Emerging Cyber Security Challenges after COVID Pandemic: A Survey

Arjun Choudhary[1], Gaurav Choudhary[2*], Kapil Pareek[1], Chetanya Kunndra[1], Jatin Luthra[3], and Nicola Dragoni[2]

[1]Department of Cyber Security, Sardar Patel University of Police, Security & Criminal Justice
Jodhpur, India
a.choudhary@policeuniversity.ac.in, spu19cskp@policeuniversity.ac.in
mtcs20ck@policeuniversity.ac.in

[2]DTU Compute, Department of Applied Mathematics and Computer Science
Technical University of Denmark, Denmark
gauch@dtu.dk, ndra@dtu.dk

[3]Department of Computer and Communication Engineering
The LNM Institute of Information Technology, Jaipur, India
jatinluthra14@gmail.com

Received: March 10, 2022; Accepted: May 1, 2022; Published: May 31, 2022

Abstract

In 2019, a virus infection, COVID-19, traveled across the oceans, gained foothold in many countries, and started infecting the citizens of those countries. Soon, this virus was labeled a "pandemic" by the World Health Organization and was subsequently dubbed the COVID-19 virus. With the virus spreading across the globe, countries started going into lockdowns to curb the spread of the infection. The world came to a halt as people were asked not to leave their homes, offices, and institutions were forcefully closed. This scenario was entirely unexpected for most countries, institutions, and individuals. Amid these lockdowns, people started flocking towards the virtual world. This pandemic showed us that things that were supposed to be conducted physically were now being conducted online. Work-from-home (WFH) and study-from-home (SFH) terms and culture came into existence to ensure continuity of services. While the world was upside down and was trying to understand these new dynamics, cybercriminals took advantage of the chaos and carried out the rampant cyber crime on already suffering people and organizations. Cybercriminals known to monetize any recent system changes took this as a golden opportunity and were ready with their new modus operandi during this pandemic. In this survey paper, we have assessed and classified cyber crimes committed during the pandemic across the world. During this period, Malware attacks, Data breaches, Banking frauds, Job frauds, etc., were common. To prevent rampant cyber crimes in such situations, we have also discussed future generation solutions to tackle such issues so that critical systems and procedural checks must be in place.

keyword: Cyber Security, Threats, Attacks, COVID-19 Pandemic, Cyber Future Generation Solutions

Journal of Internet Services and Information Security (JISIS), volume: 12, number: 2 (May), pp. 21-50
DOI:*10.22667/JISIS.2022.05.31.021*

*Corresponding author: DTU Compute, Department of Applied Mathematics and Computer Science, Technical University of Denmark, Richard Petersens Plads, 322, 219, 2800 Kgs. LyngbyDenmark, Denmark, Tel: +91-9828-1076-76, Web: `https://orbit.dtu.dk/en/persons/gaurav-choudhary`

Figure 1: The major cyber affected areas and potential attack surfaces targeted by attackers in COVID-19 Pandemic.

1 Introduction

The modern world faced an unimaginable form of threat at the end of 2019 called severe acute respiratory syndrome coronavirus 2 [1] or more popularly known as COVID-19, while this contagious virus forced the whole world to cower in their homes, cause mass panic, shortages of an essential daily item and forced the whole world to go into lockdown. It enabled cybercriminals to act more aggressively, preying on already scared people. This time, every individual, institution, or nation was reeling with the new daily norms. Cyber Criminals carried out a variety of new kinds of cyber crimes that caused harm not just to computer systems or IT resources but also to the minds and fortunes of the people.

While people were more focused on adjusting to their new lockdown life, setting up their remote at home offices, and sitting down to work, cybercriminals were more concentrated on evolving their modus operandi to incorporate the theme of COVID-19 into their attacks. The change in their attack methodologies and targets could be clearly seen as the pandemic progressed. When governments launched health tracking apps and notification systems, cybercriminals started phishing campaigns, creating fake apps similar to the original ones. When governments announced the breakthrough in research for vaccines, multiple pharmaceutical laboratories were targeted in an attempt to steal the study. When vaccines and relief works were being done, cybercriminals started Man in the middle attacks to dupe the people out of their sensitive information. Cybercriminals leveraging the mass panic to further their own causes is something that is not new; COVID-19 also saw a sharp increase in themed attacks. The major cyber affected areas and potential attack surfaces targeted by cyber criminals in COVID-19 pandemic is shown in figure 1.In addition to mass hysteria, strict lockdown guidelines helped cybercriminals evade the arm of the law as almost everyone was under lockdown during the initial phases of the pandemic and no suitable SOPs (Standard Operating Procedures) were in place to counteract such adverse situations and the threats arising from it. The WFH culture provided new opportunities to employees and employers

alike. Still, the lack of proper work from home guidelines, standard SOPs, system architecture for remote work in the beginning also provided cyber criminals a new attack surface to commit their crimes. The halt to the global supply chain brought down by the pandemic caused a shortage of medicines, daily supplies, and even protective gear. The list of scarce stores during the pandemic is long; the perpetrators again churned out even this situation. This shortage halted the daily routines of almost everyone around the earth and also allowed cybercriminals to manipulate and deceive the people who were already struggling to survive this deadly and contagious pandemic. This pandemic taught us some new lessons and showed us the true nature of cybercriminals and their willingness to stoop to deficient levels to further their causes. One should heed the lessons that were learned during the pandemic. With this research we provide a concise taxonomy of cyber crimes that have ravaged the society during the pandemic [2,3]. we discuss COVID-19 themed cyber crime that have occurred in recent times and provide a timeline for the same, lastly in this study we discuss current current security oriented and future technologies that can be employed to combat cyber crimes in such catastrophic events.

1.1 Key Contributions

We have thoroughly analyzed the cyber crime tradeoff in the pandemic era and respective solutions, The key contributions of our survey are as follows:

- The study discusses the concept of pandemics/major events that affect humans globally and the associated trends of cyber crimes.
- The study provides a generalized taxonomy of the subject matter. We review and critically examine other studies related to cyber crime during the pandemic.
- The study discusses recent COVID-19 themed cyber crimes and gives a timeline of cyber crimes since the pandemic's beginning.
- The study classifies and discusses cyber crime keeping the COVID-19 pandemic in context. Furthermore, in this, we examine recent security-related solutions used to counteract cyber crimes.
- The study critically discusses future technologies that can be used to prevent cyber crimes, especially if a catastrophic event occurs again. The findings and research of the study include the global state of cyber crime during and after the pandemic.

1.2 Outline of the Paper

The rest of this paper is organized as follows. Section 2 focus on comparative studies with existing surveys and our contributions. Sections 3, 4, 5, and 6 focus on emerging cyber security concerns in the COVID-19 Pandemic, which we use as a reference classification throughout the paper. In particular, Section 3 describes a cyber crimes overview in the covid era and previous similar events. The COVID-19 relevant security threats taxonomy is discussed based on execution methods, execution classifications, and platforms. Section 4 gives details about recent cyber crime and attacks in the pandemic period. Section 5 discusses the existing cyber security solutions & Prevention mechanisms. Section 6 provides a roadmap for future generation solutions and research challenges. Finally, Section 7 concludes the cyber security attack and available solutions in the COVID-19 pandemic era, providing a brief insight into future research.

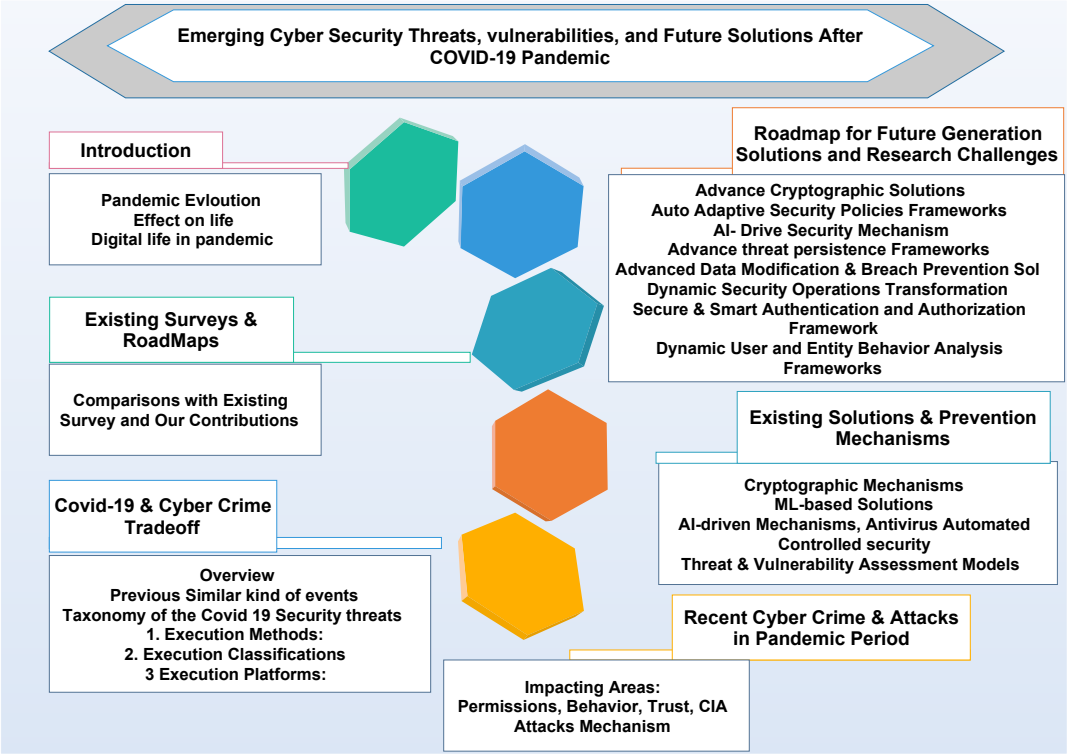

Figure 2: The layout structure of the survey.

