Data Privacy with IoT Devices & Applications: A Myth or Reality

[1]Megha Gupta and [2]Nida Khan
[1,2]Department of Computer Science, Mata Sundri College For Women,
University of Delhi
meghabis@gmail.com, nidakhan090220@gmail.com

Abstract -Today's technical world revolves around internet. When we are dealing with internet, we come across various comforts, namely pace, accuracy, connectivity, security and privacy. While using internet several protocols need to be pulled up. Buzz word of the times is IoT, where we associate internet with things. It has become a major domain of comfort. Usage of IoT is possible in every sector either it is domestic zone or public zone. Smart homes and smart grids are two of the major fields related to domestic zone where IoT turned out to be boon. Public zones have major influence in every walk of life as IoT is useful in healthcare, business, real estate. Finding solace is part of struggle when we are dealing with internet. Privacy and security remain a constant area of concern. Privacy is still foreign affair when we are indulging with internet. Like in any territory in order to ensure basic manners several rules are laid, and individuals associated with the territory are supposed to follow the same. If they are not able to do so they are penalized. Similarly, Internet facilities too, need to follow certain norms in order to achieve goals. Protocols refers to rules/norms corresponding to the system which governs every action and ensures every agreement from both the parties i.e., client and server. IoT devices are majorly popular these days. They are really wonderful systems incorporated with certain protocol. These devices are assets to today's state of conduct. Security and privacy are guaranteed with these systems as they abide by norms plugged with the same. In this paper we will be describing some of the attacks on presently used IoT devices. Majorly, paper will be having description about the major concerns related to internet of things i.e., privacy and security. Also, this paper holds some real-life case studies related to attacks on the IoT applications.

Keywords: Privacy; Security; IoT Devices; Cyber attacks

I. INTRODUCTION

IoT is one of the most blooming domains of the era. It has shaken every sector of development. IoT devices help a lot. It is affecting everyone's walk of life. IoT is benefiting in healthcare management, reducing energy consumption, automation and much more. In healthcare, it plays a vital role in collecting data of patients and that too critical ones. Security of data is major concern here. Similarly, automated vehicles are wonderful blessing. In this too privacy, security and intelligence all the three are major red spots of the issue. Communication between vehicles and infrastructure can raise questions on security and privacy. Another major sector where IoT devices have done wonders is smart grid in order to keep electricity bill balanced, smart grid gather consumption and distribution records. This again forces user of smart grid to think about security. In smart homes, there is same scenario all data gets collected for better management of the same.

In all the instances mentioned above the baseline of every domain is collection of data on cloud. Also this data is really critical and highly private. So, if any mishap took place this data can be hacked and used in various undesirable ways. This is major domain of concern as we are simply connecting devices and building up the network. In the process, if this network gets attacked by any foreign entity. This foreign entity can use this data in any unpleasant manner. To assure strong security and exclusive privacy, devices are required to follow up certain protocols.

We can easily find the increasing demands of IoT application in today's world. The sudden escalate of IoT devices can be depicted by Figure 1.

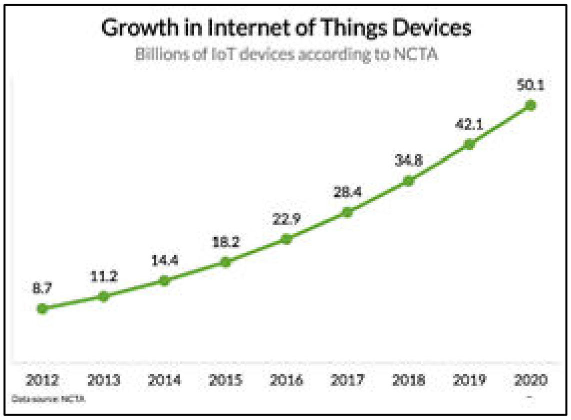

Figure1. Increasing demand of IoT devices [1]

The root cause of the perks in demand is the comfort offered by the devices. These systems are really magnificent as all them comes with best attributes namely, pace, capital and labor reduction, efficiency and accuracy. But it comes along certain concerns majorly privacy and security. Also, dependence purely on network, complexity and cost of implementation are also alarming issues overlapped with these IoT devices. Figure 2 describes the pros and cons associated with these devices.

