Cyber Attacks in the Era of Covid-19 and Possible Solution Domains

1st Isaac Chin Eian
School of Computer Science & Engineering,
Taylor's University
Selangor, Malaysia
zackteddy39@gmail.com

2nd Lim Ka Yong
School of Computer Science & Engineering,
Taylor's University
Selangor, Malaysia
limkayong001117@gmail.com

3rd Majesty Yeap Xiao Li
School of Computer Science & Engineering,
Taylor's University
Selangor, Malaysia
majesty2910@gmail.com

4th Yeo Hui Qi
School of Computer Science & Engineering,
Taylor's University
Selangor, Malaysia
jessie.yeohq@gmail.com

5th Fatima-tuz-Zahra
School of Computer Science & Engineering,
Taylor's University
Selangor, Malaysia
fatemah.tuz.zahra@gmail.com

Abstract – In this COVID-19 pandemic, the use and dependency on Internet has grown exponentially. The number of people doing online activities such as e-learning, remote working, online shopping and others have increased. This has also led to increased vulnerability to cyber crimes. Cyber security attacks have become a serious problem. The common types of cyber security attacks are phishing, malware, ransomware, social engineering, identity theft and denial-of-service. The attackers target the victims in order to get their credential information or financial benefits. Those people who are doing online activities are vulnerable to cyber threats. This is because the network is not safe. The attackers are able to code according to the weaknesses of the Internet. Once the attackers hack into the devices, they have the root access and can do whatever they want to do with the device. In this research paper, the concept of cyber security attack and detailed research about real attacks are discussed. This is followed by detailed review about the recent cyber security attacks with a critical analysis. Moreover, the paper will be proposing the latest research contribution of cyber security during COVID-19 and the implementation scenario which will give the examples about how the companies maintain privacy as well as the limitations. Then, the paper will be discussing the reasons that people are vulnerable to cyber security and the unique solution to the problems stated. Finally, this paper will conclude with an in-depth analysis with the future direction for cyber security research.

1 Introduction

Cybersecurity has become an important discipline of research due to the increase in usage of digital devices which are interconnected and linked with the Internet. Where this extensive interconnection has provided convenience to users, it has also increased vulnerability to cybersecurity issues. Researchers are focusing on this domain to provide solutions against the threats posed by attackers [1]. Common targets of cyber attacks are organizational information systems, networks and infrastructures or personal devices and networks. Since the invention of the computer in the late 1980s, cyberattacks have evolved greatly along with the innovation of information technology. Unfortunately, this increases the "surface" of coverage for cyberattacks to occur.

There are three factors that motivates the reason for cyber attacks; the spectacularity factor, the vulnerability factor and the fear factor. The spectacularity factor relates to the impact or damage that can be achieved by the malicious attacker. The damages may include a drop in publicity of the target as well as loss of income of an organization or an individual. An example of this factor is if a Denial of Service attack was launched, large e-commerce companies such as Amazon, Lazada, or TaoBao business will be halted by the attack and creates a loss in income. The next factor relates to the vulnerability of an organization or individual. Since some companies might be using outdated security systems and infrastructure, this makes them an easy target for attackers. The fear factor implies the attacker's intention to instill fear in their victims. Ransomware attacks are a good example of the fear factor being utilized by the malicious party to get what they want from the victim.

The methods or type of attacks can vary and can be divided into passive and active attacks. Passive attacks usually involve eavesdropping and monitoring of a target's incoming and outgoing traffic. Active attacks involve attackers inflicting actual harm by altering, destroying and interrupting traffic or packets. Most cyber attacks involve both passive and active attacks and follow the structure of the Cyber Kill Chain intrusion model as seen in Fig. 1. The first step, reconnaissance involves research about the target and gathering information such as email address and various personal information. Next, weaponization is when the attacker creates a malware application which allows remote access of the target's device. Delivery involves making the transmission of the weaponized malware to the target location. Common modes of transport are emails, portable USBs and web platforms. The next step is exploitation, where the injected file launches and executes the malware code. Installation is when the trojan has infected the target environment and establishes its presence. Command and control involves an established connection between the malicious party and the target in order to launch and execute commands to control the target environment. Finally, action on objective is done after all the previous set up and is the final phase of the intrusion model. To achieve the attacker's objective, they can now collect information for misuse, block the user's accessibility to services on their device or even alter and plant false data (Detecting Cybercrime Activities, n.d.) [2].

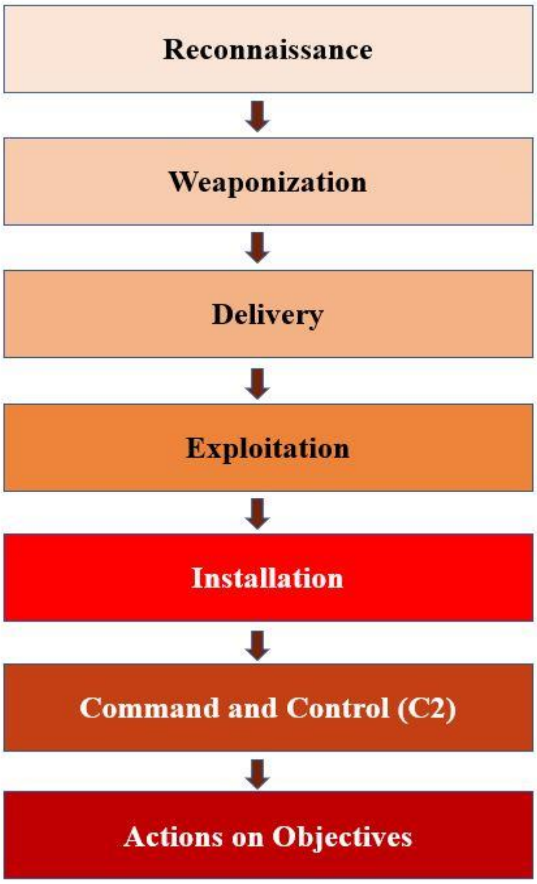

Fig. 1. Cyber Kill Chain Intrusion Model

During this recent COVID-19 pandemic, we can see that there have been an increase in cybersecurity attacks by nearly 5 times. Even so, these cyber attacks are not targeted to any single organization or entity specifically but hackers are exploiting the vulnerabilities that appear because many people are now working from home as well as the virus in general. The recent cyber attacks are showing up in the form of phishing emails and malware that relate to the COVID-19 virus. Every country is facing these attacks because everyone is looking for the most recent information about the virus, users will eventually click into the trap of the awaiting jaws of an attack. The higher the number of outbreak cases in a country, the higher the amount of what is known as lures as statistics show. Reports show approximately 60,000 emails that are related to the pandemic that contain malicious links and attachments. While there is an increase in cyber crime, there have not been many cases regarding an attack against specific organizations with visible vulnerabilities and hackers with a clear goal. (Elder, 2020) [3].