2 Comparisons with Existing Surveys and Our Contributions

Since the pandemic's beginning, there have been numerous survey publications on "cyber crime and the COVID-19 pandemic". The existing survey provided the crime and covid Situations. David et al. [4] provided a very detailed study on cyber crimes that have occurred during the pandemic, specifically within the United Kingdom. Their dataset is primarily composed of police complaints that have been filed regarding cyber crime; based on that dataset; they provide a small taxonomy of cyber crimes. This survey, although informative, does not talk about security-oriented solutions or any future generation solutions to tackle this problem. Harjinder et al. [5] dived deep into the cyber crimes that have taken place since the beginning of the pandemic in late 2019 and provided an extensive timeline for the same. However, the timeline lists cyber crimes that have happened globally; the majority of the survey is United kingdom centric. They also do not provide any future generation solution or research directions, but their survey has a detailed analysis of cyber crime concerning the COVID-19 pandemic.

Mohamed et al. [6] paper focused on malware and phishing attacks discussing modes of operations of cybercriminals and how it has changed after the pandemic; they also dwell into how German criminal law applies to such crimes. However, this research paper does not provide any research directions, future or current solutions to tackle cyber crime issues or any proper classifications for cyber crimes that have happened during the pandemic. Saqib et al. [7] Unlike other papers that also provided a very diverse category of cyber crimes that have taken place during the pandemic. This paper also offered security-related solutions to prevent and tackle COVID-19 themed cyber crimes. Steven et al. [8] focused on establishing a relationship between change in day-to-day activities due to the pandemic and lockdowns and how cyber crime has changed concerning that. This paper discusses recent cyber crimes and provides a taxonomy for the attacks but does not provide any research directions or solutions present or future to tackle the issue.

Table 1: The state-of-the art comparisons with existing surveys. {S0: This survey, S1: David et al. 2020 [4], S2: Harjinder et al. 2020 [5], S3: Mohamed et al. 2021 [6], S4: Saqib et al. 2020 [7], S5: Steven et al. 2021 [8], S6: Scott et al. 2021 [9], S7: Venkatesha et al. 2021 [10], S8: Priyanka et al. 2020 [11], S9: Ben et. al. 2020 [12], S10: Rennie Naidoo 2020 [13], S11: Muhammad et. al. 2020 [14]}

Key contributions / Papers	S0	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11
Concepts	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Key taxonomies	✓	✓	✓		✓	✓		✓	✓			
COVID-19 and cyber crime studies	✓	✓	✓	✓	✓	✓	✓	✓			✓	
Timeline	✓		✓									
Recent cyber crime and attacks in pandemic period	✓	✓	✓		✓	✓	✓	✓		✓	✓	
Classification of crime with respect to pandemic	✓	✓	✓		✓	✓	✓			✓		
Security solution and prevention mechanisms	✓				✓							
Future generation solutions	✓											
Research specific to global situation of pandemic and cyber crime	✓		✓				✓			✓	✓	✓
Research specific to a single country's situation of pandemic and cyber crime	✓	✓	✓	✓		✓			✓	✓		
Research directions	✓		✓							✓	✓	

Scott et al. [9] puts forth a new dimension to the study of cyber crime and COVID-19. The authors analyzed the whole event from a psychiatric's point of view. The authors provided key taxonomies about how cyber crimes are happening amid the pandemic and how cyber crime and human psychology have been changed due to the pandemic. But this paper also could not provide security-related solutions or any further research directions. Venkatesh et al. [10] focuses on a single type of cyber attack that is the social engineering attack, and how it has changed since the pandemic. They also discuss recent cyber crimes during the pandemic, but since they only focus on social engineering attacks, they do not provide a taxonomy for other cyber crimes. They provide general guidelines to prevent such attacks but do not discuss any security-related solutions that can be used to tackle the menace.

Priyanka et al. [11] provides an in-depth and extrinsic survey on cyber crimes that happened in India. The authors gave a taxonomy for cyber crimes and discussed various cyber crimes' modus operandi. However, the authors did not focus on cyber crimes related to the COVID-19 pandemic and did not provide any solutions to tackle the main problem. Ben et al. [12] focuses on how COVID-19 affected policies and daily life in Scotland and various crimes that have taken place during the pandemic, their study discusses future challenges in policymaking. They have discussed recent cyber crimes but did not provide a neat taxonomy. Their research and analysis do not offer any security-related solutions but are very insightful for policymakers.

Rennie Naidoo [13] provides an exciting study on cyber crime and COVID-19 and proposes an influential multi-level model of such attacks. They discussed recent cyber crimes and used the crime data to create the model. They, however, do not provide a clear taxonomy of cyber crimes. Muhammad et al. [14] primarily focused on the users' emotions towards data sharing with websites during the pandemic; they do not provide a taxonomy for the cyber crimes, nor do they focus on recent cyber crimes that have

happened. Their study lacks future research directions and solutions for tackling the problem. Table 1 provides a comparative view of all surveys and this survey. The layout of the survey is presented in Figure 2. This layout provides the insight view of survey. We used a bottom-up approach to understand cyber crime and COVID-19 status better. Firstly, we reviewed almost all literature that mentions the cyberattacks and COVID-19, published no earlier than 2019. Then we started to classify articles, papers, books based on reference classification and attacks methods. We focused on existing approaches are recently used against the mitigation of cyberattacks. We concentrate on the most mentioned attacks and prevention methods, and based on them; we created the main categorization of the requirement of the future solution after the COVID-19 pandemic.

In this work, an analysis of all the types of threats and attacks is done. Each kind of attack is explained in great detail. A timeline is also provided for the major attacks that have taken place in sync with the pandemic timeline. Many research papers have been reviewed that focus on such kinds of attacks, but the fact that how this affected an area-specific or a nation has not been done in previously published papers. Different types of existing security mechanisms are listed which can be employed to prevent falling into such traps. Combined with this, many literature reviews are done, which discuss their novel take on each type of solution. Finally, a future roadmap with various possible solutions and the current progress is discussed thoroughly.

3 COVID-19 and Cyber Crime Tradeoff

This section establishes a relationship between the COVID-19 pandemic and the changes that have taken place in cyberspace concerning various cyber crimes. This section also looks at previous events that have affected people's day-to-day activities adversely and how cybercriminals modified their modus operandi to exploit such unfavorable situations. This section will also look into some of the research work already published regarding the topic "COVID-19 and Cyber Crime". Lastly, this section also aims at creating a taxonomy of cyber threats concerning the COVID-19 Pandemic. Cybercriminals leveraging mass panic and anxiety within the society during a natural disaster event or an event that has caused massive shifts in day to day routines of the community is something that is not new. Cybercriminals change their modus operandi quickly and leverage the mass panic to further their causes. To elaborate, after hurricane Katrina, the Federal Bureau of Investigations, USA, set up a Hurricane Katrina Fraud Task Force, during its three year operation period, this task force charged 907 people for committing fraud, their operation found out that, after the aftermath of Hurricane Katrina, multiple websites surfaced on the internet in less than a week after, claiming to be charities and organizations that would help people with recovering from the disaster. These seemingly legitimate websites defrauded people of their money and even stole the user's PII (Personal Identifiable Information).

Similar to Hurricane Katrina, in 2018, after Hurricane Florence devastated the western hemisphere, fraudulent websites on similar grounds to those seen in hurricane Katrina started showing up on the internet. These websites had one thing in common, and they had synonyms related to "charity", "relief" in their domain names. It was estimated that there were at least 137 such domains after hurricane Florence and phishing attacks also saw an increase. After the earthquakes in Ecuador and Japan, the Federal Trade Commission issued alerts about fraudulent donation emails that would infect users with malware or phish them for their money and PII. Similarly, US-CERT issued advisories posted about the Nepal Earthquake disaster stating that fraudulent emails related to donations and charities for combating the Nepal earthquake disaster can direct users to malware-infected websites and could dupe them of their money. Time and again, it has been seen that cybercriminals have preyed on the mass panic to further their malicious causes, and the COVID-19 pandemic could not be thought of as an exception to that.

David et al. [4] discussed the state of cyber crime during the pandemic within the confinements

of the United Kingdom. Their dataset is largely based on the police records of the cyber crimes that have been reported since May 2019. They present the readers with two hypotheses; firstly, both cyber dependent and cyber-enabled crime have increased during the pandemic, and secondly, cyber crimes have primarily affected individuals. Harjinder et al. [5] provided a concise and detailed timeline of cyber crimes that have taken place since the first reports of COVID-19 infection in Wuhan, China. They also provided an analysis of modus operandi used by criminals. Lastly, they also focused on how COVID-19 and cyber crime have affected the workforce. Mohamed et al. [6] focused on the state of cyber crime during the pandemic within Germany. However, they primarily focus on phishing and malware attacks. Constraining from just these two types of attack vectors, they discuss how cybercriminals have changed their modus operandi at various stages of the pandemic. Similar to [4], Steven et al. [8] focused on cyber crimes that have taken place within the United Kingdom during the pandemic. The majority of their datasets have been acquired from police records. However, unlike [4], they aimed to predict the future crime rates using the ARIMA model and historical data. They also presented the readers with a time-series analysis of the said data. Moreover, they provided readers with three hypotheses, which are as follows -

- The amount of cyber-crime witnessed during the first few months of the pandemic was higher than expected.
- Traditional frauds saw a decrease, whereas cyber-enabled crimes saw an increase during the pandemic.
- Individuals were more likely to fall victim to such cyber crimes as compared to organizations.