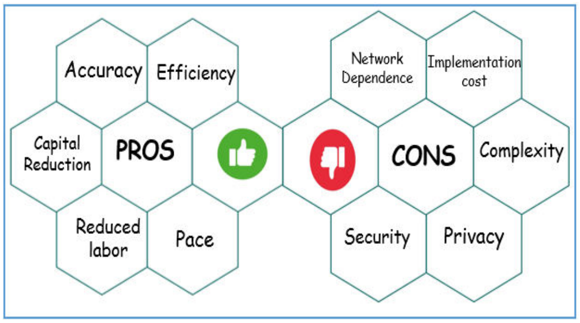

Figure 2. Pros and Cons of IoT devices

The key of IoT devices is that data is getting gathered in cloud and this data is highly private, critical for end users. This data needs to be secured. If this data gets interfered by any external source is really terrible and this causes user to think twice before questioning on security and privacy. There are various attacks in IoT devices. Also many cases are reported till date due to attack on IoT data. Attack on data leads to many undesirable events.

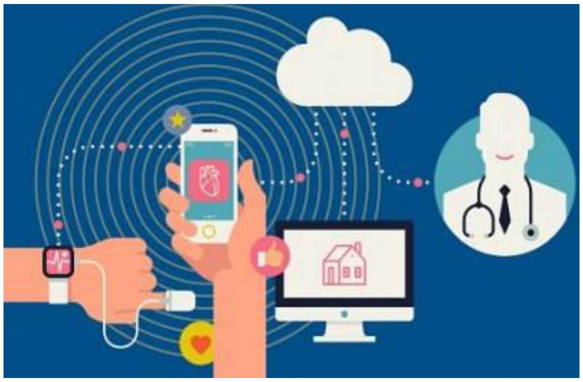

Figure 3. IoT based HealthCare System [2]

Consider an IoT based healthcare system which allows better management and real-time analysis of data. Figure 3 depicts a small IoT based network. Various IoT devices are now-a-days easily avail by clients, such as fitness bands. An individual using fitness band gets regular updates about health reports like BP, heartbeat, pulse rate and many more. So, for an instance an individual's heartbeats were reported fluctuating majorly because he was suffering from heart attack and his data is stored on cloud. A small network will be created between hospital and individual's place. This network holds real-time data. But if this network gets corrupted by any unfair entity. Any mishap can take place at end-user's place. For instance, if this data was availed by some robbers; individual's house might get robbed. So, here concept of privacy and security is challenging when between networks real-time data is exchanged.

II. LITERATURE SURVEY

The work [21] objective is to find the concepts and applications based on Internet of Things with the vision to determine and address existing challenges. The book also analyses the various uses of IoT and its accompanying technologies, as well as future research prospects in this field.

Authors of book [22] provided one-of-a-kind guide, where you'll be able to take your notion from concept to reality. It's a trendy topic in technology, whether it's dubbed physical computing, ubiquitous computing, or the Internet of Things.

In book [23], author speaks about Information security and privacy standards for the healthcare industry that have been operationalized and tested. This authoritative resource thoroughly tackles information security and privacy considerations and their ramifications within the business of patient care, as written by an expert in the subject with various industry certifications.

In [24], the manual affords an overarching view of cyber protection and virtual forensic demanding situations associated with big facts and IoT environment, previous to reviewing present facts mining answers and their ability utility in large facts context, and present authentication and get entry to manipulate for IoT devices. An IoT get entry to manipulate scheme and an IoT forensic framework is likewise provided on this book, and it explains how the IoT forensic framework may be used to manual research of a popular.

In [25] author describes how to design and develop Internet of Things (IoT) solutions that provide end-to-end security and data protection on a large scale. It is unique in its detailed coverage of threat analysis, log analysis, secure design principles, impact of Smart IoT on data protection and usability in security.

