IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cyberthreats in the Covid-19 Pandemic and Possible Solutions Domains

[1]Amit Mahajan, [2]Priyanka Gupta

[1]Student, [2]Assitant Professor

[1]School of Computer Science & Engineering,

[1]Lovely Professional University, Jalandhar, Punjab

Abstract: The usage and reliance on the Internet have increased exponentially since the COVID-19 pandemic. The number of people participating in online activities such as e-learning, remote working, and online shopping has risen. As a result, cybercriminals have become more vulnerable. Cybersecurity breaches have become a major issue. Phishing, malware, ransomware, social engineering, identity theft, and denial-of-service attacks are all common forms of cybersecurity attacks. Victims are targeted by attackers to obtain their credentials or financial benefits. People who engage in online activities are at risk of cyber-attacks. This is because the network is not safe. The attackers can code in a way that exploits the Internet's flaws. When attackers gain root access to a computer, they have complete control over it and can do whatever they want with it. The definition of a cybersecurity attack is explored in this research paper, as well as extensive research on actual attacks. Following that, a comprehensive overview of recent cybersecurity attacks is presented, along with a critical analysis. Furthermore, the paper will propose the most recent cybersecurity research contribution at COVID-19, as well as a practical overview with examples of how businesses protect privacy as well as limitations. The paper would then go over the reasons why people are vulnerable to cybersecurity and the one-of-a-kind approach to the issues posed. Finally, this paper will end with an in-depth examination of cybersecurity research's future directions.

Index Terms **- COVID-19 pandemic, cybercriminals, Phishing, cybersecurity, Zoom Bombing**

I. INTRODUCTION

Owing to the increased use of digital devices that are interconnected and linked to the Internet, cybersecurity has become a significant research discipline. Although users have gained from this pervasive interconnection, it has also enhanced users' exposure to cybersecurity threats. Experts in the field are concentrating their efforts in this field to establish responses to the posed dangers by unwanted persons [1]. Personal computers, networks, as well as computer applications for businesses, and infrastructures are common targets of cyber-attacks. Since the invention of the computer in the late 1980s, cyberattacks have evolved greatly in parallel with the development in information technology. Unfortunately, this expands the “surface” of coverage available for cyberattacks.

The three reasons that inspire cyber-attacks are the spectacularity factor, risk factor, and fear factor. The spectacularity factor applies to the impact or damage that a malicious attacker might be able to inflict. A reduction in the target's exposure, as well as a lack of income for a corporation or an individual, can be among the losses. For example, if a DoS attack is commenced, e-commerce giants include as Amazon, Lazada, or Taobao’s operations would be interrupted, resulting in a loss of revenue. The next consideration is an organization's or individual's weakness. Since some businesses may have obsolete security systems and infrastructure, they are an easy target for hackers. The attacker's intention to instill fear in their victims is indicated by the fear factor. Ransomware attacks are an excellent example of a malicious party exploiting the victim's paranoia to get what they like.

Attacks may be categorized as passive or active based on their tactics or styles. Passive attacks include eavesdropping and monitoring a target's incoming and outgoing traffic. Active attacks include attackers modifying, damaging, or interrupting traffic or packets to cause real damage. Figure 1. depicts the Cyber Kill Chain intrusion model's composition. Most cyber-attacks use the Cyber Kill Chain intrusion model, which includes both passive and aggressive attacks. The first move is reconnaissance, which includes conducting research on the target and collecting information such as the target's email address and other personal details. The attacker then creates a malware application that enables remote access to the target's computer, which is known as weaponization. Delivery refers to the act of sending weaponized malware to its intended destination. Emails, USB drives, and online networks are all popular means of communication. The malware code is then launched and executed by the inserted file in the next stage, exploitation. The trojan is said to be deployed after it has entered the target area and established its existence. Command and control are where a malicious party creates a connection with the target to launch and execute orders to control the target location. Finally, after all of the previous setup, the intrusion model's final step is an operation on goal. To accomplish their goal, the hacker can now gather data for misuse, block the user's access to resources on their device, or even change and plant false data. [2].