Venkatesha et al. [10] primarily focused on the social engineering aspect of the cyber-attacks; they provided a comparison of how social engineering attacks were used before and during the pandemic. Similarly to [6] they also focus on how attackers have leveraged the changing scenarios during the pandemic and modified their social engineering attacks by changing landscapes. They explore how social engineering attacks are used as precursors to phishing attacks. Interpol's [15] report on COVID-19 related cyber threats gives a brief overview of how the threat landscape looks during the pandemic. Although no significant statistics are provided, they focus on threat areas such as malware, malicious domain registration, and ransomware. Saqib et al. [7] diversified the cyberspace attack vectors and, unlike previous papers, brought in new attack terminologies such as vishing, fearwares, disinformation, etc. Similar to the papers above, James et al. [16] tried to establish a link between cyber crime rates before and during the pandemic. They divided the pandemic era into two-time segments, namely the pre-pandemic era (November 2019) and post-pandemic era (April 2020), conducting a survey and then mathematically analyzing the data collected from the study for the two given time segments. They provided two hypotheses for their research, as

- Number of victims of cyber crime will be more in a post-pandemic era as compared to the pre-pandemic era
- Victims spend more time online in a post-pandemic era as compared to the pre-pandemic era

Their research stated that the pandemic did not radically alter the online activity or the number of victims. Although they provided a quite elaborate mathematical approach on the analysis of data, they, however, did not elaborate on how cyber attacks have changed in the post-pandemic era and what modus operandi are being used by cybercriminals, unlike other papers. Scott et al. [9] established a connection between the pandemic, cyber crime, and the effect on victims' psychology. This study was primarily centered on how human psychology gets affected after falling prey to cyber crime. They establish a

relation between human psychology post an attack and how it can lead to the victim falling for more cyber attacks. They also found a connection between the pandemic and its psychological effects on people and how cybercriminals use the pandemic to further their nefarious motives. Anh et al. [17] focused on the cyber crime market and how it has evolved during the pandemic. They provided an interesting study on how new users interact in trust-based marketplace and how old and more experienced users operate in the same userspace. For their research, they have divided their research time frame into three parts, namely, "set-up era" (from 1st June 2018 to 1st March 2019), "stable era" (from 2nd March 2019 to 10th March 2020 and "COVID-19 era" (from 11th March 2020 to 30th June 2020). Their primary analysis was done on "contracts" created by users on the underground marketplace, and they provide an elaborate paper on how underground markets operate. Although this paper goes in a different direction than other papers, their analysis of how underground markets evolve is critical. They conclude that underground markets are becoming centric towards influential users and that there has been a significant evolution in the market in previously stated three eras.

Similar to [16], Muhammad et al. [14] also relied on a survey for the data source of their research. Unlike other papers in this section, they did not provide any taxonomy for the type of cyber crime being committed during the pandemic; they pondered the term "Data Theft" but did not elaborate on how the data was stolen. Their research focuses on people's willingness to share their data with online websites and whether or not people believe that the said data can be stolen from these websites. It has been noticed that, since the pandemic started, cybercriminals have leveraged the fear and anxiety that had formed within people in the initial stages of the pandemic to their advantage by forming threat campaigns that target the same fear and anxiety. They have been known to leverage the lack of information regarding COVID-19 and strict lockdowns during the initial phase of the COVID-19 pandemic for their benefit by modifying the campaigns so that people are compelled to fall victim to them. This happened during the initial stages and when key milestones were announced during the pandemic, such as the development of COVID-19 detection tests, the announcement of vaccine developments and distribution, and the projection of multiple waves of COVID-19 [18].

3.1 Taxonomy of Cyber Threats in the age of COVID-19

At the very base level, cyber crimes can be broadly divided into two categories based on how technology is used while committing said crimes; the two categories are -

1. **Cyber Enabled Crimes** - Crimes that can be committed using traditional methodologies without using any computer resources, but now they are being executed at an aggravated rate with the aid of computer resources, fall into this category. Online fraud, disinformation campaigns, extortion, etc., can be classified as cyber-enabled crimes [19].

2. **Cyber Dependent Crimes** - Unlike cyber-enabled crimes, cyber-dependent crimes are those crimes that can only be committed via the use of computer resources. Hacking, Denial of Service Attacks, Data Breaches, etc., fall into this category [19].

Similar to the above classification, cyber crimes can be further classified into other categories based on whether the culprit is an organization or an individual; these categories are -

1. **Organized Cyber Crime** - These cyber crimes are often committed by a group of experienced individuals or an organization. They use sophisticated methods to commit cyber crime and often crack down on hard. Organized cyber crimes primarily deal with building and deploying malware, leading espionage campaigns, large-scale disinformation campaigns, extortions in the form

Table 2: The state-of-the-art-works classification of cybercrime based on the use of technology and organization structure.

References	Classification based on use of technology		Classification based on the attackers organization structure		Other Methods
	Cyber Dependent Crime	Cyber Enabled Crime	Organized Cyber Crime	Un-Organized Cyber Crime	
David et al. [4]	✓	✓	×	×	×
Harjinder et al. [5]	✓	✓	×	×	×
Muhammad et al. [14]	×	×	×	×	✓
Mohamed et al. [6]	×	×	×	×	✓
Saqib et al. [7]	×	×	×	×	✓
Steven et al. [8]	×	×	✓	×	×
James et al. [16]	×	×	×	×	✓
Scott et al. [9]	×	×	✓	×	×
Venkatesha et al. [10]	×	×	×	×	✓
Anh et. al. [17]	×	×	×	×	✓
Interpol [15]	×	×	×	×	✓
This Survey	✓	✓	✓	✓	×

of ransomware, etc. Often organized cybercriminals will target a large section of society, an organization, any large target, or a specific cause [20]. If a nation-state is involved in any way with an organized cyber crime syndicate, then that syndicate is also called an Advanced Persistent Threat (APT).

2. **Un-Organized Cyber Crime** - Un-Organized cyber crimes can include identity theft, scamming, phishing, blackmailing, etc. These are small-scale cyber threats that are often targeted at individuals or a category of personnel rather than a large section of society. Unlike organized cyber crime, individuals often commit un-organized cyber crimes; they may or may not be experienced. Most often, un-organized cybercriminals rely on pre-built software and lack sophistication in their crimes [21]. This also makes them more accessible to the crackdown.

Another type of classification that can be done for cyber crimes is based on a cyber criminal's attack methodologies. This classification is as follows -

1. **Denial of Service Attacks** - In this attack methodology, the attacker tends to disrupt normal services that the people use in such a way that people are no longer able to access the service. This can be done by exploiting a bug in the service to crash the service, causing Denial of Service. An attacker can also leverage the help of bots to bombard the service with network traffic or seemingly legitimate service request, effectively exhausting the resources used by the service and thus causing Denial of Service [22]. In this latter scenario, a multitude of devices are required to perform a successful attack; therefore, this is also called Distributed Denial of Service Attack (DDoS). Both forms of Denial of Service attacks are often used in conjunction with each other to increase the magnitude of the attack.

2. **Phishing**- In this attack methodology, attackers use fraudulent communication means to steal sensitive information, steal money or deploy malicious software onto the victim's devices [23]. This can also be divided into subcategories based on the methods of communications used by the attackers. The sub-classifications are as follows -

(a) **Email Phishing** - As the name suggests, emails are used as a mode of communication to carry out phishing attacks. These are most commonly used to target organizations as opposed to individuals [23].

(b) **Smishing** - In this method of communication, SMS messages are used to send out phishing attacks. This method of sending out phishing attacks is most commonly used to attack individuals [23].

(c) **Vishing** - Unlike Smishing, Vishing uses a voice medium: phishing attacks happening over phone calls. Unlike the above two categories, vishing requires attackers to actively engage with a victim to ensure that an attack is successful. In current times, people have been duped with covid vaccination appointments. During the initial days of covid, fraudsters took advantage of the situation when there was a vaccine shortage. People were rushing to get vaccinated and were ready to give any amount without any verification or advice from doctors or health agencies [23]. Currently, during the third wave i.e. January 2022 time while Omicron [24] has been spread across the world and had been feared that more than 60% of the world population will be infected with it by March 2022 as claimed by IHME (Institute for Health Metrics and Evaluation), an independent population health research center at the University of Washington Medicine. People have been rushing to get booster doses of vaccine, and fraudsters have been rapidly changing their modus operandi to dupe people over it again.

(d) **Pharming** - This form of phishing does not require any modes of communication. Still, in these methods, the attacker modifies the DNS entries for a victim to misdirect the victim from a legitimate website to a malicious website. A malware attack often aids this form of attack.

3. **Extortion** - This attack methodology, however old, has reached new peaks with the help of technology. Attackers use computer resources to extort money from gullible victims [5]. There have been recent peaks in cases where attackers morph images of victims onto images and videos using Deep learning technologies like DeepFake [25] and then use those photos and videos to extort money out of the victim.

4. **Fraud** - Like extortion, fraud, although considered a traditional crime, has reached its peak during the age of technology. The general modus operandi is to dupe the victim delivering services that do not comply with the original terms [26]. This form of a cyber attack can also be classified into subcategories based on the platform of attack. The categories are as follows -

   (a) **Shopping Fraud** - This fraud occurs when any e-commerce element is involved in any part of the transactions. It usually happens when the victim orders something from an e-commerce platform, but either it does not or receive another product [26].

   (b) **Dating Fraud** - A lesser-known type of fraud, in this fraud, victims, are duped by their online romantic partners, with whom they got in touch via social media platforms or online dating sites [26].

   (c) **Online Fraud** - This form of fraud is used to categorize any fraud that can not be categorized in the above categories. This can happen via emails, phone calls, or any form of communication media [26].

   (d) **Carding** - In this kind of fraud, fraudsters usually showcase pricey items like phones, laptops, cameras, etc., at significantly lower prices and give proof of sending the tracking receipts or ids of various e-commerce websites [26]. Sometimes, this is a fraud, i.e., neither there is any

product, nor they are selling. In another type of carding, fraudsters use the cards of various people gathered through dark web portals, and using these cards; they will legitimately buy the items from e-commerce websites. Meanwhile, they contact some victims and get a relatively lower amount from other means. Thus, the fraudsters cover themselves with minimized risk, and the victim is duped with a product being bought from another victim's credit/debit card. As and when another victim files a complaint, the Law enforcement agencies will be able to reach the victim who has bought the product through the fraudster. But the actual perpetrator will never be caught.

5. **Man in the Middle attacks (MITM)**- This form of attack methodology concerning COVID-19 is analogous to the one used in network attacks. In this attack, a criminal creates a fraudulent website impersonating a legitimate website and then tricks users into submitting their PII through it; the attacker then uses those PII to impersonate them on the legitimate websites [27].

6. **Malware Attacks**- These attack methodologies are carried out with the help of malicious code, also called Malwares; Attackers often infect their victims with malware to help them aid in other purposes [28]. Often malware is deployed using phishing attacks, and then, in turn, malware assists aid other forms of cyber crimes.

   Malware can also be classified into various subcategories based on their functions performed. This classification is as follows -

   (a) **Ransomware** - This form of malware locks victims' files by encrypting them using robust encryption techniques, and then they ask the victim for a ransom to recover those deleted files. Often these payments are collected via cryptocurrencies. Ransomware has seen a sharp rise in recent years.

   (b) **Spyware** -These forms of malware are used to covertly collect information about the victim and send them out to the command and control servers. Often used for espionage, these forms of malware often have APTs associated with them.

