Cybersecurity and Smart Cities: Establishing the Need for Capacity Building

– Charru Malhotra
E governance Expert, IIPA, charrumalhotra@gmail.com

– Aishvarya Srivastava
Student, BITS, Pilani, aishvarya678@gmail.com

– Vaibhav Gandotra
Student, BITS, Pilani, vaibhavgandotra99@gmail.com

The citizen-centric paradigm of governance insists on public service delivery system to be 'intelligent' and 'smart' enough to adapt itself to the ever-burgeoning needs and aspirations of its citizens. Therefore, through the umbrella concept of Smart Cities, urban governance employs 'smart' technologies such as Artificial Intelligence (AI) and Internet of Things (IoT), for resolving concerns related to various aspects of urban public services including public transportation, waste-disposal in cities, and street-lightening and so on. The Government of India (2015) has adopted an urban renewal and retrofitting program, with the mission to develop 100 smart cities across the country making them citizen friendly and sustainable. However, such a redefined 'Smart' urban scenario has a hidden cost attached to it. The recent unexpected breakdowns, such as the one that happened in cyber controls of smart city of Atlanta in March 2018, emphasis that cyber-security is a concern that cannot be wished away. Therefore, the preparedness of the urban citizenry to handle such situations is an equally important concern that too should be addressed simultaneously. Respecting this need of capacity building, the present study attempts to gauge the awareness level of urban citizenry. To address this, the study first attempts to demystify the emerging trends of Artificial Intelligence (AI) and Internet of Things (IoT), then moves on to understand the basic techniques of cyber risks that are popularly prevalent, followed by the influence of these emerging technologies on the cyber security scenario. After this basic conceptual foundation has been built, it moves on to unravel the level of cyber security awareness amongst urban citizens by conducting a primary survey with 152 valid responses. The sample that was considered for the purpose was limited to only tech savvy urban citizens *viz.* the technocrats and the technical students only. The basic idea of such of choice had been - "*if technical genre of citizens were not aware of negative repercussions of emerging technologies in their present daily lives, then the possibility of the same would be almost negligible amongst the rest*". The findings emanating from secondary sources as well as the primary survey have been weaved in the present paper through well-defined five modules including Introduction, Review of Literature, Findings and Observations of the primary survey, followed by Discussions and Concluding Remarks. Once the need for the study has been established, general comparative study regarding awareness of different factions of society about this issue is done with the help of a survey.

Key words: Citizen-centricity, public service delivery, urban governance, Artificial Intelligence(AI), Internet of Things(IoT), Smart Cities, Cyber Security, urban citizens

Introduction

For ages galore, defence and military applications have been using state-of-art technologies such as advanced intelligent networking and laser sensors for detection and imaging of targets. However, these technologies seem to now have become all-pervasive, completely disrupting the complacent zones, and creating a newer set of opportunities and challenges for common men in all aspects of their existence. Even the realm of public service deliveries has got a complete digital make-over with the implementation of Artificial Intelligence (AI) and Internet of Things (IoT), the proof of which can be best savoured in a smart city implementation. In a smart city, millions of smart (IoT) devices with sensors and internet connectivity are connected to each other, capturing and sharing millions of zettabytes of data that is eventually pushed to remote data centers (called cloud). Such a city boasts of interconnected smart homes, connected self-driving

cars, connected logistics and so on. More interconnected these devices and services are, the more vulnerable they might become. For instance, the entire city could be pushed to 'dark ages' by 'wriggling' into city's centralized control center. Such vulnerable scenarios of interconnected smart cities, had probably been visualized by fiction writers ahead of city planners or policymakers. As an example, it was way back in the year 1970, the movie ' Colossus: The Forbin Project' had depicted that the connected computer systems from the U.S. (called as "Colossus" in the movie) and another one of similar type from Russia (called as "Guardian" in the movie) connect on sly and nuclear war is threatened. This fictional scenario was probably a prophecy of sorts for the smart city of Atlanta (Georgia) that was brought down to its knees by a targeted ransomware virus, presumably 'injected' by an enemy country. It was in March 2018 that a ransomware attack by two Iranian hackers, SamSam breached into Atlanta's network. [1], disabling all its public services. More than 6 million citizens of the city had no access to city Wi-Fi, international airport, public databases. Even its municipal services including utility, parking, and court services were totally stalled and several years' worth of data was also destroyed. This American city had to spend almost $10 million to recover its services. It's a cyber web and a slight glitch in its interface can cause damage on a serious level. Indeed, with the increased usage of the Internet and IoT (Internet of things), the threat to cyberspace is rising exponentially with IoT gaining new a new name-*Internet of Threats* [2].

Therefore, the preparedness of the urban citizenry to handle such situations is an equally important concern that too should be addressed simultaneously. Respecting this need of capacity building, the present study attempts to gauge the awareness level of urban citizenry. The moot premise of the study, therefore, is- "*Are urban citizens aware about cybersecurity threats posed by emerging technology scenario*?"

