ISSN 2350-109X
www.indianscholar.co.in

Indian Scholar

An International Multidisciplinary Research e-Journal

INTRODUCTION TO DIFFERENT IOT DEVICES AND POTENTIAL CYBER ATTACK THREATS

Manyaa Doshi
Utpal Sanghvi Global School
manyaaddoshi@gmail.com

Abstract

With the ever-growing advancements in technology come a new feature in devices and they are known as IoT devices. Smart, cunning, efficient and dangerous at the same time, these devices are now widely used in every possible industry in the world be it healthcare (restocking medicines, pharmaceutical markets, remote patient care, etc.), environment management (devices used to test quality of air, soil and water), retail stores (reordering inventory, electronic transfer of payments, etc.) and so much more. This paper describes the different kinds of IoT devices most common today, different cyberattacks and how they affect the devices and to what extent and finally an experiment to predict attacks on the mentioned devices from the various cyberattacks possible. In the end it will be very easy to draw cohesive conclusions and observe the trends in the cyberattacks posed on different devices.

Keywords: remote patient care; affect the devices and to what extent; draw cohesive conclusions

Introduction

The Internet of Things is a broad terminology which is crucial to be understood when living in a generation where robots are the new humans. Together with understanding where and for what these devices would be used, it is also important to take note of specific attacks that could be posed and to protect ourselves, our wealth and our loved ones from being held hostage. The main aim of this paper is to explain, in detail, the meaning of IoT devices, where they are used most commonly today and what are the threats posed to them. It also puts light on the subject of different cyberattacks that most of us didn't know about. There isn't only one cyberattack; there are a number of them under the term 'cyberattack' so it is extremely necessary that each one of us is well equipped with knowledge about how and which kinds of devices would be attacked with which cyberattack type. Isn't it interesting to know terms like the Mirai, Distributed-denial-of-service attack, Man-in-the-middle, Botnet and Advanced persistent threats?

It's actually even more interesting to know how they work and how hackers seem to find a way into the most complexly coded software and websites. Explore with this paper, the different threats and possible outcomes of a cyberattack on IoT devices.

ISSN 2350-109X
www.indianscholar.co.in

Indian Scholar

An International Multidisciplinary Research e-Journal

MISA Global Partnership
MEMBERS OF INTERNATIONAL SCHOOLS' ASSOCIATION

Theory

Stage 1: Understanding IoT devices

What exactly are IoT devices? IoT devices are hardware objects that are virtually connected to other devices and are programmed to transfer information to other devices wirelessly over internet. These devices do need human intervention but only till a certain extent. Think about it this way; you need to reach office in 20 minutes and the drive there is 30 minutes long. You still need to finish breakfast and remove the car from your garage. How about if you could just, with a click of a button on your phone, could ask your car to come outside the garage which saves you time and energy?

Especially with the growing car industry currently exceeding technological expectations, it is now humanly possible to ask your car to come out of your garage. Car companies such as Tesla by Elon Musk has come up with an electronic car that responds to commands which are given out by you from your phone. However, why don't we look at the potential threats and attacks that could be planned out which amplifies into a very big potential threat to you and your device? IoT isn't as simple as it seems. With the technology growing so rapidly it is impossible to stop and understand where many of us, either in producing or using the device, might go wrong. Some of the leading industries where IoT devices are used to most are home, agriculture, banking, offices, schools and much more. There are so many varieties of IoT devices from Autonomous mobile bots, Asset management, Environmental monitoring, IoT run supermarkets to supply chain management, etc. these particular industries use a lot of IoT devices especially now where all communication, reordering inventory, purchasing and selling happens through internet.

Autonomous mobile bots:

Automated robots are devices and robots that are programmed to transfer and transport a large quantity of goods during in-house tasks. These are required and used by many leading companies in order to more efficiently allocate their employees and make use of modern technology to perform and duplicate human behavior without having to be constantly monitored. How do they work? These devices have a light sensing method that detects and understands the surroundings in light in the form of a pulsed laser to measure ranges on Earth. This is known as the LIDAR which stands for Light Detection and Ranging. The LIDAR bounces laser light off surroundings for the device to understand them and detect any set obstacles that might come in the way from getting to where they are required. This is because there are inputted maps of the work environment which guides them to their destination.[1] Amazon for one is using AMR to transport its inventory from one shelf to another. Not only that but these robots made by Kiva systems actually could hold up to 450 kgs and pick out the desired quantity of goods and bring it to the desired person of authority. [2] However, still not experienced by Amazon, many believe that in the future there are likely to be a number of possible threats to the subordinates.