Privacy Engineering by Nishant Bhajaria in MEAP began January 2021 Publication in Fall 2021. A great high-level resource on privacy as it relates to the data collected by business software systems - Joe Ivans.[3] Privacy Engineering is a hands-on manual to architect a present-day and flexible seclusion program for your institution. It will provide engineering solution that that excites the end-user to meet crucial lawful demands and this develops trust between client and server.

In [26], author captures the modern day studies in Internet of Things, its applications, architectures, and technology. The book specifies capacity destiny instructions and technology that facilitate perception into several scientific, business, and customer applications.

The work [27] depicts The Internet of Things (IoT) could be a network of devices and sensible things that gives a pervasive atmosphere within which individuals will move with each the cyber and physical worlds. Because the range and sort of connected objects still grow and therefore the devices themselves become smarter, users' expectations in terms of adaptive and autonomous digital environments are on the rise.

III. ATTACKS ON IoT DEVICE

The IoT is much all over today. As a result, businesses got to bear in mind of the various sorts of IoT cyber security threats so as to safeguard devices themselves likewise because the knowledge is being collected. [4]

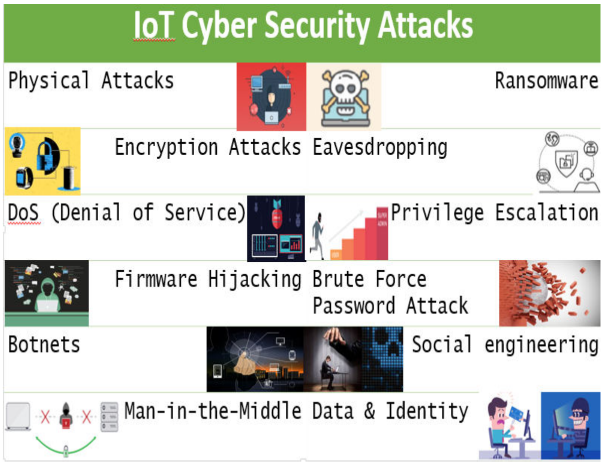

Figure 4. IoT cyber security attacks

Figure 4 lists IoT cyber security attacks. There are various attacks being reported in recent past. Security and privacy have always been a challenge in the world of networking. The main cause behind the same is the data collection. When a network is created data is stored over the cloud. This data is crucial and personal. If by any way this cloud gets hacked and then the information will be raid by the raider. Any unpleasant activity can take place at end-user's place.

Given below is a brief description about cyber security attacks [4-13].

Physical Attacks: When IoT devices can be physically accessed by anyone, physical attacks occur. Because the bulk of cyber security threats originate from within an institution, it's critical that your IoT devices are kept in a secure location, which is often not possible. Many physical cyber security attacks start with an adversary inserting a USB drive to transmit malicious code, which is why it's more critical than ever to keep your USB drive safe.

Privilege Escalation: Hackers look for flaws and weaknesses in IoT devices to access resources that are typically protected by apps or user profiles. In this type of attack, hackers use their newly acquired privileges to distribute malware or steal sensitive data.

Encryption Attacks: Cryptography uses hiding the data to be transmitted this is to make sure that only end-user is able to view it. This is accomplished by encoding the data to be transmitted at the sender's end and decoding the data at the receiver's end.

When data from an IoT device is not secured, an intruder can sniff it and save it for later use. “Once encryption keys are unlocked, cyber-assailants can install their own algorithms and take control of your system,” according to the report. Encryption is a must-have in the IoT ecosystem as part of your cyber security efforts for these reasons.

The field of cryptography is an old one and dates back to 2000 B.C. in Egypt. Figure 5 shows a brief look at the basic working of cryptography.