About the Study

Two fields of Emerging Trends i.e. Artificial Intelligence (AI) and Internet of Things (IoT), will be covered in this study. It will also focus on cybersecurity issues related to AI and IoT and how they create an impact at both microscopic and macroscopic level.

Various facets of AI and IoT will be analyzed to understand the severity of these issues. This will be done with the aid of various examples. The aim of the survey is to analyze the awareness among people about these emerging trends and whether they are aware of the risks that they expose themselves to. The target audience will hail from two different sections Before putting this scheme into effect, there are two issues which need consideration. First issue revolves around the security of the smart cities. The second issue deals with the awareness among the people regarding the optimum utilisation of smart cities. A survey was conducted to gain a better understanding about these issues. Its solitary purpose was to establish a comparative study of the general awareness among people regarding the cyber-security issue in India. This was also conducted to test whether they realize how much risk they expose themselves to while using IoT devices. The aim was also to find the role of security software. A Google form was uploaded and shared [3]. Seventy-six responses were gathered from undergraduate students (particularly from the engineering field) who are primarily going to be the potential users of the emerging trends in smart cities. They belonged to the age group 18-20 years and belonged to the urban population. The same number of responses were received from government officers working in somewhat related fields. They also belonged to the urban sector. To a large extent, these officers are going to be the implementers of the ongoing smart-city mission of the government. The similarity and differences between these two strata of users will help in drawing some possible conclusions. The total sample comprised of 152 respondents.

REVIEW OF LITERATURE

2.1 Connecting the Dots - AI, IoT, SmartCities, CyberSecurity

Artificial intelligence (AI), the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings. The term is frequently applied to the project of developing systems endowed with the intellectual processes characteristic of humans, such as the ability to reason, discover meaning, generalize, or learn from past experience.[4] AI is all around us. The smartphones we use (Voice assistants and portrait mode), GPS, automated driverless cars, social media news feed, drones. Everything makes use of AI in some way or the other. The Internet of Things, which is commonly called IoT, refers to the billions of devices around the world that are connected to the internet through sensors or Wi-Fi. It's a giant network

of objects that connect to the internet. Each device collects data, and this data, known collectively as big data, is exchanged and analyzed. Examples of common IoT devices include a diverse collection of small items such as smart thermostats that learn your preferred home temperature, light bulbs that alert you to outdoor air quality, smart locks that you can open from an app on your phone. It also includes bigger items such as driverless vehicles, jet engines, and sensors on a machine in a manufacturing plant, which can also be called machine-to-machine (M2M). These days even things like trees and bedsheets are being connected to the internet through sensors. IoT can be used in various sectors as well – manufacturing, smart cities, retail, healthcare, transportation etc.

Smart cities have their roots in AI and IoT. If Smart City is considered to be the building, then AI and IoT are the bricks. Before dwelling further, let's see what exactly is a smart city. A complex ecosystem of municipal services, public and private entities, people, devices interconnected to each other on a digital platform. It pair devices and data to the city's physical infrastructure and services to reduce overall cost and enhance sustainability. It will help to reduce traffic congestion, increase air quality, improve cleanliness facilities etc. Life will become easier but the citizens might have to pay a price for it. Since this whole city revolves around cyberspace, detection and patching up of cybersecurity breaches should be their prime priority. After all Forsyth F. had rightly commented in his popular fiction titled Fox (2018), "*The boy beat the Koreans with a few lines of computer code that no one else in the world could have thought of*".

Cyber security refers to the practice of ensuring the integrity, confidentiality and availability (ICA) of information. The ability to defend against and recover from accidents like hard drive failures or power outages, and from attacks by adversaries is represented by cyber-security. The latter includes everyone from script kiddies to hackers and criminal groups capable of executing advanced persistent threats (APTs), and they pose serious threats to any organization or enterprise. The process includes protecting systems, networks and programs from attack, damage or unauthorized access. In simpler words, it refers to the security of cyberspace from cyberattacks or adversaries. The mere architecture of computer systems makes it prone to cybersecurity breaches. A little carelessness on our part can be a potential victim to frauds, hacking, scams and endless digital attacks.

To understand security aspects first we need to be aware of various ways by which cyber-attacks generally take place. Here we are mentioning some techniques with examples which was used in recent cyber attacks:

1. Phishing: It is a way by which a malicious email or message is sent to the user which appear to be from a reputable source / government office but generally contains a URL or an attachment which once viewed may install malware on to the system or may steal important information like passwords, etc. Recently, Wipro became a victim of an advanced phishing attack that affected many employee accounts and even customers of the firm. [5]

2. Ransomware: It is a method by which access to user's system data is locked and a ransom is demanded in the form of virtual currency such as bitcoin to return access to the user. In 2017, two major and intertwined ransomware attacks spread like fire around the world, causing shut down of hospitals in Ukraine and radio stations in California, and this became the time when ransomware became an existential threat. The first attack was named Wannacry which we are familiar with today. [6]

3. Crypto jacking: Crypto jacking or malicious crypto mining is a threat which is present on a system secretly and try to mine cryptocurrency (digital currency) from the system by various methods. Quick Heal (security software provider) claims that it had detected more than three million crypto jacking malware between January to May 2018. [7]

4. Identity Theft: It is a practice of stealing the victim's identity by grabbing important information such as license number, PAN number. The cyber attacker pretends as he is the victim and may do something illegal which may cause further problems for the victim. This is also called credential theft. The biggest example is the Ukrainian power grid attack. [8] In this attack, the criminals specifically used Black Energy 3 and made frequent loggers their victim by performing credential theft.