Asset management:

IoT helps asset management become more precise and detailed and allows consumers and businesses to see the flow of their assets- from whom to whom they are going. Asset management is the tracking of assets to see whether they are working based on their expected

ISSN 2350-109X
www.indianscholar.co.in

Indian Scholar

An International Multidisciplinary Research e-Journal

key performance indicators. It also allows firms to get real time data and observe and predict movements and provides interpretation for e.g., to see how much the price of one stock in the stock exchange would change. [3]

Environmental monitoring

Environmental monitoring is using tools and devices to improve the quality of the surroundings, it consists of three parts; air, water and soil. It is setting parameters to enable the environment become more cleaner and have sustainable growth. IoT plays a big role in this new system. With the help of iot the government can make decisions easily as real time data is given about the air filtrationsystem, fertility of soil, garbage dumped in water, etc. nowadays IoT uses frequent sampling methods to test the air and water regularly and detect any infection. Much of the farming is done by manual labor and IoT lets farmers water, fertilize and improve the condition of soil and much more by using a much more uniform and consistent technique. [4]

Supply Chain Management

Supply chain management is the distribution and keeping track of goods going from one supplier to another. It is closely observing the cycle of products from the time they are raw materials till they are distributed to consumers. How does IoT help?

With speculating close onto each and every stage of production, IoT softwares allow producers to predict fluctuations in demand and understand where when and in which conditions the goods are in. This is mostly done when products are attached with a GPS system that tracks goods from one place to another. This also carries on until the supplier has restocked the inventory. It is not only manufacturers. Retailers and big superstores like Walmart use JIT which is just-in-time inventory control that restocks the products by ordering it on their own once it reaches a particular 'reorder' point. However, such devices won't work in areas with too much radio or internet traffic thus making it easier for a third party to get access to information using a number of attacks.

IoT run Supermarkets

With everything around, us industrializing, it is not a shock that supermarkets too now are run and operated by scanning of barcodes and cashless transactions. The new Amazon Go is a supermarket that uses computer vision and deeper AI systems to track how much a person has bought and automatically add it to their online cart. The process begins when a consumer scans their way through Amazon Go's entry bar and starts picking out whatever they were looking for. There are no humans or employees in Amazon Go making it a completely AI operated store. Then with the use of sensors the products are added to the bag with the quantity purchased too. There are even cameras that track he number of items one has bought and a 'facial recognition' software that generates a biography of the customer; they have a filed patent to support this too. IoT keeps the products fresh and clean. The consumer then just walks out and pays the amount through Amazon Wallet. As easy as that.

There are however manual errors and obstacles that could arise such as a glitch in the system or access to the server could change room temperature settings and spoil the stock or may add too many products in the bag. This way Amazon makes use of its 'Just Walk Out' technique.

ISSN 2350-109X
www.indianscholar.co.in

Indian Scholar

An International Multidisciplinary Research e-Journal

MISA Global Partnership
MEMBERS OF INTERNATIONAL SCHOOLS' ASSOCIATION

These stores operate using the same technology used by self-driven cars which is deep learning and computer vision. [5]

Stage 2: understanding different kinds of cyberattacks on IoT devices

What are cyberattacks? The word is split into two: cyber as in internet, computers, technological appliances; and attack is to ambush a particular thing. Cyberattacks are carried out by cybercriminals, they launch an attack on computers, softwares, mobiles, etc. to hack, steal, exploit or destroy data on one's device. Cybercrime costs are expected to rise another 15% to $10.5 trillion USD in 2025 from $3 trillion in 2015. [6] This just shows how much harm is posed to consumers using computers and those who rely on technology to store their data. Now within the rising solutions to protect data is Cloud. Cloud or Apple's iCloud stores data on the internet and can remotely be accessed by anyone who has the necessary credentials to login. In cloud data is stored in the servers instead of the hardware or desktop and is supposedly invented to make life easier. Comparatively, now it has become much easier to hack into a system that depends on clous because anyone from anywhere can hack the device's server. These cyberattacks on the cloud are called APT's (advanced persistent threats [explained below])
There a number of cyberattacks that have started taking place on a variety of devices. In fact, most of the devices mentioned above could be hacked using different tools and mechanisms.