The first case we can explore is regarding stolen email addresses and passwords from organizations that have been working on fighting COVID-19 that were reported on April 21st, 2020. Organizations that were affected are the World Health Organization (WHO), World Bank, US Centers for Disease Control and Prevention (CDC), the Gates Foundations, the US National Institutes of Health (NIH), the Wuhan Institute of Virology. The hackers responsible are unknown but dumped the email addresses and passwords on online platforms such as 4chan, Pastebin and Twitter. From what was posted, it was reported that many of the passwords obtained were extremely weak, where some people had "password" as their email password. It is also suspected that the intrusion into their systems were not recent, and some of the emails might have come from previous branches of the organizations from years back. WHO reported that the leaked emails and passwords did not make a huge impact but did affect an older extranet system that has now been migrated to a more secure authentication system. The impact of this attack puts the general public in danger because emails can be used to impersonate organization staff in order to further exploit the naivety of the general public. The method of which these emails and passwords were obtained by hackers was not disclosed in the report by WHO but it is suspected that the motivation behind the attacks are because of certain conspiracy theories that blame these organizations for spreading the COVID-19 virus. (WHO, 2020) [4].

Since many people all over the world are working from home due to the pandemic, Zoom applications for online meetings have seen a growth in users but unfortunately also seen a rise in attacks due to several vulnerabilities. One of the threats is called "Zoom bombing" where hackers arrive in zoom meetings and classes in order to cause disruption or eavesdrop on conversations. Hackers have been known to use an online tool known as zWarDial that allows them to find meeting IDs that are not secured with passwords. Meetings that are not secured with a password allows intruders to slip into meetings without the host's knowledge. (Holmes, 2020) [5]. Zoom also fell victim to a credential stuffing attack especially since its recent growth in users. A credential stuffing attack is executed using lists of previously compromised user accounts and the assumption that users will reuse usernames and passwords for multiple service accounts. This attack is possible because Zoom does not compare registration usernames and passwords with known breached accounts details. Hackers most likely went through the process of analyzing the Zoom account registration procedure in order to determine if the attack was possible. A cybersecurity firm known as Cyble found more than 500,000 Zoom accounts on sale on the dark web on hacker forums. (CPO Magazine, 2020) [6].

The Department of Health and Human Services (HHS) faced a DDoS attack in March 2015. Hackers attempted to bombard HHS servers with millions of requests with the suspected motive of delaying HHS's response to assist COVID-19 cases. The department was able to evade the attack because of security measures that were already in place. The origin and party involved with the assault on their network has not yet been uncovered and not much information regarding this attack has been released. (Matthews, 2020) [7]. In another incident Italy's social security website, INPS was breached in April 2020. After Italian citizens rushed to apply for coronavirus relief packages, the website crashed due to large amounts of traffic and opened the door to an attack. Personal information of users such as names, home addresses, phone numbers and tax codes were made visible to everyone to see. If someone were to continuously refresh the page, different personal data shows up in the registration form for the relief package. The government recovered by rebooting the website with patches in place to remove any breaches that occurred. Based on an interview with Andrea Ganduglia, CEO of Frequenze Software states that anyone that visited the website between 9 and 11am on April 1st might have had their personal data exposed (Bannister, 2020) [8].

1.1 Recent Cybersecurity Attack Types

The first attack type we'll explore is Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. This type of attack bombards a target system to block service requests from clients, and it has occurred during the pandemic to slow down response to coronavirus cases. It can be launched from many host machines that have been infected with malware that allows the attacker control over them. DoS attacks do not give the attacker direct benefit unless the attack was launched by a competitor or launched in order to execute another type of attack. There are many ways to execute a DoS attack, such as SYN flood attack [9], teardrop attack, smurf attack, ping of death attack and botnets. Recent DoS attack scenarios we see in the news are attacks on HHS in 2020, GitHub in 2018, and BBC in 2015. From Fig. 2, we can observe the flow of commands from the attacker and the flow of attack traffic to the target in a DDoS attack.

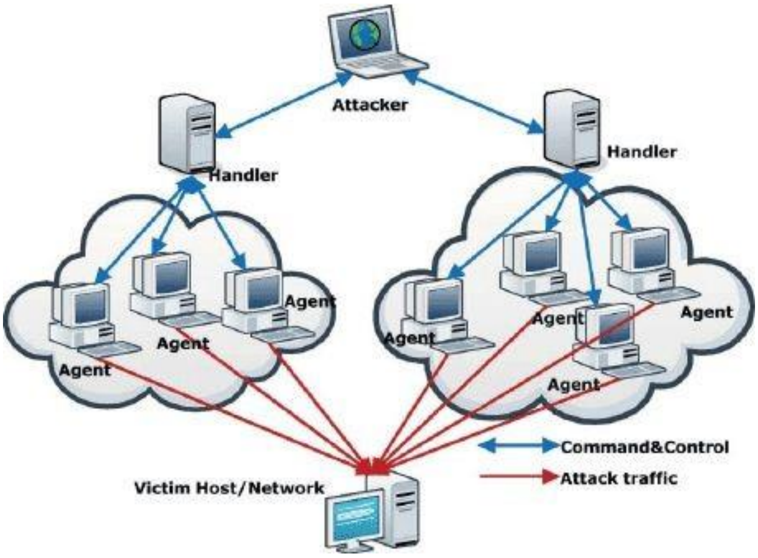

Fig. 2. Flow of commands from the attacker and the flow of attack traffic to the target in a DDoS attack [10]

Man in the Middle (MitM) attacks, as the name implies, is when the attacker intercepts the line of communication between a client and server. This type of attack happens to be a threat to those who are working from home especially those without security guidance from their companies. There are 2 ways of execution; session hijacking, and replay. Session hijacking involves the malicious party masking their device with the IP address of the target client through IP spoofing in order to trick the server into thinking it is still maintaining session with the client. Replay attack involves the attacker saving past messages and packets [11] in order to send them to the host server at a later time to impersonate the original client that sent them. Although, replay attacks can be countered with the implementation of session timestamps. Fig. 3 shows the attacker that has obtained the client's IP address and is communicating with the web application while the victim has been disconnected from the session.