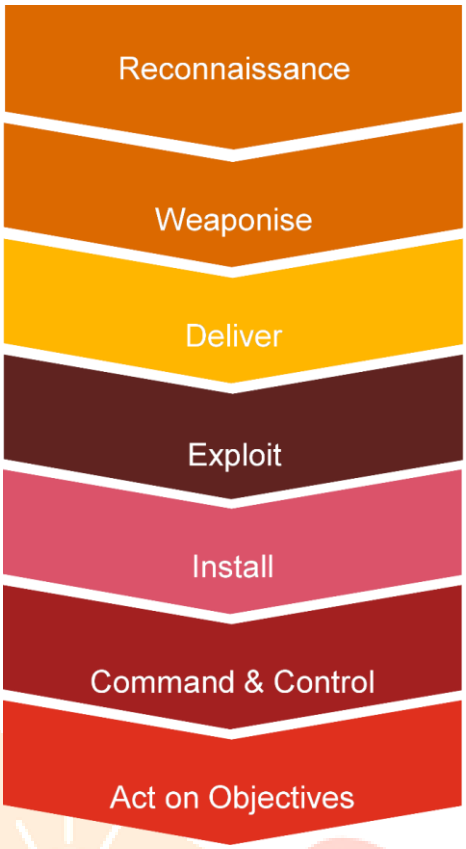

Fig. 1. Cyber Kill Chain Intrusion Model

We can see that cybersecurity attacks increased by nearly 5 times during the recent COVID-19 pandemic. Even so, these cyber-attacks are not directly aimed against any one company or entity; rather, hackers are taking advantage of the weaknesses that have emerged as a consequence of the virus in general, as well as the fact that many people are now working from home. The COVID-19 virus has been the target of recent cyber-attacks in the form of phishing emails and malware. Since everybody is searching for the most up-to-date information about the virus, users can finally click into the pit of the attack's waiting jaws. According to statistics, the more epidemic cases there are in an area, the more lures there are. About 60,000 emails related to the pandemic, according to estimates, carry malware connections and attachments. Although cybercrime is on the rise, there haven't been many instances of attacks against individual entities with established vulnerabilities or hackers with a specific target. (Elder, 2020) [3].

The first case we can look at is the theft of email addresses and passwords from organizations working to combat COVID-19, which was announced on April 21st, 2020. The World Health Organization (WHO), the World Bank, CDC, the Gates Foundation, NIH, and the Wuhan Institute of Virology were among the organizations affected. The identity of the hackers is unclear, but they leaked email addresses and passwords on 4chan, Pastebin, and Twitter. Many of the passwords obtained, according to what was written, were extremely weak, with some people using the word "password" as their email password. It's also conceivable that the intrusion into their networks was not new, and that some of the emails originated from former divisions of the company dating back years. The leaked emails and passwords did not have a major effect, according to WHO, but they did affect an older extranet scheme, which was later upgraded to a more reliable authentication system. since emails may be used to impersonate business employees to further exploit the public's gullibility The WHO study does not expose the method by which hackers gained access to these emails and passwords, although it is suspected that the attacks were inspired by conspiracy theories accusing these organizations of spreading the COVID-19 virus. (WHO, 2020) [4].

As a result of the pandemic, many people around the world are working from home, and Users of Zoom apps for online meetings have increased, but unfortunately, so have attacks due to numerous vulnerabilities. The "Zoom bombing" is one of the dangers in which hackers enter Zoom meetings and classes to interrupt or listen in during discussions. The unwanted persons or attackers have been known to use zWarDial, an online platform that aids in the discovery of meeting IDs that aren't password-protected. Intruders will sneak into meetings without the host's knowledge if they are not password-protected (Holmes, 2020) [5]. Zoom was also a victim of a credential stuffing attack, which has become more common as the company's user base has grown. A credential stuffing attack is carried out using lists of already infected user accounts and the assumption that users will reuse usernames and passwords for separate service accounts. Since Zoom does not equate registration usernames and passwords with established breached account data, this attack is possible. Hackers most certainly went through the process of testing the Zoom account registration protocol to see whether they could carry out an attack. According to Cyble, a cryptography firm, more than 500,000 Zoom profiles were for sale on the dark web on hacker pages. (CPO Magazine, 2020) [6].

In March 2015, the Department of Health and Human Services (HHS) was subjected to a distributed denial-of-service attack. To delay the department's response to COVID-19 events, hackers attempted to spam HHS servers with millions of requests. The agency was able to stop the attack due to existing security procedures. The source and group responsible for the attack on their network have yet to be identified, and little information about the attack has been released. (Matthews, 2020) [7]. Another incident occurred in April 2020, when Italy's social security website, INPS, was hacked. The website crashed due to high traffic after Italian people rushed to apply for coronavirus relief packages, allowing an assault to take place. Users' personal information is made public, including their identities, home addresses, phone numbers, and tax codes. If a user continues checking the page, the relief kit registration form will display different personal details. The government was able to recover by restarting the website with updates

in place to fix any security flaws that had occurred. Anyone who visited the website between 9 a.m. and 11 a.m., according to Andrea Ganduglia, CEO of Frequenze Software, on April 1st had their personal information revealed (Bannister, 2020) [8].