Mirai Malware attacks- the Mirai attacks are very common and very known to a lot of firms, consumers and potential users by now. A Mirai attack is when devices are turned into controlled bots that will respond to the commands given by the hacker. It is mainly used in large scale attacks and mostly to hack home appliances. It primarily targets smart homeappliances such as IP cameras and smart TVs, etc. So how does it work? Mirai is very similar to a contagious virus. These are infected within computers and they replicate themselves, making it only worse. it is not only an appliance attack but recently also stared being called as a botnet attack. This is because the vulnerable IoT devices are connected to other command and control devices, thus becoming a large-scale hack and has affected millions of devices and kept security professionals busy. *[7]*

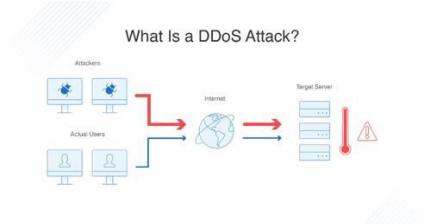
Ddos attacks- Ddos (Distributed Denial-of-service attacks) are when the hackers temporarily programme the device to not be able to respond to the host's commands and this gives the hacker enough time to divert the customer traffic to other platforms. Ddos attacks' main purpose isn't to collect or hack information but to make the server overwhelmed with too much traffic so that they give up the IP address of much larger connected devices. Attackers do this by performing a botnet attack wherein a lot of bots request for passwords and the traffic on the software/ website may reach an optimum level and this was the website or platform becomes unavailable to consumers. There have been so many real life incidents that have been Ddos attacks and those who have harmed and destroyed days' worth of business of many service companies.[8] A recent February 2020 attack is the Amazon Web Services attack where an unidentified customer was attacked where all information was available on cloud. It used a technique known as the *Connectionless Lightweight Directory Access Protocol (CLDAP) Reflection which depends on third party customers and amplifies the data sent to the victim's IP address by 70 times. [9]*

ISSN 2350-109X
www.indianscholar.co.in

Indian Scholar

An International Multidisciplinary Research e-Journal

MISA
MEMBERS OF INTERNATIONAL SCHOOLS' ASSOCIATION



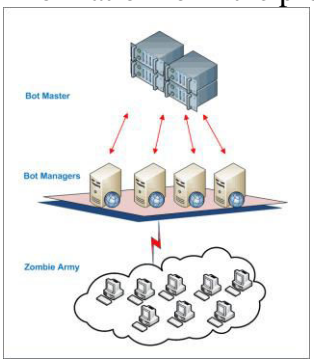
Advanced Persistent Threats- are some threats that have been constant for the cloud network. This is when the system has been attacked a particularly long time which given plenty of time to attackers to potentially damage the platform. These attacks compared to others are much more sophisticated and during this period of time the victims are unaware of this. These attacks take a lot of time to prepare and come at final conclusions; every single detail is planned and that's what makes them so successful and silent at the same time. Compared to Ddos these attacks' main aim is to collect information over a long time which means it is not just a 'dip in' attack. These contain three stages:

1)infiltration which is getting into the system and installing a malware software that basically spreads and infects the device

2) expansion- this is when hackers broaden their base and may decide to go after more confidential information and hack into employee's system as well with the help of employee codes

3) extraction- after the data has been moved up to a secure place then the main aim is to get out of the system without getting detected. The main task since the beginning was the extraction because this is when most of the hackers get identified and caught. [10]

Botnet attacks- a very simple term to understand in the botnet attack. Botnet attacks have become increasingly popular with the growing number of firms using robots and capital-intensive production. Botnet attacks are when a group of bots perform a Ddos attack, steal, spam or disrupt information form the production process. These are a part of Ddos attacks.



The Mirai Botnet attack of 2016 was when the bots conducted a Ddos attack and infected over 600,000 devices. Interestingly it was the first botnet attack to hack into weak IoT devices.

ISSN 2350-109X
www.indianscholar.co.in
Indian Scholar
An International Multidisciplinary Research e-Journal
MISA MEMBERS OF INTERNATIONAL SCHOOLS' ASSOCIATION

Man-In-The-Middle attack- personally, MITM attacks are the most intriguing. These attacks aren't very common such as malware and ransomware however they are equally (or more)dangerous.