5. Watering hole attack: It is a method by which malware is inserted on those websites particularly which are frequently visited by the members/employees of particular organization/group. This is specifically done to get access to the data and system of a particular organization and thus access to the network at the desired target. Back in 2013, digital attackers injected malicious code into the U.S. Department of Labour's (DoL) website which the workers as well as contractors frequently used. The site redirected them onto a page which was full of vulnerabilities for a cyber-attack. [9]

6. Hacked in translation: It is a new kind of cyber trap also known as attack through subtitles. Malware is cleverly inserted in subtitles through JavaScript code and important information from the system is stolen.

Demystifying the Changing Scenario

Large military, government, corporate, financial, organizations, firms even individuals collect and store large amounts of unprecedented data on their computers and other devices. This can be sensitive information such as bank details, personal details, intellectual property which in the wrong hands, can result in the vulnerability of data with severe consequences. Another reason is the rising cost of breaches. Cyber-attacks can be financially difficult for businesses to bear. It not only refers to the monetary loss but also the reputational damage associated with it. Customers can lose their faith in their company and invest elsewhere. A poor reputation in terms of cybersecurity can also serve as a hindrance in acquiring new contracts. Incidentally, development in technology and alliance with AI and IoT have resulted in more frequent and sophisticated attacks. These attacks are indistinguishable from the normal workflow of the system. They are more efficient, cheaper, more easily accessible and more difficult to prevent. As a result, the companies need to be more aware of their surroundings and implement security controls that will help them to detect and protect malicious attacks before they can cause damage. With an increase in the number of devices connected to the internet, cybersecurity risk also increases. It not only increases the speed of performing the tasks but also offers the users greater accessibility and control over their devices. It becomes important to understand that this risk is not only limited to big companies but is a big issue for nations to worry upon as it may affect their entire population even without any time for getting prepared for this disaster. A recent example is the Ukrainian power grid attack which was studied in great detail in our study because of its uniqueness of being a very well-coordinated attack and victimizing a significant number of population [10] Several substations containing many Kilovolts of power were disconnected for three hours as a result of cyber-attack. Such attacks direct us to make our architecture, active defense as well as passive defense systems better as the adversaries are thinking of new techniques of attacks every day. India has also been lately in the news owing to cyber attacks. India's power sector is facing at least 30 cyberattacks a day, Mint reports, quoting unidentified sources. The attacks — originating mainly from China, Singapore, Russia and the CIS countries — have kindled fears of terrorists hacking the country's power infrastructure to cause economic disruption, especially now that India has an integrated national grid. Officials say grids between 220 kv and 765 kv are safe, but the 132 kv grid managed by states is "pretty insecure". In recent years, hackers have targeted the Tehri dam in Uttarakhand and launched ransomware attacks on several state discoms such as Haryana and Telangana. [11] IT services giant Cisco estimates there will be 50 billion connected devices globally by 2020– so this problem will only worsen with time. Thus, it will be wise to conduct regular vulnerability assessments to help identify and address the risks presented by these assets. [12] Moreover, the increase in the availability of these tools will pave the way for the less skilled hackers to come into the industry. This will widen the circle of threats making it even more difficult for the organizations or the cybersecurity professionals to prevent an attack. The commercialization of cybercrime has made it easy for anyone to obtain the resources they need for launching damaging attacks, such as ransomware and crypto mining.

With more than 20 billion devices being connected to the internet by 2020, cybersecurity has become more of a social issue than a technical problem [13]. With more and more awareness increasing regarding the issue of cybersecurity, cyber attackers are finding new ways to target our devices.

Thus, these attacks are only possible

as more and more devices are being connected. Artificial Intelligence role on the issue is still not clear. If the AI algorithms are infected by any of the above-discussed methods, it can lead to huge disruption which is even beyond the imagination of humans. Though both AI and Cybersecurity are essentially discussed together with the increasing role of artificial intelligence in our IoT devices, it will become impossible to stop these crimes without the use of AI. Soon, AI will have the ability to replace human cyber experts but the problem lies in the fact that AI can only imitate humans in the best possible way. But the human brain has other unique features such as means to think critically, make predictions, make deviations to what was predicted earlier. Current cybersecurity features require the capacity to scrutinize and work on a large amount of data which is only possible through AI algorithms.