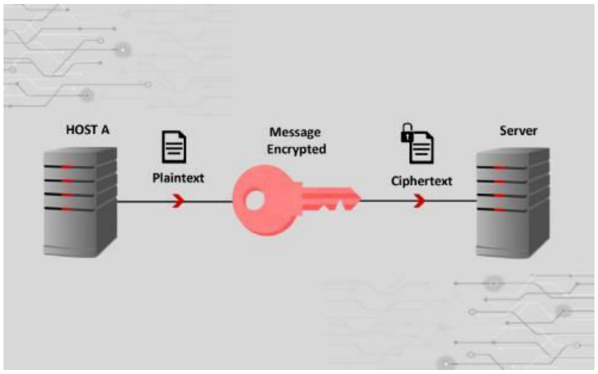

Figure 5. Working of cryptography [5]

DoS (Denial of Service): A Denial-of-Service (DoS) attack is one that attempts to bring a machine or network to a halt, rendering it unreachable to its intended users. DoS attacks work by inundating the target with traffic or delivering it information that causes it to crash. The DoS attack deprives genuine users (workers, members, or account holders) of the service or resource they expected in both cases. An additional type of DoS attack is the Distributed Denial of Service (DDoS) attack. A DDoS attack occurs when multiple systems orchestrate a synchronized DoS attack to a single target.

Firmware Hijacking: Firmware sits outside of operating system; it lives on a stage that can’t generally be visible with the aid of using the working device or applications jogging inside it. This loss of transparency makes it in particular tough to understand if the firmware has been attacked and inflamed with malware. The firmware additionally offers hackers the “keys to the kingdom” with regards to your device. If compromised, attackers can rewrite the working commands to your computer, server, router, or different hardware. Some of the troubling statistics that the study found included: Firmware attacks have increased by 5x over the last 4 years.

Botnets: A bot is set up through a kind of trojan, a shape of malware hiding for your running gadget ready idly through for commands from a command and manage server this is managed through a criminal, called a botmaster or bot herder. A botnet makes use of your laptop in conjunction with heaps of different gadgets which mean the cybercriminals on the wheel can harness nearly limitless computing power. Figure 6 shows how a botnet works.

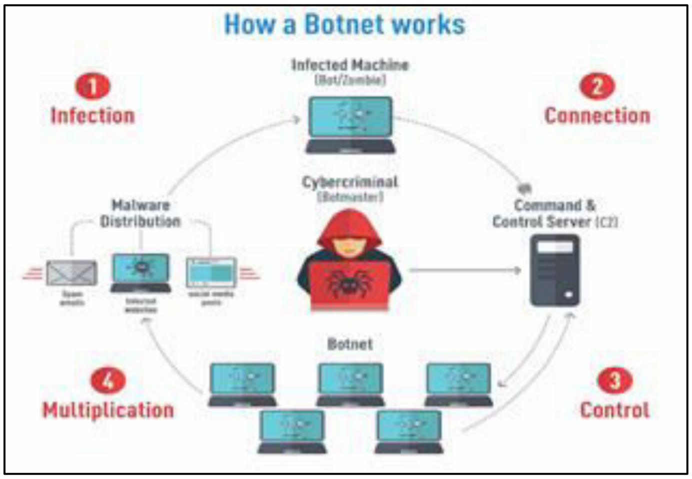

Figure 6. How does botnet works? [8]

Man-in-the-Middle (MITM): A man-in-the-middle attack (MITM) is a general term for when a perpetrator positions him in a conversation between a user and an app by either eavesdropping or pretending to be one of the parties, making it look like exchange looks is on the way.

The aim of an attack is to steal personal information such as login details, bank account information, and credit card numbers. Typically, targets are financial application users, SaaS companies, e-commerce sites, and other websites that require login.

Ransomware: It is a type of malicious software (malware) that fears to issue or jam allowance to information or a computer system, usually by encrypting it, until the casualty pays a ransom fee to the attacker. In many cases, the ransom demand comes with a deadline. If the casualty doesn't pay in time, the data is gone forever. Ransomware attacks are all too common these days. Major companies in North America and Europe alike have fallen victim to it. Cybercriminals will attack any consumer or any business and victims come from all industries.

Social engineering: It is the act of manipulating individuals in order that they surrender personal statistics. The varieties of statistics that criminals are searching for can vary, however whilst people are targeted, the criminals are commonly seeking to misinform the person into giving them passwords or financial institution statistics. Or they may be seeking to get right of entry to a laptop so as to secretly set up malicious software program so as to then supply them get right of entry to private statistics, in addition to giving them manipulate over the laptop. Typically, social engineering hacks are accomplished with inside the shape of phishing emails, which are looking for to have you ever reveal your statistics, or redirects to web sites like banking or buying web sites that appearance legitimate, attractive you to go into your details.