doi:10.20944/preprints202009.0630.v1

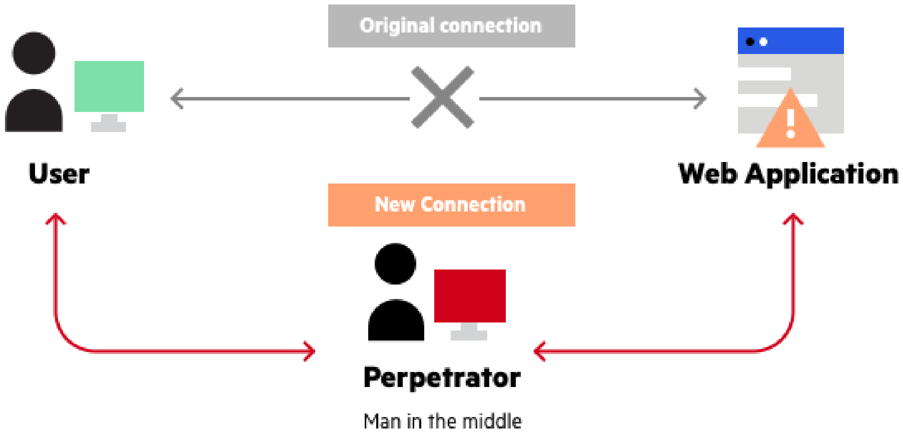

Fig. 3. Man in the Middle attack demonstration [12]

One of the most common types of cyber attacks are phishing and spear phishing attacks. Phishing attacks impersonate emails or social media links from legitimate sources in order to obtain personal information from a target. This type of attack involves the naivety of human curiosity and technical trickery. Forms of delivery of phishing attacks are through emails that contain malware, or links to illegitimate websites or downloads. Spear phishing is a targeted type of phishing attack, which involves reconnaissance on the target and creating personalized messages that are relevant to the target. This makes spear phishing difficult to identify, defend and prevent. Spear phishing can be done with website cloning to obtain social media logins or email spoofing by forging the origin of the email or sender's email address. An example of spear phishing attack is a case from 2011 involving the RSA security unit from EMC corp. The target was fooled by a Flash object that was embedded in an excel file and therefore falling victim. In order to avoid phishing attacks researchers have proposed various statistical and machine learning approaches. One such proposal includes a solution to phishing website detection by employing feature selection algorithm to assess whether a website is legitimate or malicious [13].

Another type of attacks include password attacks which are still effective in this era due to its wide use to authenticate users in an information system. Passwords can be obtained through sniffing, brute force, dictionary attack and sometimes phishing. Brute force approach involves guessing the password by using common combinations, and this is especially effective if the target used a weak password. Example of this can be seen in Citrix System's breach from October 2018 to March 2019 through password spraying. The dictionary attack approach involves a list of common passwords to attempt in order to gain access to a target's account, device or network. This can be done by comparing the encrypted password from the target and encrypted list of common passwords. Example of dictionary attack was back in January 2009 when a hacker known as GMZ hacked into a twitter account that belonged to a staff of Twitter and was able to compromise some other high profile accounts by resetting their password and allowing access to other hackers. Some other password-related attacks include shoulder surfing and spyware. Solutions to these have been proposed in the form of enhanced password models such as one presented in [14] where multi-elemental approach is proposed to protect mobile devices from aforementioned two attacks.

Another approach to trigger attacks is by using malicious software also known as malware which is any unwanted software that is installed onto a target device without the user's consent. Malware can use the device to spread to other devices by replicating itself and hiding in useful applications. There are many forms of malware attacks including, macro viruses, file infectors, ransomware, trojans, logic bombs, etc. By far, ransomware is the most common form of malware because it costs less and easier to execute compared to other forms of malware, therefore increasing the payout of the attack. Ransomware encrypts a target's valuable or sensitive data in order to block access. The target must then pay a ransom in order for the preservation and safe return of the data. The attackers can threaten to delete or resell the data on the black market and this causes trouble especially for those in a high ranking position or big companies. Encrypting the files with cryptoviral extortion technique makes it even harder to reverse the encryption process without the decryption key and forces targets to give in to the ransom which is usually paid in cryptocurrency. Examples of famous ransomware attacks are Locky in 2016, WannaCry in 2017 and NotPetya in 2016 (Melnick, 2020) [15]. Static analysis and dynamic analysis are two commonly used techniques to detect malware while some researchers have proposed hybrid of these two methods such as in [16] where authors have proposed a classifier-based approach to detect malware in android applications while using a combination of static and dynamic analysis along with other parameters.

2 Literature Review

There are many latest research contributions on cyber security. One of the recent research papers in analysis of cyber security crimes during COVID-19 period. In [17] authors highlighted the cyber attacks and cyber crimes related to the pandemic. All the cyber crimes and cyber attacks are becoming more and more serious nowadays and there are a lot of victims who are targeted. This is because the attackers want to gain some benefit from them such as financial benefits. During COVID-19 pandemic, this circumstance has become much more serious compared to other periods. This research showed a timeline of the events that is related to cyber attacks or cyber crimes during COVID-19 pandemic. The report showed that there are 43 cyber attacks and cyber crimes and they can be categorized into phishing, hacking, denial-of-service (DoS), malware, financial fraud, pharming and extortion. This proved that during COVID-19 pandemic, the rate of cyber attacks and cyber crimes increased. This is because most of the activities are online. Not only that, the number of unemployed also increased based on the research. Then, there will be more people staying online at home. These people will try to gain some financial benefits through cyber attacks or cyber crimes. The analysis in this research paper can raise the awareness of government, media and other institutions. The analysis can show to the public which they need to take some actions in order to prevent cyber attacks or cyber crimes [17].

Another recent research presents 10 deadly cyber security threats amid COVID-19 [18]. Due to the rapid spread of COVID-19, there is an increase in the use of technology. This will cause more cyber risk of cyber attack. E-learning and working from home environments cause many new users signing up for Microsoft Team, Zoom and other online meeting software applications. This might cause the users to become vulnerable to cyber attack. Especially for those users they are using Zoom, Zoom has undergone many security and privacy issues. This research paper shows that the top ten cyber security issues are DDoS attack, malicious domains, malicious websites, malware, ransomware, spam emails, malicious social media messaging, business email compromise, mobile application and browsing application. The research shows that there were a total of 907k spam messages, 737 malware attacks, and 48k malicious links since April 2020. Furthermore, there were about 220 times increase in spam email during February to March 2020. Fig. 4. shows that there is an increase in malware and phishing websites were visited during COVID-19 [18].

