisements
Indian Registry for Internet Names and Numbers (IRINN) [72]	Data breach	Cyber Espionage/Ransom	Critical data owned by organizations was exposed, effecting over 6000 ISPs
Reliance Jio [73]	Data breach	Unauthorized access	Unauthorized access to Reliance Jio servers
Air Indigo [74]	Twitter handle hijacked	Unknown	Defamation by public abuse
Electra Card [75] and EnStage [76]	Data breach	Unknown	45 Million USD stolen from ATM machines worldwide
ATM debit card breach [77] of major Indian banks	Data breach	Malware injection	3.2 Million Debit card details were stolen

Table 3. [63] List to cyber-attacks targeting Indian companies and governmental organizations

5 Strategic solutions

Looking at these, reports suggest India is highly vulnerable to cyber-attacks. Bearing the responsibility to the lives of 1.3 billion people, the Indian state has a responsibility to be able to

develop its cybersecurity strategy and culture. It should be able to withstand such attacks on its crucial data and should also be able to fight back in this space. India's capabilities should be at par with the USA, UK, China and Russia. To attain this magnitude, I suggest a few steps to start with:

5.1. Government Infrastructure:

Government should focus on strengthening and improvising its infrastructure as well as its workforce. This can strengthen public data which is controlled by government such as Aadhaar biometric data, various subsidies, data flowing through IRCTC and many other such websites and reducing foreign threats to Indian intelligence agencies.

5.2. Economic/Market leverage strategy:

India has a very large market and an ever-growing scope for new products and innovations. Using India's market size and capability to produce indigenous solutions, mainly to produce social apps, enabling less interference of foreign countries/companies. This enables the data (public's publicly available data) to stay inside the country itself and not be dependent of foreign policies or sanctions. This will enable and enforce Indians to use indigenous substitutes to social media (where most of the personal data is available freely) such as Yandex [78], VK [79] in Russia and Baidu [80], WeChat [81] in China and replace social apps like Facebook, WhatsApp and Google's search engine.

5.3. Educational upskilling:

India lacks educational balance between different types of skills due to limited educational options / degrees / certifications to choose from. Embedding Cybersecurity as a subject in educational system throughout the country's schools would appeal many students to choose career in cybersecurity. Adding specialized certifications would open another plethora of

options for individuals to explore. Gaining skills in this field will also improve employment options, hence answering another major problem of India, unemployability.

5.4. Developing Hacker culture:

India has a miniscule hacker culture till date and a few scattered professionals. Introducing hacker culture in India by conducting hackathons, bug bounty programs, crypto and encryption conferences and various other competitions would be both, a great learning and a skillful practical environment for its participants. This also will interest a wide audience and not just the participants and investors, enabling growth in revenue which can then be invested back in this community.

5.5. Public Education:

Creating awareness among people will certainly make them think about the probable consequences of their data privacy, their social media habits and their online presence. This will make them apt towards any such problem they may face. Educating people around such threats via counseling and advertisements is a must.

However, there is a bigger picture of India's cybersecurity situation than these five solutions can answer for, which cannot be neglected. India lacks large scale semiconductor manufacturing companies, that can make and provide for India's rising electronic gadget (smartphones, smart TVs, computers etc.) needs. Due to lack of semiconductor processes in India, it cannot make its own chips to run on devices and hence relies on other companies such as Intel [82], AMD [83] for it. These chips come equipped with Intel Management Engine (IME) [84] or AMD Platform Security Processor (AMD PSP) [85] respectively which can access a device remotely without any permission of the user bypassing any hardware and

software security levied by the user or the OS of that device giving it ‘Ring 0 Access’ [86]. Using this Ring 0 Access, one can access the ‘baseband processor’ [87] to give them access to the entire device via radio enable wireless network. This can cause serious damage to one’s personal data and can be exploited / mined without any limit. If these chips are continued to be used as they’re now, India will be the consumer/slave of security decisions, intentions and sanctions of foreign companies, countries and even criminals. Hence a large-scale semiconductor manufacturing company is the need and the answer to secure India’s devices.