Data & Identity Theft: The news is full of horrible, unpredictable hackers who gain access to information and money with all kinds of awesome hacks, but we are often our security biggest enemy. It is in the hands of malicious thieves and opportunists.

The main strategy for the theft of personal information is to accumulate data, with a little patience and a lot to find. Please refer to. Excellent aggregation of personal identity with data from smart watches, fitness trackers and smart phones, smart fridges, etc., if available, in addition to common data available on the internet combined with social media information. Learn more about. For users, targeted attacks to steal personal information can be easier and more sophisticated.

Eavesdropping: Eavesdropping attacks occur through the interception of network congestion. By eavesdropping, an attacker can get passwords, credit card numbers and other sensitive data that a user might be transferred over the network. Eavesdropping can be passive or active.
Passive eavesdropping - The information is gained by hacker over a network web by hearing to the message getting imparted.
Active eavesdropping - A hacker busily snatch the data by sending queries and behaving as friendly unit or customer care representative. This is called probing, scanning or tampering.

Detecting passive listening attacks is often more important than detecting active listening attacks. Indeed, active attacks require the attacker to start with passive listening in order to recognize active units. The best corrective for eavesdropping is data encryption.

Brute Force Password Attack: It is the cyber equivalent of trying every key on your key ring and finding the right one -- brute force attack (also called brute force cracking). About 5% of data breach incidents in 2017 were caused by brute force attacks. Brute force attacks are simple and reliable. Assailants let a computer do the work - for example, by trying different combinations of usernames and passwords until they find one that works. A brute force attack in progress is the best countermeasure: once attackers gain access to the network, it's much more difficult to catch them.

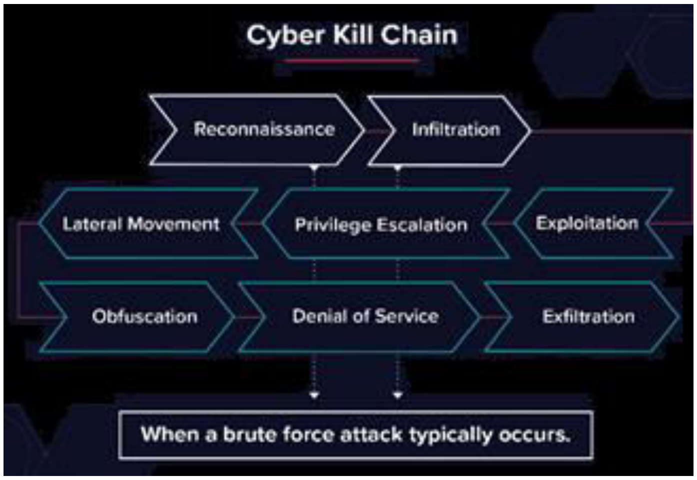

Figure 7. How brute force attack? [13]

Figure 7 displays motive behind brute force attacks.

IV. PREVENTION AGAINST CYBER ATTACKS

To prevent the cyber-attacks as discussed in above section 3, following measures should be taken. [14]

- Ensure that your computers, tablets, and smartphones are protected with reputable internet security software.
- Passwords for device accounts, Wi-Fi networks, and connected devices should be strong and unique.
- Keep your IoT devices close to you if you are using it in a public area.
- When data is getting transmitted over public Wi-Fi for secure transfer look for trusted VPN.
- Be careful while making transaction in public spaces like café, small stores, etc.
- On IoT device try to disable all unnecessary ports and devices.
- Try to protect data which is transferred over a network.
- Secure communication is key of protection against such attacks.
- Associate required protocol required over the web in order to safe guard IoT device or IoT system.

V. CASE STUDIES

A. Tesla Automated Car Hacked

Recently, World have moved towards automation. Automation has always leaded to speedy and safe travel. Various industries are shifting their ways towards automation. This industry is marking its way in every walk of life. Automating gadget means getting control over same by developing a network. Various car industries too have moved towards automation. Most famous in the race is of automated vehicle is Tesla.