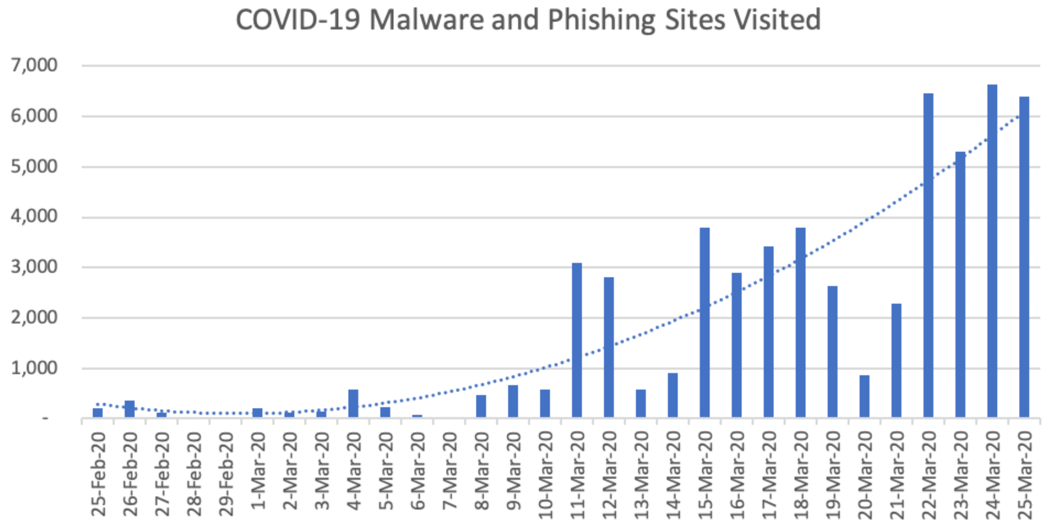

Fig. 4. Graph representing increase in visiting malware and phishing websites during COVID-19 [19]

Furthermore, there is another research about the cyber security impact during COVID-19 as a challenge to internet safety. This research explains how the attackers used the weaknesses of humans due to coronavirus fear. The attackers will send some coronavirus malware, coronavirus spam emails and coronavirus fake information websites. The attackers used the anxiety of people as they are trying to get new information online everyday. This makes people vulnerable to cyber attacks as they will click in any posts or links that are related to COVID-19. A malware can cause the loss of data. The attackers will send some emails related to coronavirus so that the victims will click in the link in the email. One of the famous coronavirus malware is Emotet which is a malware that can get the financial information of the victims and the victims would not notice that. The attackers are able to get financial benefits from the victims through this Emotet malware. For coronavirus spam emails, the attackers use social engineering techniques in order to cheat people by using their weaknesses. Then, the attackers are able to obtain the credential information of the victims like password or credit card number. They can do anything they want with all the credential information. Lastly, for fake coronavirus information, the attackers will use some fake websites which are related to corona virus such as how to prevent coronavirus, awareness and news so that the users will subscribe to the website and the attackers will get financial benefit (Kenneth, Olajide, 2020) [20].

In [21] multi-level cybercrime models in the era of pandemic are discussed and crime incidents influenced by Covid-19 are analyzed. During COVID-19 pandemic, there is an increase of online users. The research shows that there are more than 43,000 new users. However, there is also an increase in cyber attacks. More online users cause the attackers to take advantage of it. Fig. 5 shows that there are about 61% of phishing among cyber attacks. The organizations that are usually targeted are social networking sites, online banking sites and firms of technology. This is because the online activities such as e-learning, working from home, online shopping, entertainment, communication, donations, news report and social applications are easy to be targeted by the cyber attackers [21]. Researchers are actively participating in finding out possible solution domains to mitigate the problems that have arisen and escalated due to the pandemic. Some of them include the use of telecommunication technology, big data analytics, 3D printing, and artificial intelligence [22]. It is expected that effective solutions can be developed using these technologies, although the ongoing work is still in its infant stages.

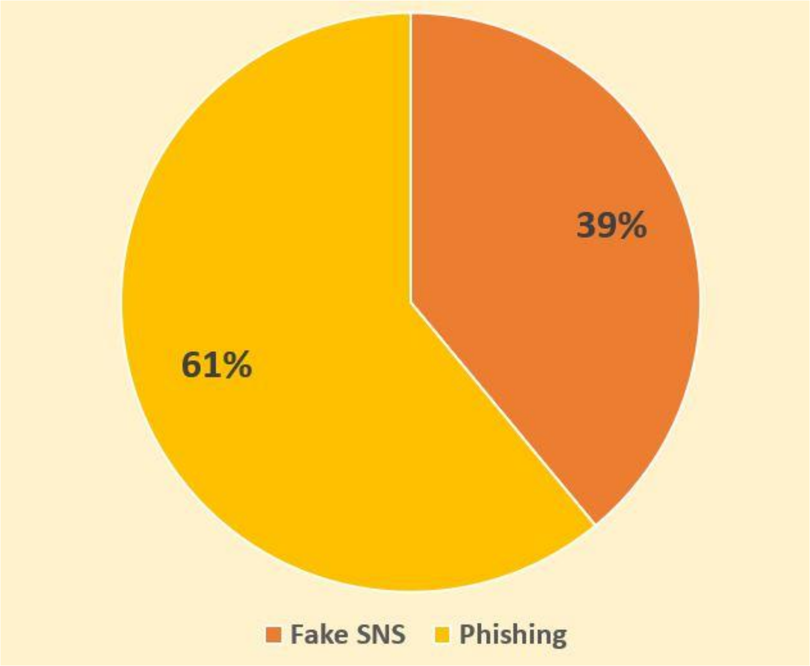

Fig. 5. Active cybercrime incidents [21]

Similarly, in [23] authors have studied the surge in cyber crimes and security challenges faced by people during COVID-19 such as increases in hacking and data stealing issues. Digital gadget users were surveyed and the graph in Fig. 6 shows that 48% of people agree that they had provided some data to online sites during COVID-19 pandemic whereas 13.40% of people did not provide any data to online sites. 40.20% of people remained uncertain. Some also agreed that their data and information was either stolen or otherwise attacked by cyber criminals during COVID-19 pandemic.