There are 5 types of MITM attacks:

1) ARP cache poisoning- the Address Resolution Protocol allows hackers to intercept the conversations between two network providers. They either continue listening to
2) the conversation and interpreting the communication, hijack the system, alter communication (malicious failure) or conduct a Ddos attack.
3) DNS cache poisoning- this is where the hacker might send the customers a fake website and baits the customer into visiting them to then send out a phishing mail
4) HTTPS spoofing – is where the hacker's website looks very similar to the original except there is a minute change not very visible clearly. Now that the website is saved/bookmarked the hacker can successfully tap your conversations without having put himself in danger.
5) WIFI eavesdropping- allows hackers to eavesdrop and listen to the traffic through tricking people to connect to unsecured/ public networks
6) Session hijacking- this hacking is a very interesting approach. The hacker specifically waits for the victim for e.g., to log into their bank account and then uses the smart cookie and logs into the same account from their own browser.

Experiment:

Usually, it isn't possible to carry out iot device hack experiments however this section talks more about whether or not all possible devices could be hacked ornot.

many devices however with the growing number of legal websites and tools could be used to hack and break into systems. As seen above there are so many types of cyberattacks, and those were only the most common ones. Under some specific circumstances, such as under extreme security and protection protocols, it might not be impossible but possibly difficult to hack into a system as such. One of such is the IoT run supermarket: Amazon Go. Just launched in 2018, the supermarket doesn't till date have any problems or hacks, or atleast they are unknown. This is a significantly big achievement because it is very easy to think of ways hackers could earn a good amount of profit just by virtually looting a supermarket.

These are a few hypothetical ways, when iot categories are grouped with possible hacks, systems could be damaged.

1. Autonomous Mobile bots with botnet attacks- the most common way to think about a hack on the warehouse bots is ofcourse the botnet attack. Botnet attacks are programmed when a large number of bots are attacked together to disrupt either the production process or more. It's usually the large-scale businesses who use AMBs so it is rather expected there will be a number of them. This clearly gives an explanation why it would hypothetically mean that warehouses could be attacked on a very large scale. All of the devices could be programmed to hack into the system or steal data. A large number would cause enough traffic do initiate a Ddos attack also. Instead of moving traffic form one website to another, it could be programmed to obey commands.

ISSN 2350-109X
www.indianscholar.co.in

Indian Scholar

An International Multidisciplinary Research e-Journal

MISA
MEMBERS OF INTERNATIONAL SCHOOLS' ASSOCIATION

The impact and its significance: if any botnet attacks do take place it is likely to cause so much harm to the firm and consumers. However, compared with other kinds of potential threats in different categories, this one might be less jeopardizing. If for.eg amazon's fulfillment service is hacked, it would mean many of the consumers may be given damaged, wrong or may even have to wait long periods for their products to arrive. This would infact cause a system failure especially for a big brand like amazon and may even destroy their reputation. Less harm to consumers, comparatively more to producers Real life example: The Level One Robotics and Control Inc attack in 2018 had resulted in 100 company's sensitive data to be leaked online on a platform that contained confidential information, VPN addresses and customer as well as employee data. This company gave automation solutions to more than 100 automation companies including Tesla, Toyota, Ford, etc. this used Rsync as a platform to transfer data from within the company. IP addresses should be made available to only the designated managers and supervisors to avoid future ransomware attacks. [11]

2. Asset management clubbed with MITM
Asset management is all about securing and protecting assets and wealth. Hackers, once they know this, can very easily access the places one's invested, bought stocks
in and secured their wealth. However not all MITM techniques could be used here. Some of the ones that would be spot-on would-be session hijacking and DNS cache poisoning.
Why session hijacking? This is because when a user might try to login in to check the current values of their stocks or might login online to check on their wealth, hackers could access the cookie and information and could login from their own browser. DNS cache poisoning can bait the visiting into logging into a fake account just very easily giving access details to the hacker.

   The impact and its significance: asset management attacks could deeply harm the consumer, their possessions and their money at risk. Consumers could lose a lot of money if the attackers have access to sensitive information. Not only that but if the banks do not know about it soon, the virus could spread, hackers could expand their framework and even leak passwords of other users. If the attack becomes a long drawn one even government attack could be hacked into affecting a much larger proportion of the economy

   Real life example: the atm banks in Kolkata, India were hacked through an MITM attack where hackers physically entered the atm to insert stolen cards of fake cards and before which they entered a black box to activate a proxy server. This way when money is withdrawn, banking details wouldn't be asked for as the proxy server wouldn't need them to access the money form the atm. [12]

3. Environmental monitoring hacked through Mirai
Mirai attacks are on smart home appliances are quite famous. The environment management systems could very easily be controlled and hacked using Mirai and it could legitimately destroy the environment and the precisionof the work. It is very much

possible that the system could be hampered with and one virus in one system could ruin all programmed in connecting computers as well.