II. LITERATURE REVIEW

There are numerous recent contributions to cybersecurity research. During the COVID-19 timeframe, one of the most recent research papers in the study of cybersecurity crimes was published. The writers of [9] focused on the pandemic's cyber-attacks and cybercrimes. In recent years, both cybercrimes and cyber-attacks have become more intense, and the number of victims has increased. This is due to the attackers' need to take something from them, such as financial gain. In comparison to other times, the situation has gotten much worse during the COVID-19 pandemic. During the COVID-19 pandemic, this study provided a timeline of events related to cyber-attacks or cybercrimes. According to the report, there are 43 different types of cyber-attacks and cybercrimes, including phishing, hacking, DoS, malware, financial fraud, pharming, and extortion. This showed that during the COVID-19 pandemic, the number of cyber-attacks and cybercrime rose. This is because the majority of the operations are conducted online. Not only that, but according to the study, the number of unemployed people has grown. Then, more people would stay at home and use the internet. These individuals may attempt to profit financially from cyber-attacks or cybercrime. The findings of this research paper have the potential to raise awareness among the government, media, and other organizations. The findings would inform the general public what actions they can take to stop cyber-attacks or cybercrime [9].

In the wake of COVID-19, a new study identifies ten deadly cybersecurity risks [10]. The use of technology is increasing as a result of the rapid spread of COVID-19. This would increase the likelihood of a cyber-attack. As a result of e-learning and operating from home settings, many new customers sign up for Microsoft Team, Zoom, and other online meeting software applications. As a result, users could become vulnerable to cyber-attacks. Zoom has had numerous security and privacy issues, especially for those users who use it. According to this research report, the top ten cybersecurity threats include DDoS attacks, malicious domains, malicious websites, malware, ransomware, spam communications, malicious social networking messaging, business email breach, mobile server, and surfing program. Since April 2020, there have been 907k spam messages, 737 malware attacks, and 48k malicious links, according to the report. Furthermore, between February and March 2020, there was a 220 percent rise in spam email. Figure 2 depicts a rise in the number of malware and phishing websites visited during COVID-19 [10].

Besides, during COVID-19, another study was conducted on the cybersecurity effect as a threat to internet safety. This study describes how the attackers exploited human vulnerabilities caused by coronavirus fear. Coronavirus malware, coronavirus spam emails, and coronavirus fake knowledge websites will be sent by the attackers. When they attempted to get new information online every day, the perpetrators preyed on people's paranoia. People are vulnerable to cyber-attacks as a result of their ability to click

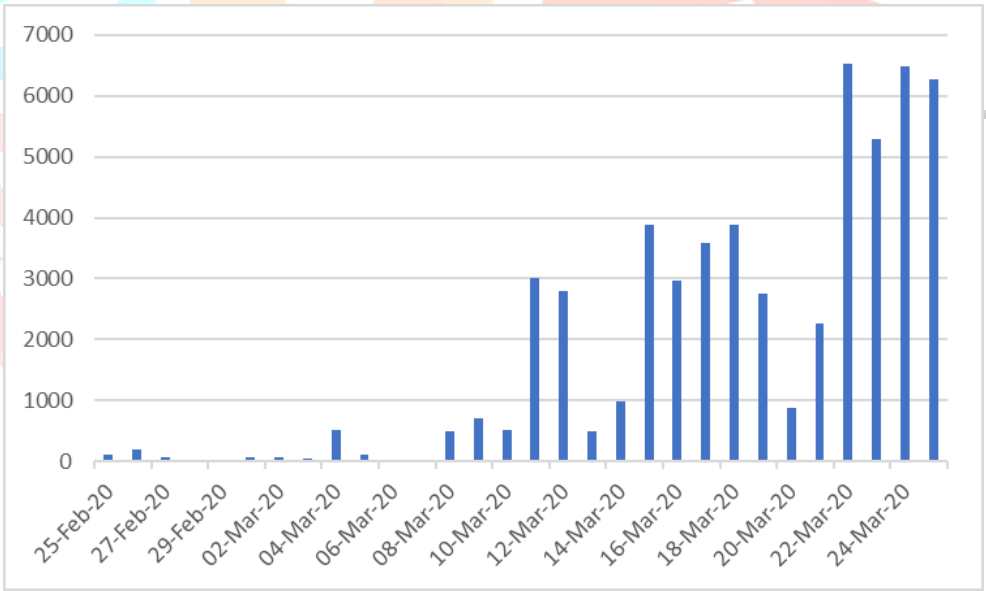

Fig. 2. Graph depicting the rise in malware and phishing website visits during COVID-19 [11]