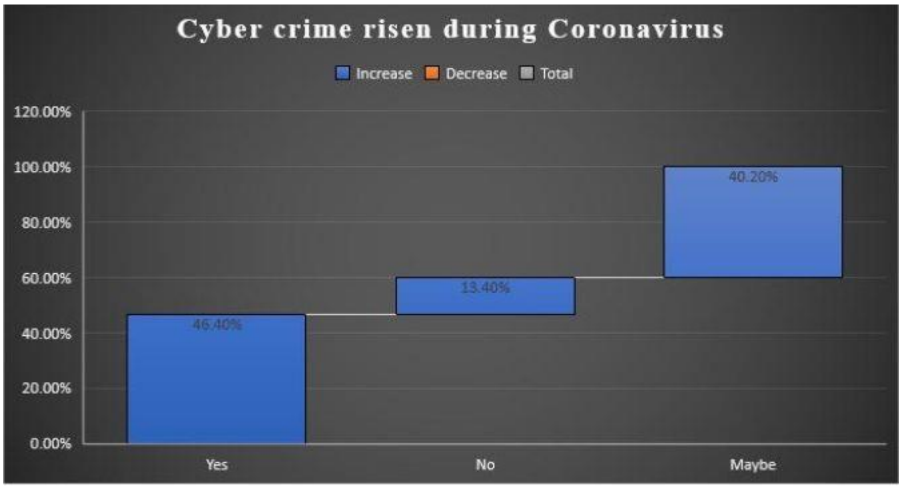

Fig. 6. Graph representing level of increase in cybercrimes during pandemic [23]

3 Security Deployment Scenarios

Many companies took extra precautionary steps during this Covid-19 season to protect their customers' data seeing that many cybersecurity cases arise in this unprecedented time. In this report, the network infrastructure and security system of two technology giants in the IT industry, Google and Microsoft will be further detailed. Google protects its clients' data by employing more than 500 full-time professionals in computer security to handle data security [24]. There are a few key points on how Google network infrastructure works. For instance, Google runs its server centers by utilizing custom equipment, and the equipment runs on a custom file system and operating system. Every one of these systems is tested and improved for execution and maximum security. As Google handles the whole hardware system, it can rapidly react to any shortcomings or threats that may occur. Additionally, Google's network architecture and developed applications are intended to run on the greatest availability and reliability. The information collected is distributed and circulated over Google's servers and data centers. In the case where a machine falls flat or even a whole datacenter is down, the data will in any case still be available. Each of the datacenters is tightly monitored and implements security measures such as biometric identification and laser-based surveillance. Google also works and owns data centers worldwide to ensure the services needed are ongoing 24/7 [25].

Furthermore, as in Google's security report, Google ensures its products are examined by security and privacy experts all through the product life cycle [26]. This will guarantee the data is taken care of properly and no unauthorized access is permitted or conceivable. Patches are constantly deployed through automated network analysis. Google also actively scans for vulnerabilities and consistently performs penetration testing, external audits, and quality assurance. Google's security report also emphasizes on encryption and is the pioneer cloud service provider to ensure full forward secrecy on its service. All data are encrypted and protected by security technology such as TLS and HTTPS while moving internally between not only internal servers but to devices as well. Encryption wise, Google changed the length of the RSA encryption keys from 1024 bits to 2048 bits and the keys are renewed every few weeks. Consequently, to stay updated on cybersecurity issues, Google maintained a close relationship with the security research community [26].

Other than Google, Microsoft also has its own customized network infrastructure that protects its clients' personal data. Microsoft network infrastructure is based on a layered approach, this is to prevent unauthorized personnel from accessing the data. There are five layers of physical security in Microsoft datacenters. Upon arriving on Microsoft datacenter, one must request access and be able to provide a valid reason for the visit, an example for a valid reason will be for auditing purposes. Then only the Microsoft employees will grant access for the visit. The granted access is only for the approved area that is required, and the permissions are only limited to an amount of time. If the permission expires, the individual has to request and gain approval again **[27]**. Microsoft also sets the facility perimeter on its data centers. All individuals that arrive at the data centers are required to have a well-structured access point which are tall fences that are made of steel and concrete. All data centers are surrounded by surveillance cameras, and all footage is supervised by a security team. Other than fences, the entrance of the datacenter is built with two-factor authentication biometrics. An individual must pass through the entrance in order to enter the datacenter [27].

Correspondingly, when entering the datacenter, one has to pass through a full-body metal detection screening. In order to minimize the risk of unauthorized information being transported out or entering into the datacenter, Microsoft only allows approved devices to the datacenter floor. Moreover, they are security cameras observing the front and back of every server rack. Just as entering the datacenter floor, a full-body metal scan is required again before leaving the floor. And finally before leaving the datacenter, an extra security scan is performed again. All visitor badges must be returned to Microsoft upon leaving the facility [27]. However, there are some limitations faced when we are trying to research the network infrastructure of the companies. For instance, we are unable to conduct physical interviews with the employees of Google and Microsoft as we are limited by the current rules of social distancing. Moreover, we believe that their internal security architecture is considered to be sensitive and hence the information is private and confidential.

4 Issues and Challenges

During COVID-19 pandemic, people are vulnerable to cyber security because of the increase of online activities such as e-learning, work from home, online shopping and others. In this developed digital world, it is hard for everyone to remain updated about the new information of the devices and how to stay safe online. Furthermore, people also need to ensure all their software and devices such as computers, i-Pads and mobile phones are up-to-date. However, most of the people choose to ignore the notification that requests them to update their device because they think that the updating process is troublesome and requires an amount of memory on their device. This will make their device become vulnerable to cyber security because the hackers can hack into their device easily as it is not up-to-date [28]. Moreover, phishing attacks also make people vulnerable to cyber security during COVID-19 pandemic. The attackers will try to trick a person to give them some important information or their credential data such as username, password and credit card numbers so that the attackers can penetrate into the victims' devices and download malware in their devices. The most common type of phishing attack is using email as their main tool. The victims will receive a spoofed email and if they click on the malicious link, ransomware or malware can be installed in their devices. Phishing attacks are normally used to target an individual or an organization so that the attackers can take advantage from them.

Furthermore, there are many security bugs in software applications that cause people to become vulnerable to cyber security. People might download more software applications during COVID-19 pandemic such as Zoom, Microsoft Teams and Google meeting. This is because hackers can write code based on the weaknesses of the software application. A device can be easily targeted if the software applications have many unknown security bugs. The hackers will package the code into a malware and install it in the device and make the particular device vulnerable and compromise the device by using the malware to attack the weaknesses of the software. Then the device will compromise and the hackers can take unauthorized control of the device. They can access anything and steal the victims' information [29]. Several solutions have been proposed to increase the security level of digital devices and applications in various domains, such as unmanned vehicles which are a cause of increased privacy issues. In [30] authors have proposed to develop a privacy detection model which will increase security in commercial drones.