   (c) **Adware** - This form of malware is seemingly harmless compared to other forms of malware; the primary purpose is to showcase unsolicited advertisements to the victims. They often become a nuisance rather than a threat.

   (d) **Fearware** - The primary purpose of these forms of malware is to instill fear within the victim. They are often used in disinformation campaigns but are limited to disinformation. Ransomware can also be classified as fearware.

   (e) **Crimeware** - This umbrella term is given to a class of malware that facilitates cyber crime, making it easier for the attacker to victimize gullible people. The above states that malware categories can also fall under this category but are not limited to these.

7. **Identity theft** - Identity theft is one of those traditional crimes which have increased its reach and severity with the help of technology. Primarily PIIs are stolen via malware or phishing attacks. Primary targets in such attacks are individuals. To explain in simple terms, attackers use the PII of the victim and then masquerade themselves as the victim on an online platform; they can use their stolen identity to commit fraud or further their motives [29].

8. **Espionage** - Similar to identity theft, espionage is also a traditional crime that is now being aided by technology. Espionage often leads to hacking attacks or is administered by a hacking attack. In espionage attacks, attackers usually target organizations and try and steal their sensitive information that is crucial to the functioning of that organization, such as the protocol stack being used, the

Table 3: The state-of-the-art-cyber crime works based on the various attack methods and patterns. Abbreviations: M1: Malware Attacks, M2: Denial Of Service Attacks, M3: Hacking Attacks, M4: Phishing Attacks, M5: Extortion, M6: Fraud, M7: Man in the Middle Attacks, M8: Social Engineering Attacks, M9: Disinformation, M10: Espionage, M11: Advance Persistent Threats, M12: Identity Theft

Authors	Key Contributions	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12
David et al. [4]	Discusses about cyber crime in United Kingdom and establishes a relation between an individual's routine during the pandemic and cyber crime	✓	✓	✓	✓	✓	✓						
Harjinder et al. [5]	Provides a timeline of cyber crimes that have taken place since the starting of the pandemic	✓	✓	✓	✓	✓	✓					✓	
Mohamed et al. [6]	Discusses how modus operandi of attackers have changed since the starting of the pandemic, focuses on malware and phishing attacks that have happened in Germany	✓			✓			✓					
Saqib et al. [7]	Discusses how COVID-19 has affected the CIA triad, discuss a large variety of cyber attacks such as fearwares, disinformation campaigns, vishing and many more	✓	✓		✓		✓			✓			
Steven et al. [8]	They focus on cyber crime that happened during the pandemic within the UK, they provide a time series analysis of their data and use ARIMA models to predict future crime rates.	✓		✓		✓	✓						
James et. al. [16]	They discuss cyber crime rates before and during the pandemic within the USA, They mathematically analyze their survey data to provide more context between cyber crimes and daily routines.	✓					✓						✓
Scott et al. [9]	Discusses the psychological effect of the pandemic and cyber crime on an individual.	✓			✓	✓	✓			✓			
Venkatesha et al. [10]	Discusses about how social engineering is used to target victims and how these attacks have changed since the start of the pandemic				✓				✓				
Anh et. al. [17]	Discuss how underground markets has evolved before and after the pandemic, they also focus on how new users interact with the market	✓		✓									

infrastructure used by an organization, what type of servers are being used, etc. Unlike hacking, in espionage, attackers target crucial data and any information that is crucial to an organization [30].

9. **Hacking**- Hacking is an umbrella term for attack methodologies aiming to gain illegitimate access to a private or otherwise restricted resource. In this context, unlawful access can be defined as the access for which the owner of the said resource has given no explicit permission to the person

gaining the illegitimate access. The main motive of any hacking attacks is to exfiltrate confidential information about/owned by the victim [4].

Hacking can further be classified into subcategories based on what an attacker targets computer resources. The classification is as follows -

(a) **Server**- In these scenarios, servers of an organization or individuals are targeted. Servers are generally used to store data and are a popular target for hackers.

(b) **Personal Devices** - In this attack scenario, unlike Hacking/Server, personal devices belonging to an individual are being targeted. Personal devices can include phones laptops. They are a treasure trove for attackers as they can contain many personally identifiable information or PII such as bank details, private photos, etc.

(c) **Social Media Accounts** - Attackers, in this case, target a person's social media accounts, potentially aiming to blackmail the victim or to perform various nefarious activities that can include but are not limited to posting obscene material, sending threatening emails, messages or impersonation. Especially in the age of pandemics, where everyone is online, social media accounts are a popular target for attackers after servers.

(d) **Critical Infrastructure** - In this form of a hacking attack, attackers target a nation's critical infrastructure; in this context, critical infrastructure is that infrastructure that can cause massive loss of life or substantial economic loss if damaged by any means. Although we do not see daily attacks in critical infrastructure, the attack can be traced back to a state-sponsored APT whenever a critical infrastructure is attacked.

(e) **Others** - This category is used to club attack targets that do not fall under the above four primary types.

Tables 2 and 3 provide a summarized overview of the taxonomy devised for cyber crime happening during the COVID-19 pandemic.

4 Recent Cyber Crime and Attacks in Pandemic Period

cyber crime is not a new crime. These types of crimes such as malware attacks, phishing, ransomware have happened before. Still, after the corona pandemic, as soon as people started to work from home, the attack vector for cybercriminals increased multi-folds. According to a report by the Financial Services Information Sharing and Analysis Center (FS-ISAC), in February 2020, more than 5000 acts of cyber crime were registered every week; by the end of April, more than two lakhs were registered per week [31]. That includes data breaches, phishing, malware attack, DoS attacks, etc. This is why most financial institutions started investing more in cyber security than ever before. In cyber security investments, they began putting firewalls, IDS software, antivirus, and security centers in the form of all these essential services.

Apart from financial cyber crime, there has also been an increase in cyber crimes that directly target the common person, such as online banking fraud, job fraud, covid relief fund fraud, fake news, and many more. Due to Lockdown, people were in their homes and used to spend a large part of their daytime on the internet, due to which criminals also made them their target. Criminals used to try to make them victims with activities related to corona.

In table 4, the details of cyber-attacks that happened recently have been discussed. DocuSign is one of the most famous electronic signature programs. Table 3 provides the state-of-the-art-cyber crime works based on the various attack methods and patterns. It is a widely trusted choice by most users for any official document. However, threat attackers abused this trust when a phishing email linked

Table 4: Recent cyber-crime incidence in COVID Pandemic

Cyber Attacks	Attack types	Attack date	Impacted areas	Attack Mechanisms
DocuSign Phishing Campaign	Phishing	May 2020	Confidentiality	Social Engineering
Hackers exploit HMRC Coronavirus Job Retention Scheme with phishing email scam	Phishing	April 2020	Trust, Finance	Social Engineering
DoS on epidemic	DoS	Feb 2020	Availability, reputation, critical services	Flooding services, Crashing services
Data loss by spoof health care mail	Spoof email Ransomware	June 2020	Availability, Data Loss	Malware attack
REMCOS malware	Phishing Malware Attack	Jan 2020	Finance	Malware attack
Remcos RAT Revisited	Trojan Malware attack	Jan 2021		Malware attack
Coronavirus-themed malware with malicious Microsoft Word documents	Phishing Emotet malware AZORult	Feb 2020	Information stealing	Malware attack
Prolonged shutdown	RCE	Aug 2021	Integrity, Confidentiality, Reputation, Data leak	MITM
Espionage attack on Indian Satellite Communications		Sep 2020	Data breach, reputation	Espionage
Netwalker ransomware	Ransomware	2021	Financial loss	Malware attack
Cyber-attack on Czech hospital	Hack	2020	Data breach	
Domino's Pizza Data breach	Hack	April 2021	Data breach, Trust, Reputation	Spy/ Passive attack
MobiKwik Data Leak	Hack/Key compromise	Feb 2021	Data breach, Sensitive information	Passive attack
Upstox Data breach	Hack/Key compromise	April 2021	Confidentiality, Trust	Passive attack
Air india data breach	Hack	Feb 2021	Trust, Financial lose	Passive attack
Juspay data leak	Hack	Jan 2021	Information leak	Passive attack
Nebraska Medicine computer network outage	Ransomware	Sep 2020	Availabilty, Data theft	Malware attack
King of Prussia malware attack	Malware attack	Sep 2020	Financial lose	Malware attack
UVM Health Network shut down	Hack	Oct 2020	Availability, Data theft	
Job Fraud	Online Fraud, spoof	2021	Money loss	Spoofing
PM care fraud	Online Fraud, Spoofing	2020	Money loss	Spoofing
Vaccine Cyber Espionage AstraZeneca in the UK	Espionage Phishing email Malware attack	2020	Data loss, Confidentiality	Social engineering, malware attack
Fake COVID-19 test kit	Online fraud	2020	fraudulently money theft,	Phishing, Social engineering
spymex virus	Virus inject	2020	Confidentiality, Behaviour, Data theft	Malware attack
Virus alert API	Virus inject	2021	Behaviour, Confidentiality	Social engineering, malware attack

to a malicious COVID-19 document was sent to around 60,000 users. Moreover, it was an advanced attack with three layers of obfuscation to ensure the attackers could steal credentials. This leveraged the trust of DocuSign users and the awareness of COVID-19. This awareness was also abused in another phishing scam targeting the applicants of the government's Coronavirus Job Retention Scheme. This has been repeated in such emails to target the public's cautiousness. But, prevention is better than cure always, and it is better to keep regular snapshots and backups to prevent any downtime due to such malware. F-Secure tracked down such coronavirus-themed phishing campaigns and found that all of them were linked to some malware. The malware mainly belonged to the RAT or Remote Access Trojan family. These aim to allow the attackers to remotely control complete systems, mimic owner behavior and exfiltrate the accurate data. Remcos RAT is one such case that is part of the similarly themed phishing campaign in Colombia. The campaign used additional layers and payloads to ensure malware delivery.