on some COVID-19-related articles or connections. Malware can result in data loss. The hackers will send the suspects coronavirus-related emails in the hopes that they will click on the document's link. Emotet is a well-known coronavirus that can steal financial information without the victims' knowledge. The attackers will extort money from the suspects using the Emotet malware. Coronavirus spam email hackers use social engineering techniques to trick people by leveraging their weaknesses. The hackers are then able to obtain the victims' credential information, such as passwords or credit card numbers. They can do whatever they want with the credentials information. Finally, the hackers will use some fake websites which are related to coronavirus material, such as how to prevent coronavirus, awareness, and news, to entice users to subscribe to the website, allowing the attackers to profit financially. (Kenneth, Olajide, 2020) [12].

In [13] multi-level cybercrime models in the age of pandemics, as well as crime events affected by Covid-19. There is a spike in online users during the COVID-19 pandemic. According to the study, there are over 43,000 new users. Cyber-attacks, on the other hand, are on the rise. When the number of people who use the internet increases, so does the number of attackers who use it. Figure 3 shows that phishing accounts for about 61% of all cyber-attacks. Social networking sites, online banking sites, and technology companies are the most often targeted organizations. This is because internet practices such as e-learning, operating from home, online shopping, movies, networking, contributions, news reports, and social apps are easy targets for cybercriminals [13]. Researchers are working hard to define alternative response domains for the problems that have emerged and worsened as a

result of the pandemic. Telecommunications technology, big data analytics, 3D printing, and artificial intelligence are just a few of them [14]. While the study is still in its early stages, it is expected that successful solutions will be built using these technologies.

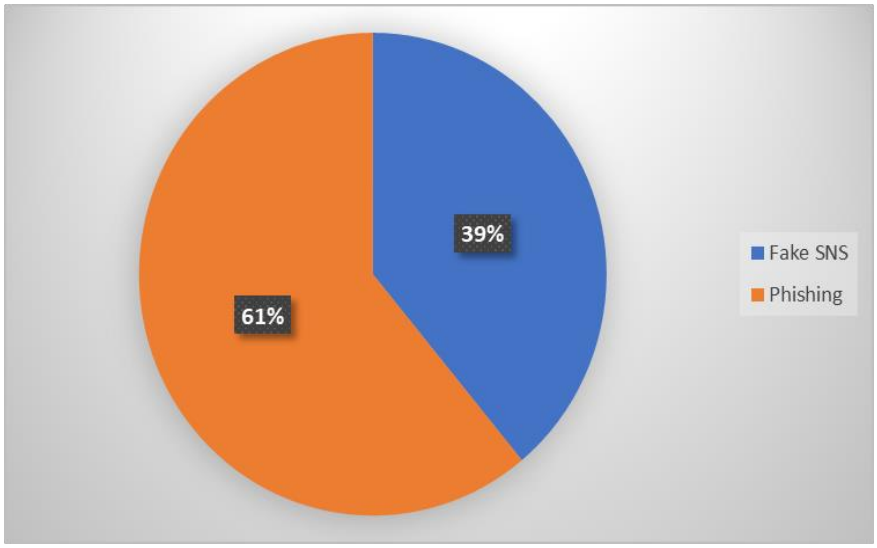

Fig. 3. Active cybercrime incidents

Similarly, the authors of [15] investigated the rise in cybercrime and security threats that people faced during COVID-19, such as increased hacking and data theft issues. Users of digital gadgets were polled, and According to the graph in Fig. 4, 48% accept that they sent any data to web pages during the COVID-19 pandemic, while 13.40 percent did not provide any data. 40.20 percent of people were also undecided. During the COVID-19 pandemic, some people said Cybercriminals stole or otherwise targeted their data and documents.