For understanding the relation between IoT and Cybersecurity, it becomes important to understand the various stages of IoT and identify the loopholes and stages which need to be worked on to save us from this technological disaster. It comprises of four stages. [14] First, are the Devices or Thing which comprises of all the sensors, machines, devices etc. which collect and gather data and information at various places. It is the raw data which is not processed upon and is probably not of any use to the cyber attackers. It can even be as random as a tree or a bedsheet. Internet Gateways come second in line. This stage of IoT remains very close to sensors and data collectors. Here the data is processed and compressed. Analog to digital conversion of data takes place through ADC. The third stage is the Fog Node or Cloud where the data is transferred to the IT world. Hence, it is also known as the IT edge stage. All the data analytics and machine learning algorithms are applied at this stage. [15] The location of edge IT is close to the sensors and data collectors thus saving the transportation cost of the data and also cases of data leaks. The last stage comprises of Cloud. It is the place where all the big data is stored. Big data is the whole of IoT data collected by the billions of interconnected devices. From here the data again goes back to the general public and the cycle continues in this way making a big question that which stage is more vulnerable?

Most of the people believe that IoT data from the Cloud is the most vulnerable stage and most cyberattacks take place to steal this data. But the case might be opposite to that. Many researchers claim that IoT data is useless but the insight is priceless. [16] The gateway to this data so that this data can be processed upon as the attacker wishes is the most vulnerable factor and securing this should be worked upon as this can lead to system failures and yet again cyber disasters.

To make digital space more secure, there is a slow but steady shift happening towards edge computing. The word edge in this context means literal geographic distribution. Edge computing is computing that's done at or near the source of the data, instead of relying on the cloud at one of a dozen data centers to do all the work. It doesn't mean the cloud will disappear. [17] It means the cloud is coming to you. Right now a large percentage of companies all across the world rely on a handful of " cloud providers" such as Amazon, Yahoo, IBM and Microsoft. [18] The scope for expansion is now limited in the cloud sector. Hence, edge computing is paving its way as a more secure means to channelize information and perform the necessary tasks.

Let's take an example to understand this better. Iphone's security and privacy features fall in the category of edge computing. By enabling encryption and biometric scan, Apple helps in minimizing a lot of security concerns for its users which might have been there in cloud computing.

It also plays a major role in autonomous vehicles -"data center on wheels". Intel estimates that on an average 40 TB of data will be generated every eight hours by the autonomous vehicles. [19] It is both unsafe and irrelevant to send all of this information to the cloud. It is unsafe because an autonomous car traveling on the road will have to send data to the cloud for analysis and decision making which can prove to be highly dangerous. An immediate action to apply brakes to prevent collision with a child can get delayed owing to this. Edge computing provides a better solution to this problem. This just highlights one facet of it. Edge computing can help with bandwidth and latency also. Latency in layman's term means the delay in sending and receiving the information. Voice assistants, video games etc. all work on this concept.

Edge computing seems like a promising field in the near future which can prove to be the backbone for smart cities in times to come.

After learning how AI and IoT are related to cybersecurity, it becomes a bit easier to understand the cybersecurity issues related to smart cities. Several factors are responsible for this. First is the 'Convergence of Cyber and Physical World'. The confluence of IT and OT allows cities to control and govern technology systems through remote cyber operations. Due to the proliferation of IoT devices, there are many entry points through which hackers can access city systems. The second issue is the Interoperability between legacy and new systems. Coexistence and frequent interaction between old and new systems and platforms result in hidden security vulnerabilities such as inconsistent security policies, lack in updates etc. Thus, each new IoT device connected to the system increases the chances of a malicious attack. An example of this is that in 2015, the US OPM's systems suffered a data breach, giving hackers access to personal records and files of 4.2 million employees. This was mainly due to OPM's old network's ability to encrypt data. [20]. Further, there are some stumbling blocks in this journey of technological advancement. It becomes important to understand whether our cities are ready to become a smart city or not. The sole reason being that the time is not far away when even wars between nations will be fought in cyberspheres. A recent example of the USA vs Iran cyber-war has certainly proved this. If this happens, the lack of cyber-security will be enough to dismantle entire countries. [21]

India's Advents

Talking about India particularly, the Smart City Mission was one of Prime Minister Narendra Modi's key electoral promises in 2014. The scheme, launched on June 25, 2015, aimed to develop 100 smart cities across the country, making them citizen-friendly and sustainable. [22]. with a risk of cyber threat and fraud in India, the government has made digital safety as the need of the hour. Keeping in mind not only the citizens, but the government has also issued guidelines for its ministers as well. Union home ministry has issued a 24-page note charting out its first social media and Internet policy for government employees. The move is to prevent security breach and ensuring sensitivity of data, as 30 attempts are made every day by foreign entities to hack into or deface government portals and unlawfully extract confidential information. A large number of employees use Smartphone and at times get exposed to malware-infected website unknowingly [23].

To further enhance the cybersecurity system in our country, the Union Home Ministry will set up the Indian Cyber Crime Coordination Centre (I4C) which will have its head office in New Delhi. [24] It will be apex coordination center to deal with cybercrimes. It will closely work with the State Government and the UT's to scrutinize the cyberspace, particularly social media. It will also keep an eye on websites that flout Indian laws and engage in illegal or inappropriate content.

Despite the large base of internet users in India, only 26 percent of the Indian population accessed the internet in 2015. By 2021, there will be about 635.8 million internet users in India i.e. around 36% of the population. So in India internet accessibility and awareness also is a major concern.