A data breach is an event where data is stolen or taken from an organization, system, and government (public information) without the permission or underwriting of the design's proprietor. Stolen data might be restrictive or confidential, such as card details, client data, or national security data. A small start-up or significant association might experience a data breach. Data breaches can be irrefutably more than a concise fear — they may change the way of growth. Associations, state-run organizations, and individuals the equivalent can experience enormous ensnarement from having complex data stolen. Whether online through the internet or offline through internal means, hackers have stolen confidential and sensitive seal data in many ways. Generally, the main reason for the data breach is technical weakness, and the second primary reason is the user's behavior. As the features increase in the upgraded system, connecting to the system also increases, providing more new attack surfaces. New technologies are created faster than the way of protection. The most significant cause of data breaches is external attacks. Data is stolen by detecting the vulnerability of any system and exploiting it. That system's information contributes the most in detecting vulnerability; the more information that system gives, the higher the probability it is to be breached. Every time there doesn't need to be a data breach due to an external attack, there may be many other reasons this has happened. Sometimes data is breached even by the company's employee accidentally; this usually occurs when an employee uses another employee's system without his consent and sees the secret data. Often, an employee of the company shares that company's data with a deaf person even with the wrong intention; it is called Insider Threat. It is difficult to catch these because these types of employees have data authority. Loss of data devices can also be a cause of data breaches. Loss of data devices can also be a cause of data breaches. There is a possibility of malware attack if the asset is compromised, after which even the regular authentication steps are of no use. There was a lot of data loss during the corona epidemic. The increase in data loss in this epidemic is worrying and is forcing us to think about this topic. Many big companies have lost a lot of confidential data of themselves and their customers. Each data breach's technology, mechanics, and impact area were different.

Medical data and financial data were the most targeted during this pandemic. The hackers conducted a cyber-attack in the year 2020, intending to graze the data of the Czech hospital and shut down all the systems. The hospital's IT staff noticed similar activity several days before the attack. The watchdog service was being used to monitor the IT infra of the hospital, which they found out many times their network had been scanned to trace the services of the hospital system. The attackers targeted medical data by simultaneously injecting ransomware malware into two different hospital servers. After the medical data, the second data that has been attacked is the user's financial data. Online transactions had increased during Covid Lockdown, ordering goods online, ordering food, in all these transactions from cash were reduced. The data breach of Domino's customers was a major cyber-attack.

In this breach, the attacker had all the details of the order from Domino's customer, which included name, address, mobile number, order details, and payment information [32]. This attack is the compromised key of Domino's' cloud server. Due to compromise, the attacker sold the data entry feature on the dark-net. This attack also caused a lot of damage to the company's reputation; many users had changed

the passwords of all their accounts. Like Domino's, the card data of MobiKwik users was stolen [33]. This happened due to the compromise of the cloud server key of this company. In this attack, sensitive information was exposed by using the passive attack mechanism. The company suffered the loss of reputation and the trust of the people and data theft. In the financial data breach, there was a major breach of investment company Upstroke and payment success company Juspay. The attack order data was hacked with the passive attack mechanism on Upstroke, after which the confidential data of millions of users, in which their card, as well as bank details, were lost.

When the criminal cheats through online means, it is called online fraud. Online fraud includes online scams, identity theft, fraud, selling fraudulent goods, and many more. At the time of this epidemic, online fraud increased a lot because many common people started seeing a lot of news related to corona on the internet. They did not understand as much as understanding the right and inappropriate content. Criminal fraud people's medical reports under the guise of Corona medicines. For online fraud, criminals use all techniques like phishing, spoofing, social engineering, etc. During this epidemic, there were many frauds in which PM Care Fund, Jobs, vaccination, and covid kits were the main ones. To assist the needy at the time of this disaster, the Government of India started the PM Care Fund. With the help of this platform, capable people are used to assisting the needy. Criminals took advantage of this new fraud. They made fake profiles of PM Care Fund many NGO's and sent them to the people, and some even shared it by making a spoof of the PM Care Fund application, due to which people had to bear financial loss due to well-being. Not everyone could recognize the Spoof application, and people eager to help started trusting this type of application. This is known as a behavior analysis fraud attack.

Due to the lockdown, many people lost their jobs, and many people left their jobs and went to their native places. Due to rising cases of Corona, the financial crisis started, and unemployment created new problems. Criminals cheated online using social engineering, spoof emails by pretending to do online jobs, and work from home, such messages and applications. Criminals used to ask the unemployed to deposit some amount first and withdraw that amount in cash. A website was prepared by spoofing the domain and phishing technology to the big e-commerce company. Many people were deceived by seeing that website and ordered COVID-19 kits, and Criminals took advantage of the fear of Corona. After the vaccine was ready for corona disease, the vaccination process was done through online registration. Cybercriminals created spoofed registration portals on which people would register, after which they would get the fake registration number. In lieu of this registration number, criminals had also received some other data along with the details of AADHAR [34]. Some criminals had also prepared applications for paid vaccination.

5 Existing Cyber Security Solutions & Prevention Mechanisms

Various criminals took advantage of this human tragedy by committing different crimes. In this tragedy of disease, due to these types of cyber crimes, it has been encouraged to promote research to improve cyber security postures of the organizations [35] and self-defense techniques. We propose to work on some of the methods which can be of utility to enhance the cyber security mechanisms currently being used across the world.

5.1 Cryptography Mechanisms

Innovative medical devices are subject to many MiTM attacks. These lead to other vulnerabilities and data breaches. Cryptographic authentication can be used to tackle this problem in IoMT (Internet of Medical Things) devices. Public key cryptography and Diffie Hellman exchange [36] are a few examples that must be employed to guarantee safety on a minimum level. A whole new attack surface has been

uncovered with the rising development of quantum computing. Supercomputers showcase an intense amount of computation speed and efficiency. Due to this, it is becoming easier to break encryption or brute-force hashes. Due to this, various new algorithms are being developed, and old ones are being improved and tested on faster computers. This emerging threat calls for new techniques to combat this complex problem. New cryptographic methods have been proposed that offer quantum resistance [37–39].

5.2 ML-based Solutions

ML (Machine Learning) can be used to detect new attacks by analyzing traffic patterns. It can classify traffic such as Bot traffic, Malware traffic, and background traffic using other techniques like Deep Packet Inspection (DPI). This classification is done by extracting features from various data-sets like Netflow. Netflow is a network protocol developed to collect IP traffic information. The network flow is monitored as traffic enters and leaves the interface. Naturally, a massive amount of data can provide a lot of incentive to find intriguing patterns and filter out valid traffic. Natural Language Processing can be used to perform cognitive analysis on cybersecurity-related documents. These can be classified into 18 different categories. A website implementing this solution is also available where documents can be uploaded, and everything happens with REST APIs. Even basic ML algorithms can also be used to combat IoT-related cyber attacks. These focus on Denial of Service attacks using the CICDoS2019 [40, 41] dataset.

5.3 AI-driven Mechanisms

CARAMEL H2020 project protects mobility-based applications. It is excellent for autonomous and connected vehicles. It uses ML techniques to detect anomalies. In conjunction with this, AI is used to mitigate the risk automatically. This combination can easily filter out various anomalies, which is vital since it is a susceptible field. AI-based cybersecurity tools can be developed efficiently by taking inspiration from the biomedical field [41, 42]. Testing of various devices can be done in phases like clinical trials. This inspiration proves to be essential in filtering out any poisoned data upon which the AI is trained. One such application can be honeypots, and this solution can be used to remove any bias present. Neural Networks can be used to implement an IDS. An Intrusion Detection System or IDS monitors traffic and alarms the concerned security teams to probe further action. It can be used to detect shell-codes and other cyberattacks. FireEye also uses a conceptual AI framework called Automatibility Spectrum. It uses a hybrid approach to add a degree of automation to repetitive tasks. It incorporates various solutions to different types of cybersecurity threats.

5.4 Antivirus Solutions

Antivirus software is used to detect, isolate and remove malware from systems. It is a fundamental component of any endpoint security system. However, most malware can evade detection with ever-changing methods. Thus antivirus systems are not sufficient on their own. Email security and privacy antivirus are designed perfectly [43]. Email security and online privacy have become the hot-spots of discussion during the testing times of the pandemic. Antivirus plays as a guard to protect the system from all types of miscellaneous entries like backdoors. Nowadays, AI-based antivirus is designed to protect and detect malware. The main advantage is the perception of patterns in malware such that even the changing methods can also not evade detection. However, if a unique variant is present, it can raise the bar of difficulty a lot.

5.5 Threat & Vulnerability Assessment Models

Blockchain-based security reference architecture is currently being used for threat hunting. It is still a new concept but one of the promising ones. With this approach, security systems are designed with everything analyzed beforehand. Cyber-physical systems are the backbone of the enterprise industry and hence, the most targeted system of attackers. So threat and vulnerability assessment models are used in defending them. Operationalization, application, and validation of organizational exposure are essential parameters of such a model. Developing quantitative vulnerability scores based on managerial judgments is significant to get reliable results. On the other hand, scenario analysis and multi-criteria evaluation serve for problem structuring [44].

5.6 Automated Controlled security

Automated controlled security is used to secure the network and the devices on it. With the emerging technology, IoT devices are used in day-to-day life. IoT-controlled security is used to deploy security based on these devices. Automated security is used to detect and mitigate phishing attacks through different media such as emails, SMSs, etc. Smart devices are used for security control in office applications. Researchers are building a framework for automated security in cloud infrastructures [45]. Similarly, wireless security systems also play a crucial role in IoT-based security. This is because IoT devices communicate via wireless media such as Wi-Fi, Bluetooth, Zigbee, etc. Hence such protection must be automated [46].

5.7 Deep learning

Deep learning is the choice of cyber-security for intelligent city planning. This is self-evident because billions of parameters can be trained as observed in various marvels like GPT-3, Codex, etc. It is implemented in organizations to detect insider threats and analyze networks. A blockchain-based deep learning approach is used to secure cyber-physical systems. Deep learning can also be used for malware detection [47]. Mail providers implement deep learning for detecting spam and phishing emails. Biometric security devices also rely on deep neural networks along with captcha analysis and steganography.