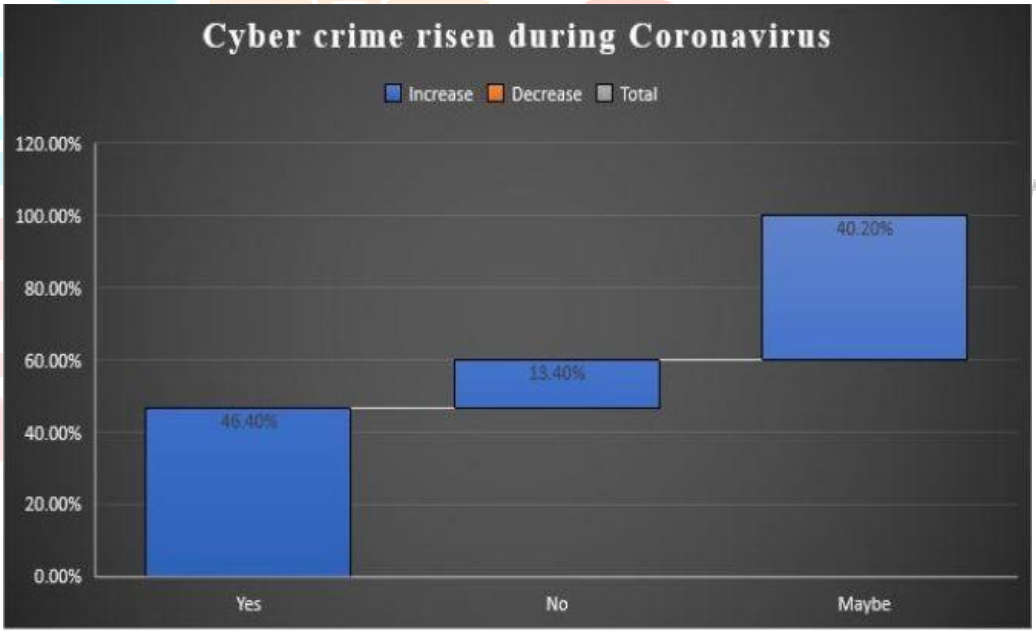

Fig. 4. Graph depicting the rise of cybercrime since the pandemic [15]

III. Increased Threats and Vulnerabilities

The NIST CSF Protect function lays out the necessary protections to ensure that essential infrastructure resources are delivered. The Protect feature aids in limiting or containing the effects of a possible cybersecurity incident. New attack vectors have arisen, leveraging COVID-19 anxiety and fears, as well as the lack of on-site staff support, and have received considerable media and cybersecurity industry attention. Table 2 shows examples of CSF PROTECT/DETECT operation in the industry. The following are some of them.

ZOOM Bombing— Trolling hackers can steal authentication credentials and insert offensive content (such as pornographic materials and violent images) into apparently safe collaborative online meetings thanks to security and privacy flaws in teleconferencing software. Interference with academic networks, such as a thesis defense delivered through university teleconference, is an example of a ZOOM bombing exploit.

Table 1. Threats and vulnerabilities caused by the coronavirus.

Threats and vulnerabilities	**Online resource**
ZOOM bombing	https://delta.ncsu.edu/news/2020/04/02/zoom-security-and privacy
Spyware and phishing	https://www.infosecurity-magazine.com/news/covid19-drive-phishing-emails-667/
Malware and phishing	https://www.webarxsecurity.com/covid-19-cyber-attacks/
Health check—ISPs, cloud providers, UCaaS during pandemic	https://www.networkworld.com/article/3534130/covid-19-weeklyhealth-check-of-isps-cloud-providers-and-conferencing-services.html

Table 2. Sample of malware and phishing attacks reported during coronavirus crisis.

Date	**Description of cyberattack**	**Type of attacks**
April 8, 2020	The risk of being exposed to hacked e-commerce websites is higher than it has ever been. In March, there was a 26% rise in web skimming	Malware
April 8, 2020	"Latest vaccine release for coronavirus (COVID-19)" mall spam spreads Nanocore RAT malware	Malware
April 8, 2020	NCSC advisory: COVID-19 exploited by malicious cyber actors	Social engineering
April 8, 2020	Fake COVID19 website is spreading Firebird RAT via fake DHL emails	Malware
April 8, 2020	Under COVID-19, the rush to embrace online learning exposes schools to cyberattacks	Zoom bombing
April 8, 2020	To get around protections, sophisticated COVID-19-based phishing attacks use PDF attachments and SaaS	Phishing, malware
April 8, 2020	The CDC has issued an alert about COVID-19-related phone scams and phishing attacks	Phishing

Source: (Webarxsecurity Website, https://www.webarxsecurity.com.)

COVID-19 Phishing Attacks— There were false, malicious emails that claimed to be from the Centers for Disease Control and Prevention, according to FBI bulletins (CDC). They either had malware attachments or were attempting to steal user credentials.

Malware— A Corona Trojan is an example of malware that overwrites the master boot record and disables hard disc storage. During the pandemic, ransomware attacks on healthcare systems have increased. Table 2 depicts malware and phishing attack snapshots.

Network Availability— Although core communication networks and clouds maintained adequate performance despite significant traffic increases, some collaborative applications experienced spikes in service outages, as shown in Table 1.