6 Conclusion – Intent/Foreword

It is a saddening truth that India’s young population is giving away a lot of its precious time and data to these smartphones mostly in socializing and gaming and have become so addicted that prolonged distance between their smartphones and them is creating a psychological pattern of anger and stress. By using these social media apps, they’re unaware of the security threats that are posed against them. Their data being easily available and accessible through social media puts them in a high risk as someone out in the world (whom they might not even know) is looking at all their personal data without their consent. This can influence a person’s life in a very distinctive number of ways. By giving one’s own details not only one enters in the self-created zone of mass surveillance but also gives up on our personal privacy. The worst of all, many don’t have the slightest clue about the whole data consumption process by social media apps. Today these apps have become a strong base for surveillance, social engineering and identity thefts by requesting all types of permissions to capture your personal data, from your photos to your contacts, from your GPS location to your last mobile payment, from your mood to your debit/credit card details.

References

[1] Radhakrishnan Abhimanyu, The Economic Times, 'First Android Phone in India launched today', June 23, 2009. [Online]. Available: https://economictimes.indiatimes.com/tech/hardware/first-android-phone-in-india-launched-today/articleshow/4689118.cms. [Accessed: September 23, 2018].

[2] Wikipedia Contributors, Wikipedia: The free Encyclopedia (Wikipedia.org), 'iPhone 3G', May 17, 2019. [Online]. Available: https://en.wikipedia.org/wiki/IPhone_3G. [Accessed: May 30, 2019].

[3] Amitash, DifferenceBetween.net, 'Difference Between iPhone and HTC Magic', January 9, 2018. [Online]. Available: http://www.differencebetween.net/object/gadgets-object/difference-between-iphone-and-htc-magic/. [Accessed: May 30, 2019].

[4] Naveen Athresh, Globonomics!, 'iPhone 3G all set to be launched on 22nd Aug 2008 in India', August 20, 2008. [Online]. Available: https://ecofin.wordpress.com/2008/08/20/iphone-3g-all-set-to-be-launched-on-22nd-aug-2008-in-india/. [Accessed: May 30, 2019].

[5] Wikipedia Contributors, Wikipedia: The free Encyclopedia (Wikipedia.org), 'HTC Magic', August 19, 2018. [Online]. Available: https://en.wikipedia.org/wiki/HTC_Magic. [Accessed: September 24, 2018].

[6] Google public data, Google.com, World Bank, 'Population', July 6, 2018. [Online]. Available: https://www.google.com/publicdata/explore?ds=d5bncppjof8f9_&met_y=sp_pop_totl&idim=country:IND. [Accessed: September 25, 2018].

[7] Wikipedia Contributors, Wikipedia: The free Encyclopedia (Wikipedia.org), 'Internet in India', September 25, 2018. [Online]. Available: https://en.wikipedia.org/wiki/Internet_in_India. [Accessed: September 28, 2018].

[8] Wikipedia Contributors, Wikipedia: The free Encyclopedia (Wikipedia.org), 'Open-source software', October 6, 2018. [Online]. Available: https://en.wikipedia.org/wiki/Open-source_software. [Accessed: October 9, 2018].

[9] Statista.com, 'Market share of mobile operating systems in India from January 2012 to December 2017', October 9, 2018. [Online]. Available: https://www.statista.com/statistics/262157/. [Accessed: October 9, 2018].

[10] Statcounter.com, 'Mobile Operating System Market Share Worldwide', October 15, 2018. [Online]. Available: http://gs.statcounter.com/os-market-share/mobile/worldwide. [Accessed: October 15, 2018].

[11] Wikipedia Contributors, Wikipedia: The free Encyclopedia (Wikipedia.org), 'Series 40', October 7, 2018. [Online]. Available: https://en.wikipedia.org/wiki/Series_40. [Accessed: October 17, 2018].

[12] Wikipedia Contributors, Wikipedia: The free Encyclopedia (Wikipedia.org), 'Android (operating system)', October 26, 2018. [Online]. Available: https://en.wikipedia.org/wiki/Android_(operating_system). [Accessed: October 26, 2018].

[13] Wikipedia Contributors, Wikipedia: The free Encyclopedia (Wikipedia.org), 'iOS', October 28, 2018. [Online]. Available: https://en.wikipedia.org/wiki/IOS. [Accessed: October 28, 2018].

[14] Wikipedia Contributors, Wikipedia: The free Encyclopedia (Wikipedia.org), 'Symbian', November 4, 2018. [Online]. Available: https://en.wikipedia.org/wiki/Symbian. [Accessed: November 5, 2018].