Hidden backdoor program is also one of the vulnerabilities to cyber security during COVID-19 pandemic. Hidden backdoor program is a program that purposefully creates computer security vulnerabilities. At the point when a manufacturer of the computer can install any problem or code in order to permit it into a device so that they have the authority to access the device for some purposes such as repairing. This is called a backdoor program. However, when a backdoor program is installed silently, then it is called a hidden backdoor program. The customer would not know the existence of this backdoor program. This will cause many vulnerabilities as the attacker can easily access the user's devices and compromise the computer device [31].

Another area of digital technologies which is highly vulnerable to security attacks is Internet of Things (IoT) and smart infrastructure [32]. In theory, these domains are well established from convenience viewpoint. However, they are one of the major causes of increases in security attacks because of their insecure implementation. Main reason is interconnectivity of devices with each other and with the Internet and generation of huge amounts of data on this network. Attackers can obtain sensitive data like health information from such smart systems (Fig. 7) . They usually consist of resource-constrained devices running on low-power and lossy networks. Due to these characteristics, traditional security protocols cannot be used in these systems. Moreover, there is a lack of suitable protocols as well as appropriate security tools which can be integrated for secure deployment. Researchers are working in this field to provide solutions, however, it is still in its early phases in comparison to exponential insecure deployment. One of the many solutions can be a lightweight and secure authentication scheme, an example of which is a scheme proposed by authors in [33]. However, there are still many gaps and loopholes in secure implementation of IoT devices due to which they have become an easy target of security and privacy attacks.

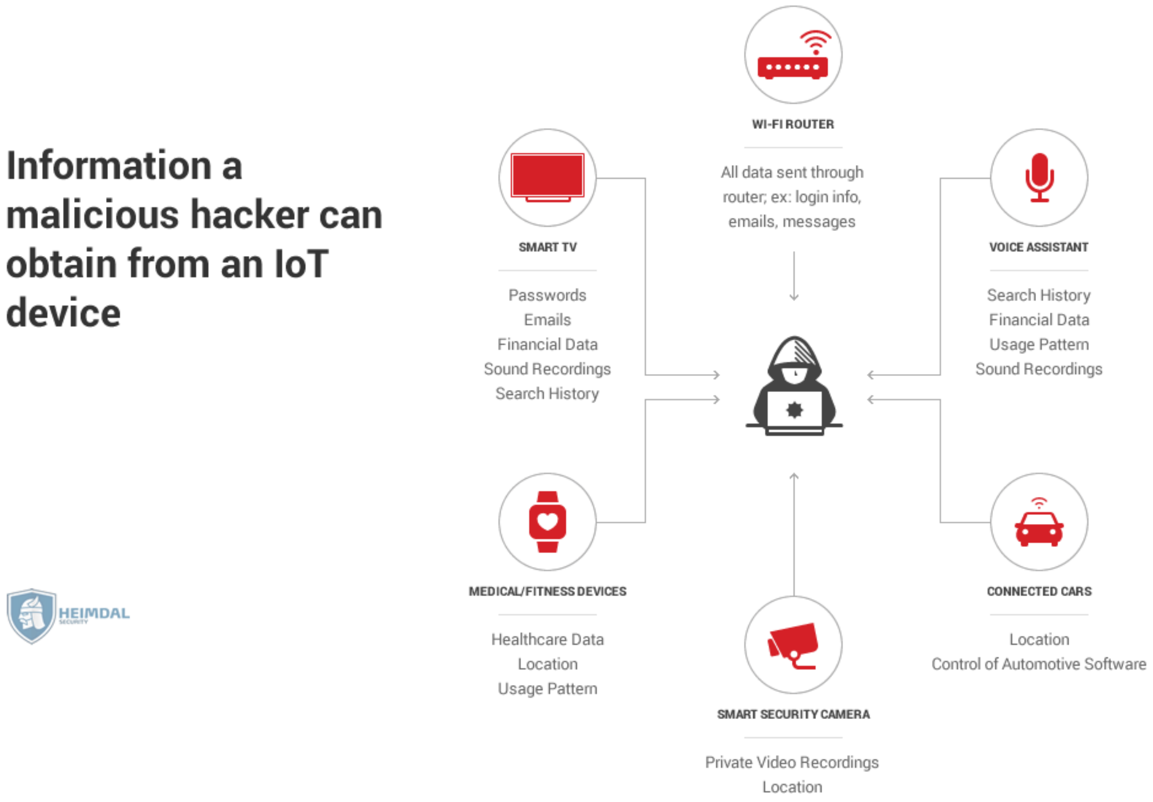

Fig. 7. Information a malicious hacker can obtain from an IoT device [34]

Lastly, using malware as an attack tool is also vulnerable to cyber security during this COVID-19 pandemic period. Malware is a program which can harm a computer device. There are many types of malware such as ransomware, trojans, worms, botnets, adware and spyware. A malware can access a device and steal sensitive personal data like username, password, address and credit card number. It also can monitor the activity of the computer. A malware can cause damage to the data and system of the device. Malware can be spread by using email or a website. There will be a link for the users to click in. Once the users click the link, a malware will be installed in their device. So, people need to be aware of this vulnerability to protect themselves against malware [35].

5 Unique Solution

Technology is advancing rapidly and with that there is an increase of cyberattacks and elevated frequency of malicious attacks. We suggest a unique solution whereby we use the advancing technology of artificial intelligence to detect and prevent threats before it begins rooting itself in a computer system. The artificial intelligence program will act primarily to scan, verify and raise alerts of suspicious packets coming into the system. We can think of this like an advanced defender or firewall program. It's secondary task will also be to scan and review current stored files in the computer system and raise alerts for them. The artificial intelligence implementation gathers data from a server in which it liaises with to view patterns or common attacks on the system. Therefore, in two parts, the program will act to filter out all files and data as to whether it is harmful, deactivating, auto-deleting or cutting off its access to the computer system unless approved by the user. The artificial intelligence system will utilize its machine learning capabilities as when a user rules out a potential threat as harmful, the program will learn of its pattern and send the data to a server where it will store the pattern. All other computer systems using this program will be able to refer to the stored patterns on the server. This will ensure that the system learns these attacks and can prevent them efficiently before it begins.