Tesla is one of the most blooming industries in terms of introducing automated vehicle. Tesla support collaborative intelligence in order to implemented automation in cars. It is humans who eventually assemble cars, because this task requires flexibility and some creative problem solving, which are virtually impossible for robots [15].

To strength the energy of Collaborative Intelligence, business leaders should perform the following three analyses. [15]
1. Value analysis:-First, listing and understand all the responsibilities required at each degree inside the value chain and what their contribution is to value creation.
2. Task analysis: - Subsequent, analyze every undertaking to apprehend the abilities required to master it.
3. Skill analysis: - Finally, classify every ability as premiere for machines, for human beings, or hybrid.

Collaborative intelligence calls for assigning responsibilities that are notably automation-vulnerable to machines and people that require initiative and flexibility to people. It's far people who subsequently gather automobiles, because this mission calls for flexibility and a few creative trouble fixing, which are really impossible for robots.

Two researchers have shown how a Tesla — and in all likelihood other automobiles — can be hacked remotely with none person interaction. They completed the assault from a drone.

This was the end result of research performed 12 months with the aid of Ralf-Philipp Weinmann of Kunnamon and Benedikt Schmotzle of Comsecuris. The analysis turned into to begin with wi-finished for the Pwn2Own 2020 hacking opposition — the contest presented a automobile and different considerable prizes for hacking a Tesla — but the wi-findings had been later mentioned to Tesla thru its malicious program bounty program after Pwn2Own organizers decided to briefly cast off the automotive category because of the coronavirus pandemic. The assault, dubbed TBONE, involves exploitation of vulnerabilities affecting ConnMan, an internet connection manager for embedded devices. An attacker can take advantage of those flaws to take full control of the infotainment device of a Tesla with none consumer interplay. A hacker who exploits the vulnerabilities can perform any assignment that everyday consumer ought to from the infotainment system. That includes beginning doors, converting seat positions, gambling tune, controlling the air conditioning, and editing steering and acceleration modes. But, the researchers defined, “This attack does no longer yield drive control of the car even though.” [16]

They confirmed how an attacker should use a drone to launch an assault to hack a parked vehicle and open its doors from a distance of as much as 100 meters (roughly 300 ft). They claimed the take advantage of labored towards Tesla S, 3, X and Y models.

“Including a privilege escalation take advantage of which includes CVE-2021-3347 to TBONE might allow us to load new Wi-firmware in the Tesla car, turning it into a get admission to point which can be used to take advantage of other Tesla cars that come into the sufferer car’s proximity. We did no longer want to weaponize this make the most right into a Trojan horse, however,” Weinmann stated [16].

Tesla patched the vulnerabilities with an update pushed out in October 2020, and it has reportedly stopped the use of ConnMan. Intel changed into also informed for the reason that organization become the authentic developer of ConnMan, however the researchers said the chipmaker believed it turned into now not its duty [16].

The researchers learned that the ConnMan factor is widely used inside the car undertakes, that can imply that comparable attacks can be released in opposition to other automobiles as well. Weinmann and Schmotzle turned to Germany’s country wide CERT for help in informing potentially impacted vendors; however it’s presently unclear if different producers have taken action in response to the researchers’ wireless endings. The researchers find their wireless endings on the CanSecWest convention earlier this year. That presentation additionally includes a video of them hacking a Tesla using a drone. [16]

During the last years, cyber security researchers from numerous companies have confirmed that a Tesla may be hacked, in many instances remotely. It’s not the primary time that it’s been proved that Tesla can be hacked.

In November ultimate year, a Belgian security researcher observed that it turned into possible to steal a Tesla the use of just Bluetooth. He determined vulnerability inside the Tesla model X, with a series of safety flaws in its keyless access machine which means an assault should take gain of this device to scouse borrow an automobile. “Fundamentally, a fusion of vulnerabilities permits a hacker to scouse borrow a version X in a few minutes,” the researcher Lennert Wouters stated. “Whilst you combine them, you get a much extra powerful attack” [17].