[15] Wikipedia Contributors, Wikipedia: The free Encyclopedia (Wikipedia.org), 'Windows Phone', November 6, 2018. [Online]. Available: https://en.wikipedia.org/wiki/Windows_Phone. [Accessed: November 6, 2018].

[16] Wikipedia Contributors, Wikipedia: The free Encyclopedia (Wikipedia.org), 'Firefox OS', July 23, 2018. [Online]. Available: https://en.wikipedia.org/wiki/Firefox_OS. [Accessed: November 7, 2018].

[17] Wikipedia Contributors, Wikipedia: The free Encyclopedia (Wikipedia.org), 'Tizen', November 7, 2018. [Online]. Available: https://en.wikipedia.org/wiki/Tizen. [Accessed: November 8, 2018].

[18] Sumeet Goyal, LinkedIn SlideShare network, 'Price Sensitivity of Indian Consumers', March 17, 2014. [Online]. Available: https://www.slideshare.net/sumeetgoyal3/price-sensitivity-of-indian-consumers. [Accessed: November 14, 2018].

[19] Statista.com, 'Most popular smartphone activities in India as of January 2018', November 21, 2018. [Online]. Available: https://www.statista.com/statistics/309867/. [Accessed: November 21, 2018].

[20] Livemint, www.livemint.com, 'Smartphone demographics', July 29, 2015. [Online]. Available: https://www.livemint.com/Home-Page/DMsLNQaN3gqtgO9rHbwtAJ/Smartphone-demographics.html. [Accessed: November 23, 2018].

[21] Wikipedia Contributors, Wikipedia: The free Encyclopedia (Wikipedia.org), 'WhatsApp', September 20, 2018. [Online]. Available: https://en.wikipedia.org/wiki/WhatsApp. [Accessed: September 26, 2018].

[22] Wikipedia Contributors, Wikipedia: The free Encyclopedia (Wikipedia.org), 'Facebook', October 2, 2018. [Online]. Available: https://en.wikipedia.org/wiki/Facebook. [Accessed: October 3, 2018].

[23] Wikipedia Contributors, Wikipedia: The free Encyclopedia (Wikipedia.org), 'Facebook Messenger', October 13, 2018. [Online]. Available: https://en.wikipedia.org/wiki/Facebook_Messenger. [Accessed: October 22, 2018].

[24] Wikipedia Contributors, Wikipedia: The free Encyclopedia (Wikipedia.org), 'Snapchat', October 30, 2018. [Online]. Available: https://en.wikipedia.org/wiki/Snapchat. [Accessed: October 31, 2018].

[25] Wikipedia Contributors, Wikipedia: The free Encyclopedia (Wikipedia.org), 'YouTube', November 1, 2018. [Online]. Available: https://en.wikipedia.org/wiki/YouTube. [Accessed: November 1, 2018].

[26] Hotstar, www.hotstar.com, 'Hotstar', November 22, 2018. [Online]. Available: https://www.hotstar.com/about-us. [Accessed: November 22, 2018].

[27] Wikipedia Contributors, Wikipedia: The free Encyclopedia (Wikipedia.org), 'TikTok', December 27, 2018. [Online]. Available: https://en.wikipedia.org/wiki/TikTok. [Accessed: December 27, 2018].

[28] Wikipedia Contributors, Wikipedia: The free Encyclopedia (Wikipedia.org), 'Tinder (app)', January 2, 2019. [Online]. Available: https://en.wikipedia.org/wiki/Tinder_(app). [Accessed: January 14, 2019].

[29] Wikipedia Contributors, Wikipedia: The free Encyclopedia (Wikipedia.org), 'Grindr', January 24, 2019. [Online]. Available: https://en.wikipedia.org/wiki/Grindr. [Accessed: January 25, 2019].

[30] Wikipedia Contributors, Wikipedia: The free Encyclopedia (Wikipedia.org), 'Subway Surfers', February 9, 2019. [Online]. Available: https://en.wikipedia.org/wiki/Subway_Surfers. [Accessed: February 12, 2019].

[31] Wikipedia Contributors, Wikipedia: The free Encyclopedia (Wikipedia.org), 'Candy Crush Saga', February 25, 2019. [Online]. Available: https://en.wikipedia.org/wiki/Candy_Crush_Saga. [Accessed: February 25, 2019].