This solution, as stated before relies on advanced and advancing technology to do the brunt of the work. Even though the system will be used both passively and actively in run-time, take up more than usual resources, and may cause frustrations in the beginning, this solution is crafted to exist effectively in the long term by growing stronger and more intelligent as time goes by. The more data it collects, the more confident the program is to automatically eliminate and disrupt attacks before it inflicts damage to the computer system. This, in its smallest form will be very effective on stand-alone devices but work better on servers as more data will be inputted. This is highly valuable for companies like Google who value the security of their data and users' data greatly. It could also work incredibly well for businesses both small and large. Moreover, in this time of COVID-19 pandemic, where attacks are more frequent, it could speed up the machine learning process of the program, making it highly effective quickly. This program has the potential to remove the troubles of having to do a lot of the manual work of a user with a firewall or security program as if the program is confident enough, it will execute the directives automatically. The program would also be able to detect scams and phishing attempts when receiving email data. It will alert and warn the user of potential scams and with reasoning. The system also rules out the problem of having security bugs and backdoors in the software as it learns progressively and automatically "patching" itself. Lastly, it will also detect instilled malware in the system already and attempt to eliminate it before it inflicts greater damage.

It is recommended that this program be implemented in phases. First, in a simpler environment whereby weaker attacks are used to probe the program. Next, higher and more robust attacks will be injected to probe the system. After a period of time probing using simple attacks, Moving on to the next phase where system penetration experts and ethical hackers will attempt to bypass the program. The final phase will be where the program is actually fully implemented and provided for all paid users, whether corporate or personal. At each phase, the program is expected to learn continually the attack patterns and eventually anticipate and react to an attack. The confidence rate that the program can react correctly and execute logical directives and counter-attacks should be at least 95% before moving to the next phase. This program should be able to work closely and side-by-side with existing system firewalls as well. Our recommendation for effective usage would be to use this in a centralized network whereby all data traffic is filtered at the hub or server. As stated before, in a present time where COVID-19 forces isolation and self-quarantine, it is a good time for a program like this to be allocated resources to strengthen it. Another recommendation would be to use this program on fresh and clean computers so that the program can see the difference in the current system versus an infected system.

Spreading awareness about the importance of cybersecurity should be of high priority. It is better to educate people about cybersecurity, common cyberthreats and prevention. Like they say, prevention is better than cure. If given the task of spreading awareness about cybersecurity, we would take to a few methods. Firstly, we should utilize social media advertising. Surprisingly, most internet users are not aware of the dangers of using the internet. Advertising on these platforms, like Facebook and Instagram, have been known to subtly influence social media users. Therefore, using this psychological aspect, we can raise awareness or implant a conscious thought of cybersecurity. This aims not to instill fear of cyberattacks but to combat it using simple but effective prevention methods. Also, in terms of the corporate and business side, employees should attend seminars pertaining to cybersecurity to make aware common tactics and methods of scammers. This will also help with employees not in the IT field to detect hacking attempts or attacks on their workstations if it occurs. In the long run, the costs to send employees to seminars will be a small amount as compared with the amount of money saved from recovering from attacks and scams in a company prospect.

6 Conclusion

It is undeniable that cybersecurity is an uprising issue, especially during these unprecedented times. With the issue of the Covid-19 pandemic, many business owners, companies, and organizations have turned to digital solutions to ensure the longevity of their businesses. But with the implementation of digital solutions, many organizations ignore the threats and dangers of the cybersecurity attacks. Based on research, it is found that most business owners only take action on countering cybersecurity attacks after experiencing the attacks firsthand. While it may be lucky for some businesses, in serious cases, the data that are compromised might heavily affect the organization and customers and therefore leads the company to be unable to continue on normal operations. In our opinion, to ensure that incidents like the above did not happen, precautionary steps should be taken from the front end to the back end of every process. Every organization should own security policy, purchase equipment or software that are needed to maintain the security, hiring security professionals such as ethical hackers to perform penetration testing and only allow administrators to modify and access sensitive information.

In the future, cybersecurity will be developed with the integration of the latest technologies, such as Artificial Intelligence, Blockchain, Internet of Things, and much more. This is proven when 61% of the enterprises say, according to Forbes in 2019, that they are unable to detect data breach without the help of Artificial Intelligence. Traditional services can be expensive and risky, but with Blockchain, any transaction or trade processes within asset management are shown to be highly secure and more efficient as there is no room for error with Blockchain. With enormous amounts of data being generated day by day, Big Data can be riskier than ever. Professionals can work on their way to research and utilize machine learning to protect these data. All in all, while all these threats may sound like a totally new challenge to the next generation of security professionals, all these may only be achievable when these new technologies are firmly implemented in our daily lives. As for the current situation, every user should start taking baby steps of protecting your own personal data before it is compromised by unauthorized users.

References

[1]. Humayun, M., Niazi, M., Jhanjhi, N. et al. Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. Arab J Sci Eng (2020). https://doi.org/10.1007/s13369-019-04319-2

[2]. Detecting Cybercrime Activities. (n.d.). Cyber-Attacks Structure. [online] Available at: https://www.web-scan.eu/cyber-attacks-structure/#:~:text=and%20secure%20cyb erspace [Accessed 2 Jul. 2020].

[3]. Elder, J. (2020). Hackers have hit every country on Earth with coronavirus-themed cyberattacks. [online] Business Insider. Available at: https://www.businessinsider.com/microsoft-research-shows-coronavirus-cyberattacks-in-every-country-2020-4 [Accessed 2 Jul. 2020].

[4]. WHO (2020). WHO reports fivefold increase in cyber attacks, urges vigilance. [online]. Available at: https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance

[5]. Holmes, A. (2020). Protect your Zoom meetings with a password now — otherwise, you're leaving the door wide open for hackers to "Zoom-bomb." [online] Business Insider. Available at: https://www.businessinsider.com/protect-zoom-meetings-password-hackers-zoom-bombing-2020-4 [Accessed 2 Jul. 2020].

[6]. CPO Magazine (2020). Half a Million Zoom Accounts Compromised by Credential Stuffing, Sold on Dark Web. [online] Available at: https://www.cpomagazine.com/cyber-security/half-a-million-zoom-accounts-compromised-by-credential-stuffing-sold-on-dark-web/.

[7]. Matthews, K. (2020). Incident Of The Week: Health and Human Services Hit with Security Breach. [online] Cyber Security Hub. Available at: https://www.cshub.com/attacks/articles/incident-of-the-week-iotw-health-and-hu man-services-hit-with-security-breach.

[8]. Bannister, A (2020). INPS hack: Italy's social security website back online following cyber-attack claims. [online] Available at: https://portswigger.net/daily-swig/inps-hack-italys-social-security website-back-o nline-following-cyber-attack-claims [Accessed 2 Jul. 2020].