B. Ring, Smart Home attacked

IoT have turned dreams into reality. Smart homes are also result of same. In smart homes, every this is connected through network. Everything in home is controlled automatically. In this setup, appliances are works over information shared over the network. The main pro about smart home is efficient management of cost in terms of energy. The main disadvantage of the same is lack of security and privacy. Also, Smart homes are also prone to cybercrime attack. Some devices of smart homes were attacked in recent past by cyber criminals.

Ring is an Amazon-owned home security company which offers smart security cameras and video doorbells. The Ring doorbell is a smart home device that allows you to control your front door remotely. It's mounted next to your front door and connected to your mobile device via Wi-Fi. When someone comes to your house, you can see the person through the camera and let them in remotely. The company also offers indoor and outdoor cameras which allow you to monitor your home while you are away, check on your kids, or keep an eye on your pets. The cameras are equipped with motion sensors and a two-way talk feature, allowing you to talk to someone in real time [18]. Figure 8. shows ring security camera by Amazon.

Figure 8. Ring, Security Camera by Amazon [19]

Ashley LeMay sued Ring after a stranger talked to her daughter via a hacked indoor protection digital digicam. An unidentified hacker won get entry to to the digital digicam and its microphone and advised the 8-year-vintage that he changed into Santa and that she ought to damage her belongings. Another own circle of relatives additionally had their Ring digital digicam hacked — a cybercriminal began out speaking to them as they had been getting equipped for bed. [18]

The information traversing between the Ring device and its application is not encrypted. As a result, anyone who’s hacked your Ring device can monitor who enters or leaves your house and can even steal your Wi-Fi password. Ring showed to NBC News that it'll make two-component authentication the default putting on its new devices, which safety professionals say makes it more difficult for them to be hacked. Two-component authentication is presently an non-compulsory putting at the devices. [20].

VI. CONCLUSION

Uses of IoT devices have sharp increase in the world today. It is clearly visible our dependence on automation has turned the way of life. IoT application has provided several benefits in the way of living. These applications are comforting with pace, accuracy and efficiency. IoT comes with many standards that make up the life of people easy going. But it's really unusual to find the drawbacks of IoT world. The major points in the list are: - security and privacy. IoT works simply by establishing network between devices. The end-users find it difficult to trust due to increase in cybercrime. Cyber Attack on IoT devices and application is not a new issue. Like in recent past there is a peak increase in cybercrime rate. So, we can say that various lows are associated with IoT systems. Cybercrime is not only in the world of getting password hacked, getting Wi-Fi networks attacked but it is more. IoT is there in health care, real estate management, automation, smart home management etc. Every industry is badly affected in terms of security and privacy. Hacker simply maintain control over the network, gains credential information and turns out to be heavily effective. There are course of action by which one can avoid one's IoT device from getting attacked. Attack by hacker can cause major losses not only in terms of materialistic points, But if hacker, hacks a health care network. It can cause major loss of life too. Certain protocols are already there to be followed up by the IoT systems.

More research in protocols is to be followed up by the IoT systems or application. Some network need to issue more protocols for developing secure and end-to-end confidential web. Protocols are required to be embedded in IoT devices and applications too for better accountability of credential information being shared. More work in terms of assurance of security is to be done. New technique and algorithms are essential to develop in order to encrypt information end-to-end between cloud and client. Study is demanded in field of privacy so that client can rely on network for exchanging sensitive information over the network.

REFERENCES

1. The IoT Data Explosion: How Big Is the IoT Data Market? Published Jan, 2019 by Priceonomics Data Studio https://priceonomics.com/the-iot-data-explosion-how-big-is-the-iot-data/

2. Internet of Things: Opportunities for the pharma and health care industries By Solomon Ojigbo -01/06/2016. https://pharmanewsonline.com/internet-of-things-opportunities-for-the-pharma-and-health-care-industries/

3. Nishant Bhajaria, Privacy Engineering, MEAP began January 2021. https://www.manning.com/books/privacy-engineering

4. 10 Types of IoT Cyber Security Attacks, November 2019, https:// www.micro.ai/blog/10-types-of-cyber-security-attacks-in-the-iot

5. Prashant, Cyber Attacks Explained – Cryptographic Attacks, https://www.valencynetworks.com/blogs/cyber-attacks-explained-cryptographic-attacks/