[32] Wikipedia Contributors, Wikipedia: The free Encyclopedia (Wikipedia.org), 'PlayerUnknown's Battlegrounds', March 25, 2019. [Online]. Available: https://en.wikipedia.org/wiki/Pubg. [Accessed: March 26, 2019].

[33] Wikipedia Contributors, Wikipedia: The free Encyclopedia (Wikipedia.org), 'Asphalt 8: Airborne', April 7, 2019. [Online]. Available: https://en.wikipedia.org/wiki/Asphalt_8:_Airborne. [Accessed: April 11, 2019].

[34] Wikipedia Contributors, Wikipedia: The free Encyclopedia (Wikipedia.org), 'Asphalt 9: Legends', March 31, 2019. [Online]. Available: https://en.wikipedia.org/wiki/Asphalt_9:_Legends. [Accessed: April 11, 2019].

[35] Statista, Statista.com, 'Mobile Games', November 23, 2018. [Online]. Available: https://www.statista.com/outlook/211/119/mobile-games/india. [Accessed: November 23, 2018].

[36] Statista, Statista.com, 'Online gaming in India - Statistics and facts', November 24, 2018. [Online]. Available: https://www.statista.com/topics/4639/. [Accessed: November 24, 2018].

[37] Wikipedia Contributors, Wikipedia: The free Encyclopedia (Wikipedia.org), 'AOL', April 3, 2019. [Online]. Available: https://en.wikipedia.org/wiki/AOL. [Accessed: April 12, 2019].

[38] PTI (Press Trust of India), The Economic Times: ET Telecom, 'Data tariffs fall 93% in last three years: Telecom department', March 29, 2018. [Online]. Available: https://telecom.economictimes.indiatimes.com/news/data-tariffs-fall-93-in-last-three-years-telecom-department/63537339. [Accessed: November 28, 2018].

[39] PTI (Press Trust of India), The Economic Times, 'Average mobile data usage at 11GB a month: Nokia', February 22, 2018. [Online]. Available: https://economictimes.indiatimes.com/tech/internet/average-mobile-data-usage-at-11gb-a-month-nokia/articleshow/63032695.cms. [Accessed: November 29, 2018].

[40] Livemint's Writer, www.livemint.com, 'Internet Trends report underscores India’s mobile obsession, Jio disruption', June 2, 2017. [Online]. Available: https://www.livemint.com/Technology/ssczejSaUSVHRpaiRgPLYM/Internet-Trends-Report-highlights-Indias-mobile-obsession.html. [Accessed: December 8, 2018].

[41] Wikipedia Contributors, Wikipedia: The free Encyclopedia (Wikipedia.org), 'Geotagging', February 6, 2019. [Online]. Available: https://en.wikipedia.org/wiki/Geotagging. [Accessed: May 30, 2019].

[42] Salman SH, Medianama, '27, 482 cyber security threat incidents in India till June 2017: CERT-In', July 25, 2017. [Online]. Available: https://www.medianama.com/2017/07/223-india-witnessed-27482-cyber-security-threat/. [Accessed: December 8, 2018].

[43] PTI (Press Trust of India), The Economic Times, 'India witnessed over 6.95 lakh cyberattacks from Russia, US, others in January-Jun: F-Secure', November 11, 2018. [Online]. Available: https://economictimes.indiatimes.com/tech/internet/india-witnesses-over-4-36-lakh-cyberattacks-from-russia-us-others-in-jan-jun-f-secure/articleshow/66575477.cms. [Accessed: December 9, 2018].

[44] Bala Chauhan, Deccan Chronicle, 'India, 5th most vulnerable to cyber attacks', September 3, 2017. [Online]. Available: https://www.deccanchronicle.com/nation/current-affairs/030917/india-5th-most-vulnerable-to-cyber-attacks.html. [Accessed: December 10, 2018].

[45] Pymnts Editor, pymnts.com, 'Microsoft: India Cos Lose $10.3M From Cyberattacks Annually', December 6, 2018. [Online]. Available: https://www.pymnts.com/news/security-and-risk/2018/microsoft-india-financial-loss-cyberattack/. [Accessed: December 19, 2018].