Primary Survey- Findings & Observations

Technology is advancing by leaps and bounds every day. If you don't keep pace with it, you somehow find yourself lagging in this digital race.

Findings and Observations

a. Awareness about Recent GoI Cyber initiatives

1. Are you aware of the increase in petrol and diesel price by ₹2 which was mentioned in the Indian Budget 2019?

Fig 1.1:Govt. Officers

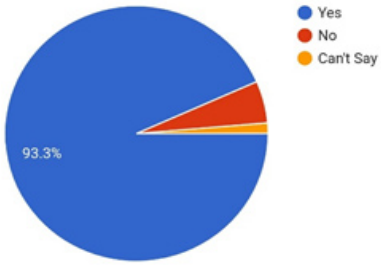

Fig 1.2: College Students

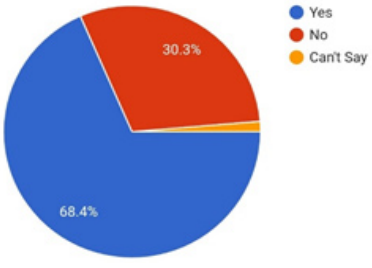

Figure1-Awareness regarding general national economic issues

2. Are you aware of the allocation of ₹100 crores to operationalize the i4C (Indian Cyber Crime Coordination Centre)?

Fig 2. 1: Govt. Officers

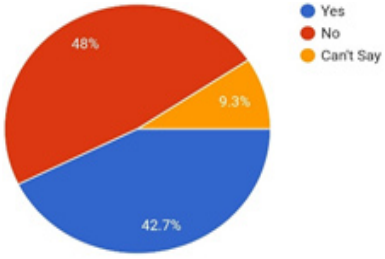

Fig 2. 2: College Students

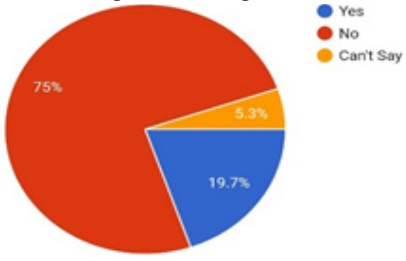

Figure2-Awareness regarding national issues related to Cyber-security

The above two figures provide statistics for the awareness among the target audience regarding national issues related to Cyber Security. This will help in assessing the general mindset of the people. The data in figure 1 and figure 2 clearly indicates that although government officers are generally more aware of the policy changes that are being brought as compared to undergraduate students in general. But both the target groups had less awareness regarding issues related to cyber security as compared to other economic issues although we have discussed that a cyber breach can equally disrupt the economy and is dangerous up to a great extent. Only 19.7% of students (figure 2.2) are aware of Indian Cyber Crime Coordination centre which is very disappointing as this group is most vulnerable to cyber threats. Almost 93% government officers (figure 1.1) are aware of the increase in diesel price while only 43% know about I4C (figure 2.1) which clearly indicates that there is an urgent need for cyber awareness as use of IoT devices are increasing day-by-day and hence the chances of cyber-crime.

3. How many times have you encountered security breaches in the last one year (such as malware attacks)? This can include your smartphones, laptops, computers etc.

Researchers at cybersecurity giant McAfee saw an average of 480 new threats per minute and an increase of 73 percent in malware which are being affected through IoT (Internet of Things) devices. The following question was asked to see effect of antivirus and protection softwares and also to see people's general awareness about how much are their devices secure. Both the target audience have almost similar feedback regarding the attack of malware attacks on their IoT devices. Here, it is surprisingly found that almost 50% of individuals (figure 3) have not encountered a malware even once on their device in last one year. This seems to be impossible without the intrusion of antiviruses and security software. This shows that Antiviruses are doing a great job in protecting our devices although citizens have a false conception in their mind that their devices are not often affected by malwares.

Fig 3. 1: Govt. Officers

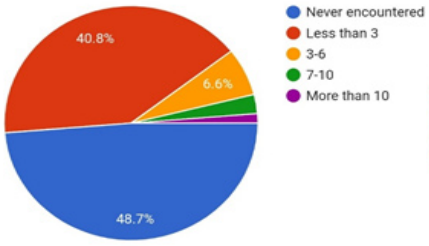

Fig 3. 2: Govt. Officers

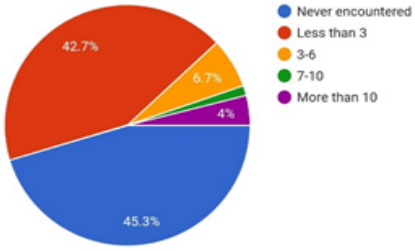

Figure3-Feedback on malware encountered and role of security softwares

4. According to you, how much risk do you expose yourself to when you use all these IoT devices (such as smartphones, laptops, etc.)?

The question was asked particularly to check the awareness among the people regarding the risks they expose themselves to when they use countless IoT devices. The data clearly shows that people were oblivious of the fact that how much risk they face while using IoT device as 37% of students (figure 4.2) and 61% of govt. professionals (figure 4.1) feel IoT devices pose moderate risk. Although the users who think that the devices didn't pose any threat are very insignificant in numbers which is a sigh of relief.