The NIST CSF Detect feature determines the tasks that should be performed to detect the occurrence of a cybersecurity incident. As shown in Table 2, the Detect mechanism enables timely detection of cybersecurity events.

IV. Security Deployment Scenarios

CEOs are often asked, "What keeps you up at night?" The CEO's response to the latest COVID-19 threats could well be "everything!" Security Architect Partners (SAP), a strategic consulting company, advises transparent dialogues at the CxO management level, incorporating core COVID-19 cybersecurity concerns such as employee morale, BC, telecommuting, and supply chain management into regular executive meetings. SAP's guidelines for addressing COVID-19's top security priorities include:

- securing remote access;
- mitigating increased fraud and malware threats;

- assessing new suppliers' (and changes to existing supplier's security posture);
- protecting core information system availability and security;
- refactoring security program priorities, architectures, and budgets;
- managing workforce morale; and
- aligning with business leadership.

The NIST CSF Respond role involves activities that should be carried out in response to a detected cybersecurity incident. The ability to contain the impact of a possible cybersecurity incident is aided by the Respond feature.

Table 3. Cybersecurity risk mitigation and response to the coronavirus.

Cybersecurity management response	**Online resource**
CxO Education (security architects partners)	https://security-architect.com/waking-up-to-the-new-covid-19-cybersecurity-reality/
COVID-19 Joint Acquisition Task Force	https://www.acq.osd.mil/jatf.html
US DHS Cyber and Infrastructure Agency (CISA)	http://www.cisa.govsites/default/files/publications/ 20_0306_cisa_insights_risk_management_for_ novel_coronavirus.pdf
NIST SP 800-46 Guide to enterprise telework, remote access, and BYOD security	https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final

The use of the NIST CSF has long been integrated into the cybersecurity management fabric of risk reduction in the United States at the federal agency level. The Department of Homeland Security (DHS) and Department of Defense information portals, as seen in Table 3, are examples of agency responses to the pandemic. Contingency plans have been activated for all US government agencies, and service disruptions are still being restored. NIST special publication 800-46 provides guidelines on host protection, information security, network security, remote access, bring your own Device (BYOD), and telework in the field of remote access.

Many businesses took extra precautions to protect their customers' data during the Covid-19 season, given the high number of cybersecurity incidents that have occurred at this unprecedented time. The network infrastructure and security systems of two technology behemoths in the IT industry, Google and Microsoft, will be examined in greater depth in this article. Google safeguards the data of its customers by hiring more than 500 full-time information security professionals [16]. There are a few important things to remember when it comes to Google's network infrastructure. Google, for example, operates its data centers with specialized equipment that runs on a custom file system and operating system. Every one of these systems has been thoroughly tested and improved for optimum efficiency and security. Since Google controls the entire hardware system, it can respond quickly to any flaws or threats that might arise. Furthermore, Google's network architecture and built applications are designed to be as available and reliable as possible. The data is distributed and shared around Google's servers and data centers. Even if a computer fails or a data center goes down, the data will still be available. Each data center is closely monitored, and security measures including biometric identification and laser-based surveillance are in place. Google also partners with and operates data centers around the world to ensure that the resources needed are available at all times 24/7 [17].

Furthermore, Google ensures that its products are reviewed by security and privacy experts during the product life cycle, as stated in Google's security report [18]. This will ensure that the data is adequately protected and that no unauthorized access is allowed or possible. Patches are implemented regularly as a result of automated network reviews. Google also conducts regular penetration testing, external audits, and quality assurance to look for vulnerabilities. Google's security report also emphasizes encryption, and the company is the first cloud service provider to guarantee absolute forward secrecy. When traveling internally between not only internal servers but also computers, all data is encrypted and secured using encryption technologies such as TLS and HTTPS. Google increased the length of the RSA encryption keys from 1024 to 2048 bits in terms of encryption, and the keys are refreshed every few weeks. As a result, Google maintained a strong partnership with the security research community to remain current on cybersecurity issues [18].

Microsoft, like Google, has its customized network infrastructure that protects the personal data of its customers. To prevent unauthorized personnel from accessing data, Microsoft's network infrastructure is built on a layered approach. Microsoft datacenters have five layers of physical protection. When visiting the Microsoft datacenter, you must first request access and be able to give a valid reason for your visit; an example of a valid reason is auditing. The visit would then be restricted to Microsoft employees only. The permits given are only for the authorized area that is necessary, and they are only for a set period. If the permission expires, the person must reapply for permission. Microsoft's data centers also have a facility perimeter [19]. All visitors to the data centers are expected to pass through a well-structured access point, which consists of tall steel and concrete fences. Surveillance cameras cover all data centers, and all video is monitored by a security team. Aside from gates, the datacenter's entrance is secured with two-factor authentication biometrics. To gain access to the data center, one must first move through the door [19].