The impact and its significance- one of the most detrimental impacts of hampering with the environment management is it affects not only the national industries but if the country is specializing then it affects the world's output of agricultural produce as well.

Real life example: the 2019 attack on the Post Rock Water District had shut down the disinfectors and water purifier machine which resulted in polluted water being circulated. This hacker previously worked in the organization but had recently resigned, allowing him access to routers which hadn't signed him off yet. In February 2021, a hacker had tried to leak large amounts of sodium hydroxide into the Florida water plant which in large amounts can lead to death but purifies water if smaller quantities are used. [13]

4. Supply chain management with Ddos attacks
Ddos would be a very scary attack on the supply chain if it had to be done. It is not only going to be robots of the same kind on the same level but bots in other parts of the supply chain. If the Ddos attack is cast on the manufacturers then if the customers
or retailer's attention is diverted because of excess traffic then probably the sales would be lost.

Impact and significance: if the sales are lost on an international basis there could be recession as well as lower GDP. If the hackers work for another country or may want to drive other businesses out of the market, Ddos attack on the supply chain devices would cause a significant harm to the competitor.

Real life example: a recent case of the REvil ransomware attack has spread over the internet. This attack was conducted through a group known as REvil who targeted the Kaseya VSA which is a software used by many leading companies- especially in the digital industry- and this REvil attack locks up the computers who provide and manage software updates until a fee is paid to them. This way they threaten the consumers too, by giving them a warning. The Kaseya VSA attack locked up to 40,000 computers worldwide from which it made a profit of $11 million. [14]

5. IoT run supermarkets baited through MITM-
MITM has various kinds of hacking techniques but one could be used to change how IoT supermarkets work. Online grocery shopping could actually have lots of potential threats. A hacker for e.g., could change the website and tweak the URL. During checkout the banking information could be accessed without the consumer even knowing.

The impact and its significance: an attack in the supermarket would usually harm mostly the consumers and the company. Amazon go which operates only on IoT would be harmed till a great extent too.

ISSN 2350-109X
www.indianscholar.co.in

Indian Scholar

An International Multidisciplinary Research e-Journal

MISA Global Partnership
MEMBERS OF INTERNATIONAL SCHOOLS' ASSOCIATION

Real life example: the Kaseya VSA REvil ransomware attack had also hacked one of the supermarkets in Sweden who was very dependent on IoT and technology for all its inventory and checkouts. Consumers however were brutally attacked, financially. Most of the customers using their own servers to place orders were attacked, not the ones who were using the Kaseya server. This harmed the company badly as they had
to stop selling through e-commerce temporarily and keep all its cloud-based softwares offline until further notice. [15]

Result

The result as clearly observed above is that all kinds of IoT devices can be hacked using different methods. Even if they are secure and safe there are always going to be loopholes in the system. If carefully mismatched with, the systems could be hacked, information could be taken a then some more.
However, there might be some devices that might be very safe. As safe as online banking sounds, there are banks also that could be hacked and actually have been. However, one pattern we say all around is that all of these categories have IoT devices that have been connected on a large scale and it is very possible that all devices could be attacked from all mediums but it is important to predict certain types that would be used for certain devices, so that firms and consumers do have a slight bit of background knowledge in order to prepare accordingly.

Discussion

There are main results obtained in the experiments and some of them are genuinely predictable however currently all hypothetical. The discussion gives a brief on what the results are and what they indicate. There are clearly a bunch of trends and patterns observed from the experiments:

1) All kinds of IoT devices could be hacked
2) Much more complex methods of hacking could be used when deciding to access bank and asset details
3) Usually more detailed and planned research could help in getting more results but that also means that the harm could be much more.

Most of the attacks are attacking on a large scale since the size of the attacks is large and hence most Ddos attacks could potentially harm an entire company. With growing technology, the categories of IoT devices becomes much more detailed thus having many more substitutes. This just gives attackers the very intention to attack and harm the business. Also, attacks are increasing so rapidly that firms actually have to now start giving more importance to cybersecurity and security procedures because none of the firms can afford to lose or become vulnerable to any more attacks.

Conclusion

With an increasing variety of IoT devices there have also been an increasing rate of cyberattacks. IoT devices are becoming weaker and more vulnerable every day and it just jeopardizes the lives of many victims more than it already has. Although there is

very little, we as consumers could do, but there are few precautions one could take to avoid getting trapped by the hackers.