Fig 4. 1: Govt. Officers

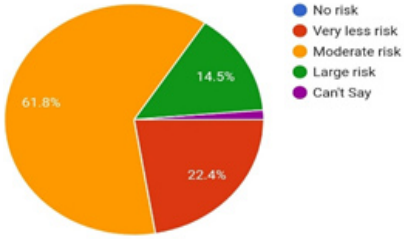

Fig 4. 2: College Students

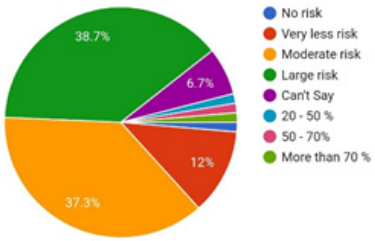

Figure4-Risk posed by IoT devices

The subsequent question will analyse people's reaction on the use of AI in cyber-security.

5. According to you, is an increase in the use of AI, IoT and Blockchain, a threat to cyberspace or a well- measured step into the future?

There are mixed reactions about introducing AI in cyber-security technology as 50.7% of govt officers (figure 5.1) and 58% of students (Figure 5.2) consider introducing emerging technologies in cyber-security both as a threat and safeguard. But the fact remains that it will be impossible to safeguard ourselves from cyber-attacks without the use of AI owing to its increased role in our machines and devices and maybe in the near future, in entire cities.

Fig 5.1: Govt officer

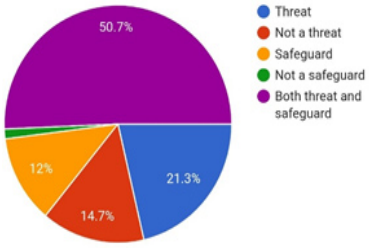

Fig 5.2: College student

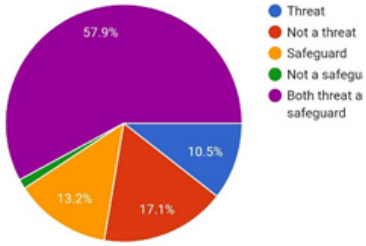

Figure5 - Opinion on introducing emerging trends in Cyber sphere

Discussions - Cybersecurity Capacity Building

Development of any new technology or adoption of any new method requires awareness. In the case of cybersecurity, awareness forms the basis of its security measures.

We wanted to take the opinion of the general public on the ongoing issue of AI-alarmist vs AI-optimist. [25] Though this issue is being debated at a level of Elon Musk and Mark Zuckerberg with Elon Musk warning to people building AI technology that it may be repurposed to be used as 'killer bots'. Elon Musk, who is presently leading Tesla and spaceX wants to convey a clear message that being the paramount users of AI they understand that it is dangerous. On the other side, Mark Zuckerberg and allies claim that vulnerabilities associated with using AI are opaque and distant whereas benefits are clear and near [26]. Till now, we majorly use Artificial Narrow Intelligence (ANI) where the machine's brain mimics human reactions for a narrow domain [27]. Pessimists believe that the time is not far when superintelligence will be introduced which will supersede human intelligence. They realize that handing over world's collective matter to an algorithm may even lead to replacement of the human civilisation [28]. Optimists lead by Zuckerberg claim that their systems get better with the advancement of AI technology and it has the potential to make the world better referring reduced use of AI as a big challenge to technological development [29].

Humans need to be familiar with the concept of cybersecurity breaches to be able to prevent it. A cyber-attack will aim to exploit the weakest link - humans. No matter how secure a system is, there are still loopholes which questions the credibility and security of the system. A little precaution goes a long way in keeping the cybersecurity attacks at bay. This is where the need for cyber security capacity building creeps in. Cybersecurity capacity building refers to the inventory of ideas and proposals that allows individuals, communities and governments to extract benefits from investment in digital security. Several models have been created and a Global Forum for Cyber Expertise (GFCE) has been set up for regulating the rules and regulation of CCB. It also comprises of a team of well-trained experts who handle all the cybersecurity issues, carry out awareness-raising initiatives etc. Given the emerging technology and the integration of smart cities with it, it becomes even more important to pay attention to the Cybersecurity capacity building approach. It offers a healthy solution to a multitude of problems like bridging the gap between the private firms handling the smart city and the government or putting the problem of ownership across the table. It can also play a major role in making the construction and implementation of the smart city program more transparent and open to changes and suggestions from its users. The CB in India can draw inspiration from Germany which has one of the best networks of ICT in the world. With the ever-advancing technology, it is crucial to not turn a blind eye to this equally important issue of managing cybersecurity in smart cities.

Concluding Remarks

The most difficult challenge in Cyber Security is the ever-evolving nature of security risks. It is crucial for cyber-experts to keep updating the technologies as the adversaries are always looking for something new to attack with. Each successful attempt will have a bigger impact than before with ever increasing IoT devices now touching the 20 billion mark. According to a recent report, India has emerged as the 'most vulnerable' to

cyberattacks due to the deployment of IoT. The country also saw a twenty-two percent jump in total number of attacks in the IoT segment during the quarter ended June. [30] Recent examples like these and countless intrusions by adversaries pose a big question mark to our smart-city projects. The data provided by the survey conducted and the secondary data used indicates that the awareness among the general public regarding the cyber-security is a big matter of concern for security in smart cities.