5.8 Cyber Hygiene

The following practices can be observed at an individual level as well as organizational level. It is crucial to use strong passwords personally, not share them with anyone, and keep them safe. Strong passwords include long-length passwords, generally a mix of alphabets (both uppercase and lowercase), digits, and special characters. With the increase in each character, the time it takes to brute-force the password, basically hit and trial every combination of characters, increases exponentially. Although a minimum length of 8 is a fixed requirement nowadays, It is recommended to have 12-16 characters with heavy randomization of all the types of characters. Using such a strong password helps a lot in prevention, but it is necessary that the same passwords are not used on multiple sites since the breach of a single password can cause catastrophic loss. This raises a problem as it is complicated to remember such passwords. Using password managers helps a lot in tackling the posed challenge. Password managers can store many passwords and encrypt them so that a data breach can avoid leaking all the credentials. Most password managers also install right into the browser, which helps log in quickly to websites and suggest strong passwords for new registrations. It is strongly advised to install robust endpoint security solutions to detect malware and unauthorized network access. Modern endpoint security encompasses a suite of solid solutions such as antivirus, anti-malware, firewall, website security, password vault, and much more. Such solutions leave little to worry about, but they don't change the internet habits of an individual

and must be looked at in retrospect to improve and prevent cyber crimes. Organizations can also employ such solutions combined with the network firewall to prevent unsolicited access to sensitive information. Other installed programs and the operating system must also be updated regularly since bugs are found every day and are usually a target of threat actors for gaining access to the resources. Each extra day of outdated software increases the probability of falling victim to cybercriminals. Everyone must stay cautious of spam or phishing emails, especially company employees, since threat actors generally use social engineering to access the credentials or other resources. These emails can be drafted as lottery or prize announcements or even from close relatives by an imposter ready to get into the system. Such emails should always be reported as spam so that the spam filters can automatically hide such emails and reduce the risk of mishaps [48]. The Government of India has also started a few initiatives to decrease the growth rate of such incidents.

Cyber Swatchhta Kendra is one such example that stands for Botnet Cleaning and Malware Analysis Centre. The aim is to provide free tools for detecting and removing such artifacts. It is mandatory now for every organization providing digital services to report to CERT-In if such cyber-security incidents occur. Specific guidelines have also been issued for Chief Information Security Officers (CISOs) to understand their responsibility in protecting organizations' assets. There are strict cyber-security laws in India, and it is advised to report crimes as it is punishable offense. It is recommended that one should improve their internet habits. It can be done by staying away from cautious websites, especially those that do not support HTTPS, depicted by a green padlock near the address bar. One should stay away from public computers and Wi-Fi networks to prevent a threat actor from sniffing the network and potentially gaining access to the credentials. These solutions and habits can help a lot in decreasing cyber crime combined with the initiatives taken by the government.

Table 5 effectively summarizes various existing state-of-the-art security oriented solutions and various researches that are have been done in the field.

6 Road-map for Future Generation Solutions and Research Challenges

Emerging cyber security concerns brings advanced requirements for adaptive cyber security solutions. This section focus on future generation cyber security solutions and research challenges.

6.1 Dynamic Security Operations Transformation

Security operations are an essential part of how an organization deals with security threats. These operations include but are not limited to monitoring networks, log analysis and management, security compliance audits, cyber-attack mitigation, post-cyber-attack cleanup. A dedicated Security operations team often manages these operations, also called the Security Operations Center. Traditional SOCs models use a lot of resources and time while dealing with a cyber-attack; many people are involved while dealing with the same; of all the resources they utilize, time is the key resource that many SOCs waste. This wastage of time can be attributed to contacting superior officers before taking any action or not being adequately trained to counter any situation. In other cases, humans are restricted by the SOPs of the SOCs [73], preventing them from making decisions on the fly or using methodologies that could potentially save a lot of time. Due to this, there arises a need to develop a better and more dynamic Security operations center capable of performing security operations on its own and using evolved methods to tackle any anomalies.

To make a dynamic system, we need to design a system that would take various input sources, make intelligent decisions based on those inputs, and take autonomous actions based on the determination it takes. This can only be done by using the means of using Machine learning [74, 75]. Machine learning

Table 5: Existing state-of-the-art solutions and prevention mechanisms (TVA: Threat and Vulnerability Assessment, ACS: Automated Controlled System, R1: Timeline, R2: IoT, R3: Privacy, R4: Confidentiality, R5: Malware Detection, R6: Data Protection, R7: IDS, R8: Integrity, R9: Availability, R10: Threat Monitoring, R11: Vulnerability Assessment, R12: Automation, R13: Device Security, R14: Confidentiality)

Paper Authors	**Security Mechanism**	**R1**	**R2**	**R3**	**R4**	**R5**	**R6**	**R7**	**R8**	**R9**	**R10**	**R11**	**R12**	**R13**	**R14**
Althobaiti et al. [49]	Cryptographic	✓		✓	✓										
Rahman et al. [50]	Cryptographic	✓	✓												
Sakhai et al. [51]	ML-based	✓													
Chesney et al. [52]	ML-based	✓	✓												
Argyropoulos et al. [53]	AI-driven	✓													
Begoli et al. [54]	AI-driven	✓													
Ahmed et al. [55]	AI-driven	✓													
Steven and Lipika [56]	AI-driven	✓													
Ty [57]	Antivirus	✓				✓									
Sivarethinamohan et al. [58]	Antivirus	✓		✓			✓								
Sidney et al. [59]	Antivirus	✓				✓									
Hamed et al. [60]	Antivirus	✓						✓							
Delaney and Jeffrey [61]	Antivirus	✓													
Scholz et al. [62]	TVA	✓						✓	✓	✓					
Zografopoulos et al. [63]	TVA	✓									✓				
Homoliak et al. [64]	TVA			✓							✓	✓			
Hassan et al. [65]	ACS	✓	✓											✓	
Alqahtani et al. [66]	ACS	✓	✓											✓	✓
Chen et al. [67]	ACS	✓	✓												
Abu et al. [68]	ACS		✓									✓		✓	
KP and Alazab [69]	Deep Learning														
Rathore et al. [70]	Deep Learning	✓			✓										
Chen et al. [71]	Deep Learning	✓	✓												
Ferrag et al. [72]	Deep Learning							✓							

can aid in making autonomous and smart decisions eliminating the need for viewing SOPs and talking to people. Smart decision-making will help any organization reduce a large amount of wasted time while responding to a threat. The advantages of using Machine learning are immense but current advancements in machine learning still lack the cognitive ability to understand human behavior [75] and understanding that is the key to building an effective dynamic security operation center.

6.2 Secure and Smart Authentication and Authorization Framework

One of the main reasons an attacker can cause havoc for an individual or an organization is the use of non-existent or mis-configured authentication and authorization frameworks. To fully comprehend the scope of this problem, we need to understand the difference between authentication and authorization; authentication means to verify whether the user seems to be who they are claiming to be, and authorization means whether a user has the privilege to access a certain resource. Authentication is carried out with the help of secret keys, also called passwords. In contrast, authorization is carried out by providing roles and maintaining a role-based access model; often, people tend to not properly configure a proper authentication and authorization flow, which helps hackers easily gain access to a restricted resource [76].

The pandemic brought forth the need to work remotely, which led to an increased attack vector, and amid the chaos, cybercriminals leveraged the new rules and working conditions for their benefit. Keeping this pandemic in mind arises a need to develop and deploy the smart and secure authentication and authorization frameworks that overcome the challenges in the current frameworks, specifically enabling the privacy of the users that use the framework. There is current research working on building a smart and secure framework with the help of blockchain technology which uses a series of smart contracts to grant access control and authenticate. This particular research uses Proof-of authenticity/Integrity (PoAI) [77] to authenticate. Although this research focuses on IoT devices, it can be expanded to incorporate individual users as well as an organization. Similar to [77, 78] also uses blockchain technology to authenticate and authorize IoT devices within an area securely, and this similar concept can be expanded on a bigger scale to incorporate individual users too.

6.3 Advance Cryptographic Solutions

Cryptography is an essential part of every communication that happens over a network, and cryptography is being used in our day-to-day lives. However, essential has drawbacks, such as being inaccessible to a legitimate user or poor performance while encrypting and decrypting data. Moreover, algorithms that were previously seen as theoretically unbreakable are now being theorized to be easily breakable with the advancement in quantum computing [79, 80]. Even during the pandemic, weak cryptographic implementations have caused enormous damages to systems of both individuals and organizations, and often they are accompanied by poor implementation of the base system itself. Keeping in mind these drawbacks, there arises a need to make a more robust and secure cryptographic solution, Studies [81–83] work on developing an advanced cryptosystem that relies on fractal functions as their core confusion function. All these studies use various fractal functions such as Mandelbrot set, Julia set [81–83] and Hilbert curve [81, 83] to create a secure encryption and decryption cryptosystem that will be quantum-safe; that is, this particular cryptosystem, unlike current cryptosystems, will be immune to quantum attacks. These studies only use fractal encryption on images; further studies should be conducted to make fractal encryption more optimized for day-to-day use and should be able to perform encryption-decryption on a large variety of data [84].

6.4 Auto Adaptive Security Policies Frameworks

The biggest problem of the organization today is the security threat. These threats can be internal as well as external. A security policy is made for these threats that apply to the entire enterprise. During and after the covid pandemic, it has not been active to respond to cyber threats so fast in the traditional way or to block part of a particular system. Auto adaptive security policy framework analyzes the behavior and auto adapts to the event before any threat occurs [85]. While static approaches significant operation and adapts for security, when the system feels that it is under attack, it processes thousands of rules to adapt to the threat. Also, it changes the firewall rules according to the adapted regulations. To protect the critical system, it breaks and isolates it. The same dynamic approach has multiple environments with many different rules. Use conditional evaluators based on network security test different profiles in a fixed amount of time. Auto calculates the changes to auto adapt the risk.

The Cognitive Cyber-Physical System adapts this security framework. Through the dynamic environment of the critical infrastructure of the cyber-physical system, it associates it with the transmission codes. The physical device is connected with the cyber-physical system, so monitoring, control center, and AI-based security points are enabled. This framework also enhances mobile devices' and wearable devices' security. The security framework is implemented through mapping in these devices. Identifying the threat, freezing, and protecting the system are all considered. After the covid pandemic, many new threads came from the remote work culture. Due to this, organizations found it difficult to monitor individual threats. This mechanism helped a lot in monitoring the employees working at the remote location, securing the organization infra and system by using tools and environment based on the framework [44].