[46] Vaishnavi Kanekal, Trak.in, '70% Of The Mobile Banking Android Apps Are Vulnerable: Appvigil', September 29, 2017. [Online]. Available: https://trak.in/mobile-banking-android-apps-vulnerable/. [Accessed: December 20, 2018].

[47] Mohul Ghosh, Trak.in, '49 Out Of Top 50 Indian Ecommerce Applications Are Vulnerable To Attacks [Wake Up Call]', September 26, 2017. [Online]. Available: https://trak.in/indian-ecommerce-apps-vulnerable-attacks/. [Accessed: December 23, 2018].

[48] Dibyendu Mondal, The Sunday Guardian, 'Smartphones prone to cyber threats', April 27, 2018. [Online]. Available: https://www.sundayguardianlive.com/news/11878-smartphones-prone-cyber-threats. [Accessed: December 23, 2018].

[49] Siladitya Ray, Medianama, 'Update: Paytm stops asking for root access on Android devices', March 9, 2018, Updated: March 13, 2018. [Online]. Available: https://www.medianama.com/2018/03/223-paytm-root-access/. [Accessed: January 10, 2019].

[50] Anu Thomas, ET Online, The Economic Times, 'Zomato hacked: Security breach results in 17 million user data stolen', May 19, 2017. [Online]. Available: https://economictimes.indiatimes.com/small-biz/security-tech/security/zomato-hacked-security-breach-results-in-17-million-user-data-stolen/articleshow/58729251.cms. [Accessed: January 17, 2019].

[51] Nandini Yadav, BGR (Boy Genius Report): www.bgr.in, 'IndiGo Airlines confirms its Twitter handle was hacked', January 31, 2017. [Online]. Available: https://www.bgr.in/news/indigo-airlines-confirms-its-twitter-handle-was-hacked/. [Accessed: March 30, 2019].

[52] Saloni Shukla and Pratik Bhakta, ET Bureau, The Economic Times, '3.2 million debit cards compromised; SBI, HDFC Bank, ICICI, YES Bank and Axis worst hit', October 20, 2016. [Online]. Available: https://economictimes.indiatimes.com/industry/banking/finance/banking/3-2-million-debit-cards-compromised-sbi-hdfc-bank-icici-yes-bank-and-axis-worst-hit/articleshow/54945561.cms. [Accessed: December 27, 2018].

[53] Nadeem Inamdar, Hindustan Times, '15, 000 transactions in 7 hrs: Cosmos Bank’s server hacked, Rs 94 cr moved to Hong Kong', August 14, 2018. [Online]. Available: https://www.hindustantimes.com/india-news/15-000-transactions-in-7-hrs-cosmos-bank-s-server-hacked-rs-94-cr-moved-to-hong-kong/story-wazUXZs3LRhcbPLg7LYx5O.html. [Accessed: January 9, 2019].

[54] Bibhas Debnath, Twitter: www.twitter.com, 'Personal Tweet from: @bibhasdn', March 8, 2018. [Online]. Available: https://twitter.com/bibhasdn/status/971724658042163201. [Accessed: January 15, 2019].

[55] Elliot Alderson, Twitter: www.twitter.com, 'Personal Tweet from: @fs0c131y', March 8, 2018. [Online]. Available: https://twitter.com/fs0c131y/status/971802119346016256. [Accessed: January 16, 2019].

[56] India Today Web Desk, India Today, 'IRCTC website hacked, information of around 1 crore people feared stolen', May 5, 2016. [Online]. Available: https://www.indiatoday.in/india/story/irctc-website-hacked-information-of-around-1-crore-feared-stolen-321712-2016-05-05. [Accessed: January 18, 2019].

[57] PTI (Press Trust of India), India Today, 'Hacked IRCTC website, made lakhs selling fake tickets before CBI got him', April 29, 2016. [Online]. Available: https://www.indiatoday.in/india/story/hacked-irctc-website-made-lakhs-selling-fake-tickets-before-cbi-got-him-320742-2016-04-29. [Accessed: January 22, 2019].

[58] ET Online, ET Online, The Economic Times, 'What's valid and what's not: Everything you need to know about Aadhaar verdict', September 26, 2018. [Online]. Available: https://economictimes.indiatimes.com/news/politics-and-nation/whats-valid-and-whats-not-everything-you-need-to-know-about-todays-aadhaar-verdict/articleshow/65961427.cms. [Accessed: January 29, 2019].