6. What is a denial-of-service attack (DoS)? https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos

7. Firmware Attacks Are Up According to a New Security Signals Report (What You Need to Know) May 20, 2021 by Nathan Drager https://www.quantumpcs.net/firmware-attacks-are-up/

8. Botnets: Dawn of the connected dead, HAYLEE, MAY 23, 2017 https://blog.emsisoft.com/en/27233/what-is-a-botnet/

9. Man in the middle (MITM) attack https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/

10. What is Ransomware? https://www.proofpoint.com/us/threat-reference/ransomware

11. 5 Common Cyber Attacks in the IoT - Threat Alert on a Grand Scale https://www.globalsign.com/en/blog/five-common-cyber-attacks-in-the-iot

12. Top 10 Most Common Types of Cyber Attacks https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/
13. Jeff Petter , What is a Brute Force Attack? June 2021 https://www.varonis.com/blog/brute-force-attack/
14. Internet of Things (IoT) security: 9 ways you can help protect yourself, a NortonLifeLock employee, Feb. 6, 2019 https://us.norton.com/internetsecurity-iot-securing-the-internet-of-things.html
15. Tesla is fixing its automation problems with Collaborative Intelligence, Alessandro Lanteri, 2018 https://www.hult.edu/blog/tesla-collaborative-intelligence/
16. Tesla Car Hacked Remotely From Drone via Zero-Click Exploit, Eduard Kovacs on May 03, 2021 https://www.securityweek.com/tesla-car-hacked-remotely-drone-zero-click-exploit
17. Researchers hack into Tesla from the sky, It's amazing what you can do with a drone, Denham Sadler, May 2021. https://ia.acs.org.au/article/2021/researchers-hack-into-tesla-from-the-sky.html
18. Ring hacked: doorbell and camera security issues, Paul Black, Jun 04, 2020 https://nordvpn.com/blog/ring-doorbell-hack/
19. Amazon to acquire Ring video doorbell maker, cracking open the door in home security market, Taylor Soper & Nat Levy, February 27, 2018 https://www.geekwire.com/2018/amazon-acquire-ring-video-doorbell-maker-cracking-open-door-home-security-market/
20. Family whose Ring camera was hacked is now suing the company, Scott Stump, January, 2020 https://www.today.com/money/family-whose-ring-camera-was-hacked-now-suing-company-t172787
21. Shakil, Samiya Khan, Mansaf Alam (Eds.), "Internet of Things (IoT): Concepts and Applications", published in May 2020
22. Adrian McEwen and Hakim Cassimally (Eds.), Designing the Internet of Things, 2013
23. Sean Murphy (Ed.),"Healthcare Information Security and Privacy", 2015
24. Dehghantanha, Ali, Choo, Kim-Kwang Raymond (Eds.), Handbook of Big Data and IoT Security, Springer International Publishing, 2019.
25.Damilare D. Fagbemi, David M. Wheeler, and J. C. Wheeler (Eds.), The IoT Architect's Guide to Attainable Security and Privacy, Auerbach Publications, October 2019.
26. Amir Vahid Dastjerdi, Rajkumar Buyya (Ed.), "Internet of Things: Principles and Paradigms" Publisher Morgan Kaufmann, May 2016.
27. Mahmood, Zaigham (Ed.), "Security, Privacy and Trust in the IoT Environment", Springer International Publishing, 2019.

AUTHOR(S) BIOGRAPHY

Dr. Megha Gupta is a PhD holder in Computer Engineering. She did her doctorate from NSIT, University of Delhi. She is presently working as an Assistant Professor in Department of Computer Science, MSCW, University of Delhi. She has presented various research papers in international conferences and published research work in SCI, SCIE, Scopus indexed international journals. Her areas of expertise include networks based on radio, cognitive, sensor, opportunistic. Presently, she is actively working in the field of machine learning & IoT.

Ms. Nida has completed her bachelors in computer science (B.Sc Honours) from University of Delhi. Presently, she is pursuing her Masters in Computer Application. Her several research papers have been published in various prestigious international conferences.