1)First and foremost is to start updating devices. Software updates really do help and prevent viruses and help fix bug problems.

2) end to end encryption- devices that are bought have a long history behind them especially second-hand devise. It is really important to secure the devices in a way that prevents hackers from getting data from the past. Probably to wipe off or erase backup data.

3) IoT network monitoring- it is also very important to make sure that all the third party or unidentified officials have been removed or blocked

There are a lot of more precautions one could take but they might never be enough. If only all manufacturers, retailers, consumers and everyone in the supply chain takes good care so that security is embedded into the product from the beginning only then will it be possible to unite us against them.[16]

References

[1] NextShift Robotics. 2021. *The Basics of Autonomous Mobile Robots | NextShift Robotics*. [online] Available at: <https://nextshiftrobotics.com/podcast/basics/> [Accessed 5 July 2021].

[2] Youtube.com. 2021. *Before you continue to YouTube*. [online] Available at: <https://www.youtube.com/watch?v=IMPbKVb8y8s> [Accessed 5 July 2021].

[3] Asset Infinity Blog. 2021. *What Is IoT and How Is It Helpful in Asset Management? - Asset Infinity*. [online] Available at: <https://www.assetinfinity.com/blog/what-is-iot-and-how-is-it-helpful-in-asset-management> [Accessed 5 July 2021].

[4] Tutorialspoint.com. 2021. *IoT - Environmental Monitoring - Tutorialspoint*. [online] Available at: <https://www.tutorialspoint.com/internet_of_things/internet_of_things_environmental_monitoring.htm> [Accessed 5 July 2021].

[5] Pocket-lint. 2021. *Amazon Go and Amazon Fresh: How the 'Just walk out' tech works*. [online] Available at: <https://www.pocket-lint.com/gadgets/news/amazon/139650-what-is-amazon-go-where-is-it-and-how-does-it-work> [Accessed 5 July 2021].

[6] Cybercrime Magazine. 2021. *Cybercrime To Cost The World $10.5 Trillion Annually By 2025*. [online] Available at: <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/#:~:text=Cybersecurity%20Ventures%20expects%20global%20cybercrime,%243%20trillion%20USD%20in%202015.> [Accessed 5 July 2021].

[7] 2021. [online] Available at: <https://blog.cloudflare.com> [Accessed 5 July 2021].

[8] 2021. [online] Available at: <https://www.cloudflare.com/en-in/learning/ddos/what-is-a-ddos-attack/> [Accessed 5 July 2021].

[9] A10 Networks. 2021. *Five Most Famous DDoS Attacks and Then Some | A10 Networks*. [online] Available at: <https://www.a10networks.com/blog/5-most-famous-ddos-attacks/> [Accessed 5 July 2021].

ISSN 2350-109X
www.indianscholar.co.in

Indian Scholar

An International Multidisciplinary Research e-Journal

[10] Learning Center. 2021. *What is APT (Advanced Persistent Threat) | APT Security | Imperva*. [online] Available at: <https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/> [Accessed 5 July 2021].
[11] https://www.miningreview.com/gold/emerging-cyber-threats-in-the-manufacturing-and-mining-sectors/. 2021. [online] Available at: <https://www.miningreview.com/gold/emerging-cyber-threats-in-the-manufacturing-and-mining-sectors/> [Accessed 5 July 2021].
[12] News, C., News, k. and attack, K., 2021. *Kolkata ATMs under sophisticated hacking attack | Kolkata News - Times of India*. [online] The Times of India. Available at: <https://timesofindia.indiatimes.com/city/kolkata/kol-atms-under-sophisticated-hacking-attack/articleshow/83096894.cms> [Accessed 5 July 2021].
[13] Cyber Security Hub. 2021. *Another Cyber Attack Affecting Water Supply*. [online] Available at: <https://www.cshub.com/attacks/articles/another-cyber-attack-affecting-water-supply> [Accessed 5 July 2021].
[14] 2021. [online] Available at: <https://www.livemint.com/news/world/ransomware-hits-hundreds-of-us-companies-security-firm-says-11625273463663.html> [Accessed 5 July 2021].
[15] mint, 2021. REvil ransomware strike may have hit more targets. p.single page.
[16] Ziniosedge.com. 2021. [online] Available at: <https://ziniosedge.com/iot-security-threats-in-retail-how-do-we-eliminate-them/> [Accessed 5 July 2021].