[59] Elliot Alderson, Twitter: www.twitter.com, 'Twitter Profile of @fs0c131y', June 1, 2015. [Online]. Available: https://twitter.com/fs0c131y. [Accessed: April 20, 2019].

[60] Elliot Alderson, Twitter: www.twitter.com, 'Personal Tweet from: @fs0c131y', January 10, 2018. [Online]. Available: https://twitter.com/fs0c131y/status/951154909189230593. [Accessed: January 30, 2019].

[61] Soumik Ghosh, www.csoonline.in, 'Alleged breach compromises a billion Aadhaar accounts; govt in denial mode', January 5, 2018. [Online]. Available: https://www.csoonline.in/news/alleged-breach-compromises-billion-aadhaar-accounts-govt-denial-mode. [Accessed: February 3, 2019].

[62] BusinessToday.In, Business Today: India Today, 'Big data breach! Aadhaar software hack raises major security concerns', September 11, 2018. [Online]. Available: https://www.businesstoday.in/current/economy-politics/aadhaar-software-hack-uidai-data-ghost-entries/story/282260.html. [Accessed: February 10, 2019].

[63] Fire Compass, www.firecompass.com, 'Overview of Top CyberSecurity Breaches In India: CyberSec-Breaches-in-India-Report.pdf', October 11, 2017. [Online]. Available: https://www.firecompass.com/wp-content/uploads/2017/10/CyberSec-Breaches-in-India-Report.pdf. [Accessed: February 17, 2019].

[64] Tech Desk, The Indian Express: Express Tech, 'Net Neutrality: Anonymous brings down TRAI website after 1mn email IDs made public', April 28, 2015. [Online]. Available: https://indianexpress.com/article/technology/social/net-neutrality-trais-website-hacked-by-anonymous-after-regulator-makes-1-mn-email-ids-public/. [Accessed: February 26, 2019].

[65] Chandan Nandy, The Times of India, 'Army officers panic as hackers steal secret data', April 9, 2015. [Online]. Available: https://timesofindia.indiatimes.com/india/Army-officers-panic-as-hackers-steal-secret-data/articleshow/46856789.cms. [Accessed: February 26, 2019].

[66] Aranya Shankar, The Indian Express, 'Hackers deface JNU library website, threaten ‘traitors’', February 17, 2016. [Online]. Available: https://indianexpress.com/article/india/india-news-india/jnus-central-library-website-hacked/. [Accessed: March 3, 2019].

[67] Hemanta Pradhan, The Times of India, 'Probe begins into OUAT website hacking case', January 16, 2016. [Online]. Available: https://timesofindia.indiatimes.com/city/bhubaneswar/Probe-begins-into-OUAT-website-hacking-case/articleshow/50606790.cms. [Accessed: March 16, 2019].

[68] PTI (Press Trust of India), The Hindu, 'ISRO's commercial arm Antrix website 'hacked'', July 12, 2015. [Online]. Available: https://www.thehindu.com/news/national/isros-commercial-arm-antrix-website-hacked/article7413823.ece. [Accessed: March 18, 2019].

[69] Special Correspondent, The Hindu, 'Kerala Government website hacked', September 27, 2015. [Online]. Available: https://www.thehindu.com/news/national/kerala/government-website-hacked/article7694665.ece. [Accessed: March 19, 2019].

[70] PTI (Press Trust of India), The Times of India, 'CBI website hacked by 'Pakistani Cyber Army'', December 4, 2010. [Online]. Available: https://timesofindia.indiatimes.com/india/CBI-website-hacked-by-Pakistani-Cyber-Army/articleshow/7038524.cms. [Accessed: March 19, 2019].

[71] Mohit Kumar, The Hacker News, 'Websites of Indian Embassy in 7 Countries Hacked; Database Leaked Online', November 7, 2016. [Online]. Available: https://thehackernews.com/2016/11/indian-embassy-hacked.html. [Accessed: March 24, 2019].

[72] Rohit Srivastwa, Seqrite Blog: blogs.seqrite.com, 'Cyber Intelligence averted major Internet service disruption in India', September 29, 2017. [Online]. Available: https://blogs.seqrite.com/cyber-intelligence-averted-major-internet-service-disruption-in-india/. [Accessed: March 24, 2019].