6.5 Advance Data Modification & Breach Prevention Solution

In the covid pandemic, data of many major organizations were breached. The major data breach in this timeline contained card data of customers of Dominos, Juspay, MobiKwik. Data controllers are expected to manage data securely by executing technical measures, for example, authenticated permission to data and encryption, and progressive measures, such as planning staff on data insurance and setting techniques for fitting induction to individual data. Perform encryption and pseudonymization (a system for overriding eventually detailed data with other near data) of individual data. Assurance of the confidentiality and integrity of data planning structures restore availability and permission to individual data if it becomes difficult to reach. Test, study, and survey measures for getting data planning, assessing, and evaluating the feasibility of technical and progressive measures for ensuring the security of dealing with the data breach.

Rule-based expressions are being used to avoid data modification and data breaches. Filters are used in the rule-based technique; these rules are configured after that. Data modification is also prevented by data fingerprinting, under which Exact matches against Exact fingerprinting technology are applied. Content-based Cross Domain Security (CDS) is like a guard standing on both sides. Its base depends on technical monitoring and alerting. Sensing any movement on the sensitive data storage place generates alerts. To control the risk of the database, the organizations have started setting up the Security Command Center, which provides the facility of risk analysis, suffering, breach control, modification control in the cloud environment. For this, these command centers mainly use Traffic Spike and Deny Ratio. Traffic Spike notifies users of a spike in traffic basis. A finding is generated when there is an increase in the allowed number of requests per second (RPS) compared to the typical volume observed in recent history. The Increasing Deny Ratio finding notifies users that there is an increase in the Ratio of traffic.

6.6 Advanced Persistent Threat Frameworks

Advanced Persistent Threats (APTs) are threat actors who gain unauthorized access to systems. The persistence and stealthiness of these threats make them unique. They often stay undetected for a lot of time. According to FireEye, before APT detection in America, the meantime was around 70 days. Often, these are state-sponsored groups which makes them more concerning. However, there are a lot of challenges in the detection as well as in the cleanup phase of such persistent threats. The ever-changing signatures and behavior of the malware make it extremely difficult for a single system to detect them [86]. Moreover, detection and mitigation of such threats take a substantial financial toll, especially for third-world countries [87]. This suggests that prevention through strong defenses is a much better approach.

Still, there are various types of solutions coming out through research often. It can be a fine-grain behavior analysis of users in the system to isolate malicious activity [86, 88]. Other solutions include network-based intrusion detection systems, traffic flow analysis, white-listed domains, and IP addresses and semantic models [87]. This involves a lot of forensic investigation and different methods, which should be efficient. Many meta-heuristic approaches are suggested for this, like a hybrid particle swarm optimization algorithm explicitly designed to enhance APT detection [89]. The variety of methods mentioned earlier often proves weak in front of complex threats in today's world. Hence, many frameworks are designed of different architectures to encompass multiple ways to form a solid defense. One such framework is HuMa [90] which is a multi-layer framework composed of three different layers. These layers contribute to the investigation of complex security events. A similar but unique approach is shown by the DFA-AD framework [91]. It is a distributed framework that employs various parallel classifiers. All the independent evaluation results are correlated to more accurate detection of such threats. These frameworks need to be updated constantly with new techniques and efficient methods to keep up with the novel malware appearing in recent APT attacks.

6.7 AI-driven Security Mechanisms

AI is outpacing every other conservative algorithm in a variety of fields. It is proving efficient, accurate, and precise due to many fine-tuning parameters. For example, the latest GPT-3 itself has 175 billion parameters [92]. The only limitation is a computation that is ever-improving. It makes AI a very suitable candidate for security or defense systems because it is the ability to find patterns quickly. The major challenge of AI security systems is the lack of trust. Studies have been conducted which show the association between an individual's attachment security and trust in AI [93]. Moreover, to build trust in users, the mechanisms should demonstrate responsible behavior. This way, various types of mechanisms like institutional, hardware, and software should be built around these claims [94]. Once this is settled, AI comes up with a lot of opportunities. AI can be used to mitigate the different issues in the 6G architecture itself. The issues can be regarding security, privacy, and ethics [95]. Another disruptive technology is Blockchain. A survey has been conducted where AI can be helpful in the emerging blockchain application. This gives rise to the concept of Decentralized AI [96] which is a combination of AI and Blockchain. It is used for analytics purposes and decision-making in unique scenarios.

7 Conclusion

COVID-19 was not the first epidemic mankind has faced, but it was unique in its true nature the way people resorted to hurt or loot other fellow personnel who are currently reeling in pain and in dire need of medication. This epidemic has suddenly forced personnel to shift their working culture from offices to home, and no one was ready with this. Suppose today, and someone searches importance of training in the information technology domain. In that case, there is no literature available. In contrast, it has been

the conception that the information technology (IT) domain is the supporting pillar for improving the way training is being imparted to the needy. In this scenario, even the information technology domain was not ready to the full extent, and cyber perpetrators took advantage of it.

cyber crime has been increasing since the inception of the internet, but during this epidemic, it became itself a new kind of epidemic which we can call a "Cydemic". Cybercriminals were the entities who always kept their eyes and ears over any slight changes in the working of any IT, thus creating a little bit of confusion among the common public and an absolutely right time for criminals to strike. The cybercriminals en-cashed this key factor during this covid time in abundance. People were not aware or ready, and there was a lot of confusion among the personnel. Lots of people lost their jobs due to the void, which occurred in the market pertaining to the covid lock-downs. These people were also part of the workforce of cyber criminals in this uncertain time, as this seems the shortcut and faster means to earn or make money while sitting in their homes. This possibility cannot be overturned anytime.

People in their homes were starving, having anxiety initially for not having any medicine for the same and later not being in the priority queue of getting vaccinated. The modus operandi of these cyber criminal has been in coherence with this fast-changing paradigm and thus gave them a niche point others. Nations build applications for helping their citizen, and criminals create their own way of trapping the innocents using phishing attacks, sometimes vishing them away. Thus people have been duped every time in a new manner. Be it a scam for any online job activity, or vaccination or oxymeter, etc. Even when governments created applications to keep track of the covid infected people, hackers were way ahead and took the data being stored or transmitted to government servers for further analysis. Since in this testing time, every individual or office was forced to resort to any readily available alternate version of the previous way of handling the activities prior to covid. This paved the possibilities of vulnerabilities or bugs into the newly developed applications, too; as for testing it, the prescribed time was never there. This analysis of ours has tried to showcase different types of crime and their modus operandi. However, this research is unique from other research as in this we have also tried to work on possible solutions in a technological fashion. Even in this, the survey and data related to cyber crime were taken from different countries available in an open manner. This research has showcased in a unique manner how to tackle the menace of cybercriminals using the technology available and filling the void with an improvement of the technological platforms.

References

[1] C.C. Lai, T.P. Shih, W.C. Ko, H.J. Tang, and P.R. Hsueh. Severe acute respiratory syndrome coronavirus 2 (sars-cov-2) and coronavirus disease-2019 (covid-19): The epidemic and the challenges. *International journal of antimicrobial agents*, 55(3):105924, March 2020.

[2] J. Yang, L. Wang, and S. Shakya. Modelling network traffic and exploiting encrypted packets to detect stepping-stone intrusions. *Journal of Internet Services and Information Security (JISIS)*, 12(1):2–25, February 2022.

[3] J. Kim, K. Kim, G. Y. Jeon, and M. Sohn. Temporal patterns discovery of evolving graphs for graph neural network (gnn)-based anomaly detection in heterogeneous networks. *Journal of Internet Services and Information Security (JISIS)*, 12(1):72–82, February 2022.

[4] D. Buil-Gil, F. Miró-Llinares, A. Moneva, S. Kemp, and N. Díaz-Castaño. Cybercrime and shifts in opportunities during covid-19: a preliminary analysis in the uk. *European Societies*, 23(sup1):S47–S59, August 2021.

[5] H.S. Lallie, L.A. Shepherd, J.R.C. Nurse, A. Erola, G. Epiphaniou, C. Maple, and X. Bellekens. Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, 105:102248, June 2021.

[6] M.B. Sleiman and S. Gerdemann. Covid-19: a catalyst for cybercrime? *International Cybersecurity Law Review*, 2(1):37–45, April 2021.

[7] S. Hakak, W.Z. Khan, M. Imran, K.R. Choo, and M. Shoaib. Have you been a victim of covid-19-related cyber incidents? survey, taxonomy, and mitigation strategies. *IEEE Access*, 8:124134–124144, June 2020.

[8] S. Kemp, D. Buil-Gil, A. Moneva, F. Miró-Llinares, and N. Díaz-Castaño. Empty streets, busy internet: A time-series analysis of cybercrime and fraud trends during covid-19. *Journal of Contemporary Criminal Justice*, 37(4):480–501, July 2021.

[9] S. Monteith, M. Bauer, M. Alda, J. Geddes, P.C. Whybrow, and T. Glenn. Increasing cybercrime since the pandemic: Concerns for psychiatry. *Current Psychiatry Reports*, 23(4):1–9, March 2021.

[10] S. Venkatesha, K.R. Reddy, and B.R. Chandavarkar. Social engineering attacks during the covid-19 pandemic. *SN computer science*, 2(2):1–9, February 2021.

[11] P. Datta, S.N. Panda, S. Tanwar, and R.K. Kaushal. A technical review report on cyber crimes in india. In *Proc. of the 2020 International Conference on Emerging Smart Computing and Informatics (ESCI'20), Pune, India*, pages 269–275. IEEE, March 2020.

[12] B. Collier, S. Horgan, R. Jones, and L. Shepherd. The implications of the covid-19 pandemic for cybercrime policing in scotland: a rapid review of the evidence and future considerations. *Scottish Institute for Policing Research*, (1):1–18, May 2020.

[13] R. Naidoo. A multi-level influence model of covid-19 themed cybercrime. *European Journal of Information Systems*, 29(3):306–321, May 2020.

[14] M. Kashif, M.K. Javed, and D. Pandey. A surge in cyber-crime during covid-19. *Indonesian Journal of Social and Environmental Issues (IJSEI)*, 1(2):48–52, August 2020.

[15] Interpol. Global landscape on covid-19 cyberthreat, April 2020. `https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats` [Online; Accessed on May 10, 2022].

[16] J. Hawdon, K. Parti, and T.E. Dearden. Cybercrime in america amid covid-19: The initial results from a natural experiment. *American Journal of Criminal Justice*, 45(4):546–562, June 2020.