As a result, anyone entering the data center must undergo a full-body metal detector screening. Microsoft only allows licensed devices into the data center floor to reduce the possibility of unauthorized information being transported out or into the data center. Furthermore, security cameras track the front and back of each server rack. Before leaving the data center floor, a full-body metal

scan is needed, just as it was upon entering. Finally, before leaving the data center, an additional security scan is run. Upon exiting the facility, all visitor badges must be returned to Microsoft. However, there are some drawbacks when it comes to researching a company's network infrastructure [19]. For example, due to the current rules of social distancing, we are unable to perform physical interviews with employees of Google and Microsoft. Furthermore, we agree that their internal security infrastructure is sensitive and that the information is also private and confidential.

V. POSSIBLE SOLUTIONS

Technology is increasingly progressing, which has resulted in a rise in cyberattacks and a higher level of malicious attacks. We propose a novel approach in which we employ artificial intelligence to identify and avoid threats before they establish a foothold in a computer system. The artificial intelligence program's main function would be to search, verify, and raise alarms when suspicious packets enter the system. We may think of it as a more sophisticated version of a firewall or a protector. Its secondary role would be to search and review the computer system's existing stored data, as well as to generate notifications for them. The AI implementation collects data from a server with which it communicates to identify trends or popular attacks on the system. As a result, the software will work in two sections to sort out all files and data and see if they are harmful, then deactivate, auto-delete, or cut off their connection to the computer system unless the user approves. When a user rules out a possible threat as harmful, the artificial intelligence system will use its machine learning capabilities to learn of its pattern and send the data to a server where it will be stored. The stored patterns on the server will be accessible to all other computer systems that use this software. This will ensure that the system knows about these attacks and can effectively avoid them before they start.

As previously mentioned, the majority of the work is done through advanced and evolving technologies. Although the device will be used both passively and actively in run-time, may consume more resources than normal, and can trigger frustrations at first, this solution is designed to be successful in the long run by becoming stronger and more intelligent over time. The more information it gathers, the more secure the software is in its ability to detect and stop attacks before they cause harm to the computer system. This will be very useful on stand-alone devices in its simplest form but will operate better on servers because more data will be inputted. This is extremely useful for companies like Google, which place a high priority on the protection of their data and that of their users' data. It could also be very beneficial to both small and large companies. Furthermore, in this period of COVID-19 pandemic, when attacks are more common, it may be possible to speed up the program's machine-learning operation, making it highly successful more quickly. This software can eliminate the hassles of a user needing to do a lot of manual work with a firewall or security program, as the program can execute the instructions automatically if it is confident enough. When receiving email data, the software will be able to detect scams and phishing attempts. It will advise and notify the consumer of possible scams, and it will do so with logic. As it discovers and automatically "patches" itself, the machine also eliminates the possibility of security flaws and backdoors in the program. Finally, it can detect malware that has already been implanted in the device and attempt to remove it until it causes further harm.

This software should be implemented in stages, according to the experts. First, in a less complex environment with weaker attacks probing the software. The device would then be probed with higher and more robust attacks. After a period of probing with simple attacks, machine intrusion experts and ethical hackers will attempt to circumvent the software in the next process. The software will be completely introduced and available to all paying users, whether corporate or personal, in the final process. The program is supposed to learn attack patterns as it progresses through each step, ultimately anticipating and reacting to an attack. Before moving on to the next level, the program's ability to respond correctly and execute logical directives and counter-attacks should be at least 95%. This software should also be able to communicate with and operate alongside existing system firewalls. For best results, we suggest using this in a centralized network where all data traffic is filtered at the hub or server. As previously reported, now is a good time for a program like this to be given resources to improve it, as COVID-19 forces isolation and self-quarantine. Another suggestion is to run this software on new, clean machines so that it can detect the difference between the current system and an infected system.

It should be a top priority to raise awareness about the value of cybersecurity. It is preferable to teach people about cybersecurity, popular cyber threats, and how to avoid them. As the saying goes, prevention is preferable to treatment. If we were given the mission of raising cybersecurity awareness, we would use a variety of methods. To begin, we should make use of social media ads. Surprisingly, the majority of internet users are unaware of the risks associated with using the internet. Advertising on these sites, such as Facebook and Instagram, has been known to manipulate social media users subtly. As a result, we can raise consciousness or implant conscious thinking of cybersecurity by using this psychological element. This isn't about instilling fear of cyberattacks; rather, it's about presenting them with easy but successful prevention methods. In terms of the corporate and company side, workers can attend cybersecurity workshops to learn about common scammer techniques and methods. This would also assist non-IT workers in detecting hacking attempts or attacks on their workstations if they occur. In the long run, the costs of sending workers to seminars would be insignificant when compared to the money saved from recovering from attacks and scams in a company.