[73] PTI (Press Trust of India), NDTV: www.ndtv.com, 'Reliance Jio Data Leak: Books On Hacking Seized From Arrested Man', July 14, 2017. [Online]. Available: https://www.ndtv.com/india-news/reliance-jio-data-leak-books-on-hacking-seized-from-arrested-man-1724892. [Accessed: March 26, 2019].

[74] Nandini Yadav, BGR (Boy Genius Report): www.bgr.in, 'IndiGo Airlines confirms its Twitter handle was hacked', January 31, 2017. [Online]. Available: https://www.bgr.in/news/indigo-airlines-confirms-its-twitter-handle-was-hacked/. [Accessed: March 30, 2019].

[75] Mayur Shetty, The Times of India, 'Global ATM heist: Cyber cheats hacked into systems of Pune, Bangalore companies', May 12, 2013. [Online]. Available: https://timesofindia.indiatimes.com/india/Global-ATM-heist-Cyber-cheats-hacked-into-systems-of-Pune-Bangalore-companies/articleshow/20008913.cms. [Accessed: April 2, 2019].

[76] PTI (Press Trust of India), The Hindu - Business Line, 'ATM heist: EnStage is 2nd Indian firm hit by data breach', November 21, 2017. [Online]. Available: https://www.thehindubusinessline.com/info-tech/ATM-heist-EnStage-is-2nd-Indian-firm-hit-by-data-breach/article20613454.ece. [Accessed: April 8, 2019].

[77] Swati Khandelwal, The Hacker News, 'Massive ATM Hack Hits 3.2 Million Indian Debit Cards — Change Your PIN Now!', October 20, 2016. [Online]. Available: https://thehackernews.com/2016/10/india-debit-card-hack.html. [Accessed: April 16, 2019].

[78] Wikipedia Contributors, Wikipedia: The free Encyclopedia (Wikipedia.org), 'Yandex', April 12, 2019. [Online]. Available: https://en.wikipedia.org/wiki/Yandex. [Accessed: April 16, 2019].

[79] Wikipedia Contributors, Wikipedia: The free Encyclopedia (Wikipedia.org), 'VK (service)', April 4, 2019. [Online]. Available: https://en.wikipedia.org/wiki/VK_(service). [Accessed: April 16, 2019].

[80] Wikipedia Contributors, Wikipedia: The free Encyclopedia (Wikipedia.org), 'Baidu', April 12, 2019. [Online]. Available: https://en.wikipedia.org/wiki/Baidu. [Accessed: April 16, 2019].

[81] Wikipedia Contributors, Wikipedia: The free Encyclopedia (Wikipedia.org), 'WeChat', April 6, 2019. [Online]. Available: https://en.wikipedia.org/wiki/WeChat. [Accessed: April 16, 2019].

[82] Wikipedia Contributors, Wikipedia: The free Encyclopedia (Wikipedia.org), 'Intel', June 1, 2019. [Online]. Available: https://en.wikipedia.org/wiki/Intel. [Accessed: June 1, 2019].

[83] Wikipedia Contributors, Wikipedia: The free Encyclopedia (Wikipedia.org), 'Advanced Micro Devices', June 1, 2019. [Online]. Available: https://en.wikipedia.org/wiki/Advanced_Micro_Devices. [Accessed: June 1, 2019].

[84] Wikipedia Contributors, Wikipedia: The free Encyclopedia (Wikipedia.org), 'Intel Management Engine', May 2, 2019. [Online]. Available: https://en.wikipedia.org/wiki/Intel_Management_Engine. [Accessed: June 1, 2019].

[85] Wikipedia Contributors, Wikipedia: The free Encyclopedia (Wikipedia.org), 'AMD Platform Security Processor', May 26, 2019. [Online]. Available: https://en.wikipedia.org/wiki/AMD_Platform_Security_Processor. [Accessed: June 1, 2019].

[86] Wikipedia Contributors, Wikipedia: The free Encyclopedia (Wikipedia.org), 'Protection ring', May 10, 2019. [Online]. Available: https://en.wikipedia.org/wiki/Protection_ring. [Accessed: June 1, 2019].

[87] Wikipedia Contributors, Wikipedia: The free Encyclopedia (Wikipedia.org), 'Baseband processor', January 2, 2019. [Online]. Available: https://en.wikipedia.org/wiki/Baseband_processor. [Accessed: June 1, 2019].