As per existing data in India, major challenge is to provide internet accessibility to all citizens. Another major challenge is to make citizens aware of the usage of these latest technologies. For this government need to implement various programmes and open skill centers in the cities. Cybersecurity capacity building has a major role to play in the implementation of this awareness-oriented approach. They will lay down the foundation for the establishment of safer and more secure smart cities.

There is no such thing which exemplifies perfection in this world. The cyberworld is no different. With its expanding realm and user-friendly interface, more users are getting connected to the web at an exponential rate without understanding the security concerns associated with it. For ensuring cybersecurity with such a huge audience, emerging technology like AI has to be incorporated in cyber-security technologies. It is a must for keeping track of the terrorists of the new smart-world or simply the cyber-attackers. This further reduces human involvement and even a small intrusion by an adversary can cause an irreparable loss. Hence we are left with no choice but to adopt these emerging trends with the implications of this never-ending technological debate in mind. As David Wong rightly said- "New technology is not good or evil in and of itself. It's all about how people choose to use it."

References

- Robertson, A. (2018, November 28). Two Iranian men charged with the ransomware attack that took down Atlanta. Retrieved from https://www.theverge.com/2018/11/28/18116213/iranian-hackers-samsam-ransomware-indictment-bitcoin-sanctions-wallet-atlanta
- Timpson, D. (2018, October 24). The Internet Of Things Is Becoming The Internet Of Threats. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2018/10/24/the-internet-of-things-is-becoming-the-internet-of-threats/#24b0943a38d0
- https://forms.gle/zxLRHRR95xY8UQVC8 (Govt. Officer's form) https://forms.gle/eF2Y38jqmitisVTY8 (College student's form)
- Copeland, B. J. (n.d.). Artificial intelligence. Retrieved from https://www.britannica.com/technology/artificial-intelligence
- Das, A., & Phadnis, S. (n.d.). Retrieved April 17, 2019, from https://timesofindia.indiatimes.com/business/india-business/wipro-hit-by-advanced-phishing-attack/articleshow/68915021.cms
- Fruhlinger, J. (2019, April 05).The 6 biggest ransomware attacks of the last 5 years. Retrieved from https://www.csoonline.com/article/3212260/the-5-biggest-ransomware-attacks-of-the-last-5-years.html
- P., Sangani. (2018, June 25). Over three million cryptojacking attacks detected between January-May 18. Retrieved from https://m.economictimes.com/tech/internet/over-three-million-cryptojacking-attacks-detected-between-january-may-18/articleshow/64730826.cms
- Case, D. U. (2016). Analysis of the cyber attack on the Ukrainian power grid. *Electricity Information Sharing and Analysis Center (E-ISAC)*.
- Norton, A. (2019, April 25). Five High-Profile Watering Hole Attacks Highlight Importance of Network Security. Retrieved from https://securityboulevard.com/2019/04/five-high-profile-watering-hole-attacks-highlight-importance-of-network-security/
- Case, D. U. (2016). Analysis of the cyber attack on the Ukrainian power grid. *Electricity Information Sharing and Analysis Center (E-ISAC)*.
- Bhaskar, U. (2019, September 11). [21] Gurevich, V. I. (2011). Cyber weapons against the power industry. Energize, 10, 40-42. Retrieved from https://www.livemint.com/industry/energy/how-cyber-attacks-are-increasing-in-india-s-power-sector-1568107532851.html
- Fehske, A., Fettweis, G., Malmodin, J., & Biczok, G. (2011). The global footprint of mobile communications: The ecological and economic perspective. *IEEE communications magazine*, *49*(8), 55-62.
- Writer, S. (2019, February 18). How Big is IoT? 20.6 Billion Connected Devices By 2020. Retrieved from https://mitechnews.com/internet-of-things/how-big-is-iot-20-6-billion-connected-devices-by-2020/
- Stokes, P. (2018, December 05). 4 Stages of IoT architecture explained in simple words. Retrieved from https://medium.com/datadriveninvestor/4-stages-of-iot-architecture-explained-in-simple-words-b2ea8b4f777f
- Bhattacharjee, S. (2019, February 23). https://www.viainsider.com/iot-architecture/. Retrieved from https://www.viainsider.com/iot-architecture/
- IIoT data is useless, but the insights are priceless. (2017, September 21). Retrieved from https://www.smartindustry.com/articles/2017/iiot-data-is-useless-but-the-insights-are-priceless/
- Miller, P. (2018, May 7). What is edge computing? Retrieved from https://www.theverge.com/circuitbreaker/2018/5/7/17327584/edge-computing-cloud-google-microsoft-apple-amazon