[9]. K. Hussain, S.J. Hussain, NZ. Jhanjhi and M. Humayun, "SYN Flood Attack Detection based on Bayes Estimator (SFADBE) For MANET", International Conference on Computer and Information Sciences (ICCIS), 1-4, 2019. https://doi.org/10.1109/ICCISci.2019.8716416

[10]. Alnakhalny, Redhwan & Anbar, Mohammed & Manickam, Selvakumar & Alomari, Esraa. (2015). An intelligent ICMPv6 DDoS flooding-attack detection framework (V6IIDS) using back-propagation neural network. IETE Technical Review. 1. 10.1080/02564602.2015.1098576.

[11]. Melnick, J. (2020). Top 10 Most Common Types of Cyber Attacks. [online]. Available at: https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/

[12]. Imperva (n.d.). Man in the middle (MITM) attack. [image]. Available at: https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/

[13]. Alyssa Anne Ubing, Syukrina Kamilia Binti Jasmi, Azween Abdullah, NZ Jhanjhi and Mahadevan Supramaniam, "Phishing Website Detection: An Improved Accuracy through Feature Selection and Ensemble Learning" International Journal of Advanced Computer Science and Applications(IJACSA), 10(1), 2019. http://dx.doi.org/10.14569/IJACSA.2019.0100133

[14]. Teoh Joo Fong, Azween Abdullah, NZ Jhanjhi, Mahadevan Supramaniam, "The Coin Passcode – A Shoulder-Surfing Proof Graphical Password Authentication Model for Mobile Devices", in International Journal of Advanced Computer Science and Applications (IJACSA), Vol 10, No, 1, pp. 302-308, 2019

[15]. Melnick, J., 2020. Top 10 Most Common Types Of Cyber Attacks. [online] Blog.netwrix.com. Available at: https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/ [Accessed 4 July 2020].

[16]. S. J. Hussain, U. Ahmed, H. Liaquat, S. Mir, N. Jhanjhi and M. Humayun, "IMIAD: Intelligent Malware

Identification for Android Platform," 2019 International Conference on Computer and Information Sciences (ICCIS), Sakaka, Saudi Arabia, 2019, pp. 1-6, doi: http://dx.doi.org/10.1109/ICCISci.2019.8716471

[17]. Harjinder, S., Lynsay, S., Nurse, J.R.C., Erola, A., Epiphaniou, G., Maple, C. & Bellekens, X. (2020). Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic.

[18]. Khan, Navid Ali; Brohi, Sarfraz Nawaz; Zaman, Noor (2020): Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic. TechRxiv. Preprint. https://doi.org/10.36227/techrxiv.12278792.v1

[19]. Security, M. (2020). Sophisticated COVID-19-Based Attacks Leverage PDF Attachments and SaaS to Bypass Defenses. [image]. Available at: https://www.menlosecurity.com/blog/sophisticated-covid-19-based-phishing-attacks-leverage-pdf-attachments-and-saas-to-bypass-defenses

[20]. Kenneth, O. and Olajide, A. (2020). Tackling the Cybersecurity Impacts of the Coronavirus Outbreak as a Challenge to Internet Safety. IJITE, vol. 8, issue 2, ISSN: 2321-1776.

[21]. Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. European Journal of Information Systems, pp.1–16. Netwrix.com. (2018). Top 10 Most Common Types of Cyber Attacks. [online] Available at: https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/.

[22]. Brohi, Sarfraz Nawaz; Jhanjhi, NZ; Brohi, Nida Nawaz; Brohi, Muhammad Nawaz (2020): Key Applications of State-of-the-Art Technologies to Mitigate and Eliminate COVID-19. TechRxiv. Preprint. https://doi.org/10.36227/techrxiv.12115596.v2

[23]. Kashif, M., Aziz-Ur-Rehman, Javed, M.K. and Pandey, D. (2020). A Surge in Cyber-Crime during COVID-19. Indonesian Journal of Social and Environmental Issues, [online] 1(2), pp.48–52. Available at: https://www.ojs.literacyinstitute.org/index.php/ijsei/article/view/22/38 [Accessed 2 Jul. 2020].

[24]. G Suite (n.d.). Google Has a Strong Security Culture. Google Cloud Security and Compliance Whitepaper [online]. Available at: https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-cloud-security-and-compliance-whitepaper.pdf

[25]. Google Data Centers (n.d.). Data and Security. [online]. Available at: https://www.google.com/about/datacenters/data-security/

[26]. Google Cloud (2020). Google security whitepaper. [online]. Available at: https://cloud.google.com/security/overview/whitepaper

[27]. Lehr, B., Kess, B., BasWassenaar, Baldwin, M., et al. (2020). Azure facilities, premises, and physical security. IN Azure Security Documentation. [online]. Available at: https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security

[28]. Protect Seniors Online. (2017). Cyber Attacks: What Makes Me Vulnerable? [online] Available at: https://www.protectseniorsonline.com/resources/cyber-attacks/ [Accessed 2 Jul. 2020].

[29]. Norton. (2019). Norton. [online] Available at: https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnera bilities-work-30sectech.html.

[30]. M. Saleh, N. Jhanjhi, A. Abdullah and Fatima-tuz-Zahra, "Proposing a Privacy Protection Model in Case of Civilian Drone," 2020 22nd International Conference on Advanced Communication Technology (ICACT), Phoenix Park, PyeongChang,, Korea (South), 2020, pp. 596-602, https://doi.org/10.23919/ICACT48636.2020.9061508

[31]. Dosal, E. (2018). Top 5 Cybersecurity Threats and Vulnerabilities. [online] Compuquip.com. Available

at: https://www.compuquip.com/blog/top-5-cybersecurity-threats-and-vulnerabilities.

[32]. Dhuha Khalid Alferidah, NZ Jhanjhi, A Review on Security and Privacy Issues and Challenges in Internet of Things, in International Journal of Computer Science and Network Security IJCSNS, 2020, vol 20, issue 4, pp.263-286

[33]. M. Almulhim, and N. Zaman, "Proposing secure and lightweight authentication scheme for IoT based E-health applications", 2018 20th International Conference on Advanced Communication Technology (ICACT), 481-487. https://doi.org/10.23919/ICACT.2018.8323802

[34]. Paul, C. (2017). IoT Security: All You Need to Know and Apply. HEIMDAL Security. [online]. Available at: https://heimdalsecurity.com/blog/internet-of-things-security/

[35]. Margaret, R., Rob, W., Debra, L. (2019). How malware works. TechTarget, SearchSecurity. [online]. Available at: https://searchsecurity.techtarget.com/definition/malware [Accessed 2 Jul. 2020].