VI. CONCLUSION

It is undeniable that cybersecurity is a growing concern, especially in these extraordinary times. Due to the Covid-19 pandemic, many business owners, firms, and organizations have turned to digital solutions to ensure their businesses' long-term viability. However, several companies overlook the risks and hazards of cybersecurity attacks when implementing digital solutions. According to a study, most company owners only take steps to combat cybersecurity threats after being personally affected by them. Although some companies may be fortunate, in serious situations, the data that has been compromised may have a significant impact on the enterprise and its clients, causing the company to be unable to continue operations. To avoid accidents like the one described above, we believe that precautionary measures should be taken from the front end to the back end of any operation. Every company should have its security policy, buy security equipment or software, hire security experts such as ethical hackers to conduct penetration testing, and only allow administrators to change and access sensitive data.

Artificial intelligence, blockchain, the Internet of Things, and other cutting-edge technology can be used to improve cybersecurity throughout the future. This is shown by the fact that according to Forbes in 2019, 61 percent of businesses are unable to detect data breaches without the assistance of artificial intelligence. Traditional asset management services can be costly and

risky, but with Blockchain, any transaction or exchange processes are seen to be highly safe and reliable, as there is no space for error. With massive quantities of data being produced daily, Big Data is potentially riskier than ever. Professionals may use machine learning to secure these data when conducting research. Overall, while all of these threats may appear to the next generation of security practitioners as a completely new challenge, they may only be possible if these new technologies are fully integrated into our everyday lives. In light of the current situation, every user should begin taking small measures to secure their personal information before it is compromised by unauthorized users.

REFERENCES

[1] [1] Humayun, M., Niazi, M., Jhanjhi, N. et al. Threats to cybersecurity and Potential flaws: https://doi.org/10.1007/s13369-019-04319-2

[2] S. Cybercrime Exercise Detection. (n.d.). Structure of Cyber-Attacks. Available at https://www.webscan.eu/cyber-attacks-structure/#:~:text=and%20secure%20cyb airspace [Accessed 2 Jul. 2020].

[3] Elder, J. (2020). Cyberattacks based on the coronavirus have been launched against every country on the planet. Available at: https://www.businessinsider.com/microsoft-research showscoronavirus-cyberattacks-in-every-country-2020-4 [Accessed 2 Jul. 2020].

[4] WHO (2020) The World Health Organization (WHO) estimates a fivefold surge in cyber-attacks and encourages caution [online]. Available at: https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urgesvigilance

[5] Holmes, A. (2020). Protect your Zoom meetings with a password right now — otherwise, hackers would be able to "Zoom-bomb" them. [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). Credential Stuffing has compromised half a million Zoom accounts, which have been sold on the dark web.. [online] Available at: https://www.cpomagazine.com/cyber-security/half-a-million-zoom-accounts-com promised-by-credential-stuffing-sold-on-dark-web/.

[7] Matthews, K. (2020). Security Breach at the Department of Health and Human Services is this week's incident of the week.. [online] Cyber Security Hub. Available at: https://www.cshub.com/attacks/articles/incident-of-the-week-iotw-healthand-human-services-hit-with-security-breach

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

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

[10] 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

[11] 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-basedphishing-attacks-leverage-pdf-attachments-and-saas-to-bypass-defenses

[12] Kenneth, O. and Olajide, A. (2020). Managing the Cybersecurity Consequences of the Coronavirus Outbreak as a Threat to Internet Security. IGNITE, vol. 8, issue 2, ISSN: 2321-1776.

[13] Naidoo, R. (2020). A multi-level influence model of cybercrime based on COVID-19. The European Journal of Information Systems (EJIS) is a peer-re, 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/.

[14] 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

[15] Kashif, M., Aziz-Ur-Rehman, Javed, M.K. and Pandey, D. (2020). During COVID-19, there was a spike in cybercrime, according to the 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].

[16] 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

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

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

[19] Lehr, B., Kess, B., BasWassenaar, Baldwin, M., et al. (2020). Facilities, premises, and physical protection are all part of Azure. IN THE DOCUMENTATION ON ADOBE SECURITY. [online]. Available at: https://docs.microsoft.com/enus/azure/security/fundamentals/physical-security