- Lohr, S. (2007). Google and IBM join in 'cloud computing'research. *New York Times*, *8*.
- Miller, P. (2018, May 07). What is edge computing? Retrieved from https://www.theverge.com/circuitbreaker/2018/5/7/17327584/edge-computing-cloud-google-microsoft-apple-amazon
- Pandey, P., Golden, D., Peasley, S., & Kelkar, M. (2019, April 11). Making smart cities cybersecure. Retrieved from https://www2.deloitte.com/insights/us/en/focus/smart-city/making-smart-cities-cyber-secure.html
- Gurevich, V. I. (2011). Cyber weapons against the power industry. *Energize*, *10*, 40-42.
- PM's Smart City Mission fails to pick up pace; 33% projects completed so far. (2018, December 17). Retrieved from https://www.businesstoday.in/current/economy-politics/pm-smart-city-mission-fails-to-pick-up-pace-33-per-cent-projects-completed-so-far/story/301505.html
- Tripathi, R. (2019, July 12). Home ministry issues social media norms for government employees. Retrieved from https://economictimes.indiatimes.com/news/politics-and-nation/no-classified-government-info-can-be-stored-on-private-cloud-services-says-home-ministry/articleshow/70185733.cms
- Indian Cyber Crime Coordination Centre Current Affairs - 2019... ..... currentaffairs.gktoday.in/tags/indian-cyber-crime-coordination-centre© GKToday. (n.d.). Retrieved February 19, 2019, from https://currentaffairs.gktoday.in/tags/indian-cyber-crime-coordination-centre
- Gunning, D. (2017). Explainable artificial intelligence (xai). *Defense Advanced Research Projects Agency (DARPA), nd Web*, *2*.
- Tansey, I. (2017, September 4). Back AI fight of the century: Musk vs. Zuckerberg. Retrieved from https://codebots.com/ai-powered-bots/musk-vs-zuckerberg
- Panchal, S. (2018, August 24). Types of Artificial Intelligence and examples. Retrieved from https://medium.com/predict/types-of-artificial-intelligence-and-examples-4f586489c5de
- Blagojevic, B. (2018, October 8). AI, Optimists vs Pessimists and Why The Singularity Isn't Near. Retrieved from https://medium.com/ml-everything/ai-optimists-vs-pessimists-and-why-the-singularity-isnt-near-5d3a614dbd45
- Clifford, C. (2017, July 26). Mark Zuckerberg doubles down defending A.I. after Elon Musk says his understanding of it is 'limited.' Retrieved from https://www.cnbc.com/2017/07/26/mark-zuckerberg-defends-a-i-again-continuing-debate-with-elon-musk.html
- Hariharan, S. (2019, August 13). India sees most IoT attacks in Apr-Jun. Retrieved from https://timesofindia.indiatimes.com/business/india-business/india-sees-most-iot-attacks-in-apr-jun/articleshow/70650684.cms

Dr. Charru Malhotra Ph.D. (IIT-Delhi) (Theme- Design Approach for Co-creation of e-Governance), MCA, DCA, MCSD, Associate Professor (e-Governance and ICT), Indian Institute of Public Administration, New-Delhi. Dr. Malhotra has ***more than 28 years*** of professional experience and is recognized as a ***global thought leader*** on tech-themes including Participatory Governance, Smart Cities, Smart Villages, ICT4D, Implementation of Emerging Technologies (AI/IoT/Blockchain) in public domain, Agile Governance, Data Privacy/Data Localization Risk Management , and so on. She has *more than* ***40 publications in recognized international and national journals***, books and has ***won several 'Best paper Awards'*** at global level (for instance, *"Ethical Framework for Machine Learning"* by IEEE/ ITU , "*Design and Implementation of Digital Service Standard-DSS*" by GoI, "*A Validated Innovative Citizen Centric Approach to e-Gov*" in ICeG, Deakin Univ, Australia).

charrumalhotra@gmail.com

Vaibhav Gandotra is currently in his third-year pursuing B.E.(Hons) Electronics and Instrumentation from Birla Institute of Technology and Science Pilani, Pilani campus. He has consistently been working on assignments related to sensors and IoT in his college life. Presently he is involved in a project related to 'Structural Health Monitoring' in Smart-cities. With an experience of working with microcontrollers in various projects, the security vulnerabilities associated to them motivates him to work on cyber-security issues in emerging trends. Apart from this, he is presently serving as the technical coordinator for IEEE BITS Pilani. He has always been a tech-admirer and loves to explore new gadgets inspiring him to work in the field of cyber-security for quite some time now. Other than academics, he manages to find some time for programming and is a swim-lover.

vaibhavgandotra99@gmail.com

Aishvarya Srivastava is an undergraduate engineering student from Birla Institute of Technology and Science Pilani, Hyderabad Campus. She is currently in her third year, pursuing B.E Computer Science and M.Sc. Physics. She has always been inclined towards the scientific aspect of life. She came across the field of Cybersecurity a few months back and wishes to research more about it. She has also completed a course on 'Usable Security' from the University of Maryland. Apart from this, she is an enthusiastic sports lover and dancer. She is fond of reading books and doesn't miss out on any opportunity to travel.

aishvarya678@gmail.com