[17] A.V. Vu, J. Hughes, I. Pete, B. Collier, Y.T. Chua, I. Shumailov, and A. Hutchings. Turning up the dial: the evolution of a cybercrime market through set-up, stable, and covid-19 eras. In *Proc. of the 20th ACM Internet Measurement Conference (IMC'20), Virtual Event, USA*, pages 551–566. ACM, October 2020.

[18] E.F. Adeniran and H. Jahankhani. A descriptive analytics of the occurrence and predictive analytics of cyber attacks during the pandemic. In R. Montasari, H. Jahankhani, and H. Al-Khateeb, editors, *Challenges in the IoT and Smart Environments*, pages 123–159. Springer, 2021.

[19] E.R. Leukfeldt, R.J. Notté, and M. Malsch. Exploring the needs of victims of cyber-dependent and cyber-enabled crimes. *Victims & Offenders*, 15(1):60–77, October 2020.

[20] A. Nicaso and M. Danesi. *Organized crime: A cultural introduction*. Routledge, 2021.

[21] D. Croasdell and A. Palustre. Transnational cooperation in cybersecurity. In *Proc. of the 52nd Hawaii International Conference on System Sciences (HICSS-52), Grand Wailea, Hawaii*, page 5598. BY-NC-ND 4.0, January 2019.

[22] I. Cvitić, D. Peraković, M. Periša, and A.D. Jurcut. Methodology for detecting cyber intrusions in e-learning systems during covid-19 pandemic. *Mobile networks and applications*, pages 1–12, December 2021.

[23] H. Abroshan, J. Devos, G. Poels, and E. Laermans. Covid-19 and phishing: Effects of human emotions, behavior, and demographics on the success of phishing attempts during the pandemic. *IEEE Access*, 9:121916–121929, August 2021.

[24] J.R.C. Pulliam, C.V. Schalkwyk, N. Govender, A.V. Gottberg, C. Cohen, M.J. Groome, J. Dushoff, K. Mlisana, and H. Moultrie. Increased risk of sars-cov-2 reinfection associated with emergence of the omicron variant in south africa. *SCIENCE*, 376(6593), March 2022.

[25] A.O. Kwok and S.G. Koh. Deepfake: a social construction of technology perspective. *Current Issues in Tourism*, 24(13):1798–1802, March 2021.

[26] K.W.F Ma and T. McKinnon. Covid-19 and cyber fraud: emerging threats during the pandemic. *Journal of Financial Crime*, 29(2):433–446, May 2021.

[27] I.C. Eian, L.K. Yong, M.Y.X Li, Y.H. Qi, and Z. Fatima. Cyber attacks in the era of covid-19 and possible solution domains, September. `https://www.preprints.org/manuscript/202009.0630/download/final_file` [Online; Accessed on May 10, 2022].

[28] B. Pranggono and A. Arabo. Covid-19 pandemic cybersecurity issues. *Internet Technology Letters*, 4(2):e247, October 2020.

[29] A. Gryszczyńska. The impact of the covid-19 pandemic on cybercrime. *Bulletin of the Polish Academy of Sciences. Technical Sciences*, 69(4):e137933, August 2021.

[30] F. Cristani. Economic cyber-espionage in the (post) covid-19 era in europe: Which (new) challenges? Proceedings of the conferences of the Department of Civil Law and Procedure, National Aviation University, 2021. `https://er.nau.edu.ua/handle/NAU/48736` [Online; Accessed on May 10, 2022].

[31] I. Aldasoro, J. Frost, L. Gambacorta, and D. Whyte. Covid-19 and cyber risk in the financial sector. Technical report, Bank for International Settlements, January 2021.

[32] Tech2 News Staff. Domino's india data breach: Name, location, mobile number, email of 18 crore orders up for sale on dark web, June 2021. `http://shorturl.at/cxyMS` [Online; Accessed on May 10, 2022].

[33] BusinessLine. Data of 3.5 m mobikwik users allegedly hacked, March 2021. `https://www.thehindubusinessline.com/info-tech/data-of-35-m-mobikwik-users-allegedly-hacked/article34192591.ece#` [Online; Accessed on May 10, 2022].

[34] A. Ghangare and A. Ranade. Aadhar card–perspectives on privacy. *Journal of International Pharmaceutical Research*, 46(5):135–142, September 2019.

[35] A. Bahuguna, R.K. Bisht, and J. Pande. Country-level cybersecurity posture assessment: study and analysis of practices. *Information Security Journal: A Global Perspective*, 29(5):250–266, May 2020.

[36] A.S. Khader and D. Lai. Preventing man-in-the-middle attack in diffie-hellman key exchange protocol. In *Proc. of the 22nd international conference on telecommunications (ICT'15), Sydney, NSW, Australia*, pages 204–208. IEEE, April 2015.

[37] V. Mavroeidis, K. Vishi, M.D. Zych, and A. Jøsang. The impact of quantum computing on present cryptography. *International Journal of Advanced Computer Science and Applications (IJACSA)*, 9(3):405–414, March 2018.

[38] J. Dey, A. Bhowmik, A. Sarkar, S. Karforma, and B. Chowdhury. Cryptographic engineering on covid-19 telemedicine: an intelligent transmission through recurrent relation based session key. *Wireless Personal Communications*, 122(4):3167–3204, September 2021.

[39] A. Im, S. Rahmadika, Y. H. Lee, B. Kim, and I. You. A note on enactment of blockchain for haccp-based cooperative model. *Journal of Internet Services and Information Security (JISIS)*, 12(1):44–56, February 2022.

[40] S. Chesney, K. Roy, and S. Khorsandroo. Machine learning algorithms for preventing iot cybersecurity attacks. In *Proc. of the 2020 Intelligent Systems Conference (IntelliSys'20), London, UK*, volume 1252 of *Advances in Intelligent Systems and Computing*, pages 679–686. Springer, Cham, September 2020.

[41] R.M. Gupta and M. Lall. Covid-19 pandemic and artificial intelligence possibilities: A healthcare perspective. *Medical Journal, Armed Forces India*, 77(Suppl2):S242–S244, July 2021.

[42] A. Majeed and S.O. Hwang. Data-driven analytics leveraging artificial intelligence in the era of covid-19: An insightful review of recent developments. *Symmetry*, 14(1):16, December 2022.

[43] G. Iakovakis, C.G. Xarhoulacos, K. Giovas, and D. Gritzalis. Analysis and classification of mitigation tools against cyberattacks in covid-19 era. *Security and Communication Networks*, 2021:21, August 2021.

[44] A. Georgiadou, S. Mouzakitis, and D. Askounis. Working from home during covid-19 crisis: a cyber security culture assessment survey. *Security Journal*, 35(2):486–505, February 2021.

[45] R.A. Carter. Dealing with data: Cybersecurity in the covid-19 era. *Engineering and Mining Journal*, 221(8):52–57, August 2020.

[46] M. Puys, P. H. Thevenon, S. Mocanu, M. Gallissot, and C. Sivelle. Scada cybersecurity awareness and teaching with hardware-in-the-loop platforms. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, 13(1):4–32, March 2022.

[47] A.A. Hussain, B.A. Dawood, and F. Al-Turjman. Application of ai techniques for covid-19 in iot and big data era: A survey. In F. Al-Turjman, editor, *Artificial Intelligence and Machine Learning for COVID-19*, pages 175–211. Springer, 2021.

[48] V.V. Burlakov, E.V. Skubriy, L.N. Orlova, G.V. Fedotova, and A.V. Sukhinin. Cyber security in the era of

covid-19: Threats to digital platforms stability and cyber hygiene rules. In E.G. Popkova, V.N. Ostrovskaya, and A.V. Bogoviz, editors, *Socio-economic Systems: Paradigms for the Future*, pages 1565–1574. Springer, 2021.

[49] O.S. Althobaiti and M. Dohler. Cybersecurity Challenges Associated With the Internet of Things in a Post-Quantum World. *IEEE Access*, 8:157356–157381, August 2020.

[50] M. Rahman and H. Jahankhani. Security Vulnerabilities in Existing Security Mechanisms for IoMT and Potential Solutions for Mitigating Cyber-Attacks. In H. Jahankhani, S. Kendzierskyj, and B. Akhgar, editors, *Information Security Technologies for Controlling Pandemics*, pages 307–334. Springer International Publishing, 2021.

[51] M. Sakhai and M. Wielgosz. Modern Cybersecurity Solution using Supervised Machine Learning. arXiv:2109.07593, September 2021. `https://doi.org/10.48550/arXiv.2109.07593`.

[52] S. Chesney, K. Roy, and S. Khorsandroo. Machine Learning Algorithms for Preventing IoT Cybersecurity Attacks. In Kohei Arai, Supriya Kapoor, and Rahul Bhatia, editors, *Intelligent Systems and Applications*, pages 679–686. Springer International Publishing, 2021.

[53] N. Argyropoulos, P.S. Khodashenas, O. Mavropoulos, E. Karapistoli, A. Lytos, P.A. Karypidis, and K.P. Hofmann. Addressing Cybersecurity in the Next Generation Mobility Ecosystem with CARAMEL. *Transportation Research Procedia*, 52:307–314, September 2021.

[54] E. Begoli, R.A. Bridges, S. Oesch, and K.E Knight. What Clinical Trials Can Teach Us about the Development of More Resilient AI for Cybersecurity. *arXiv:2105.06545 [cs]*, page 16, May 2021.

[55] A.A.H Alosaimi and M. Elloumi. Back propogation neural network based cybersecurity information retrival from repository. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 12(10):1197–1204, 2021.

[56] S. Miller and L. Bhattacharya. Cybersecurity at FireEye: Human + AI, April 2021. `https://ink.library.smu.edu.sg/cases_coll_all/339/` [Online; Accessed on May 10, 2022].

[57] T. Wickline. The Capabilities of Antivirus Software to Detect and Prevent Emerging Cyberthreats - ProQuest, May 2021. `https://www.proquest.com/openview/f04aec327c82562b1e7ce152964e442a/1?pq-origsite=gscholar&cbl=18750&diss=y` [Online; Accessed on May 10, 2022].

[58] R. Sivarethinamohan and S. Sujatha. Behavioral Intentions towards adoption of Information Protection and Cyber security (Email Security and Online Privacy): SEM model. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 12(6):56–68, April 2021.

[59] S.M.L. de Lima, H.K. de L. Silva, J.H. da S. Luz, H.J. do N. Lima, S.L. de P. Silva, A.B.A. de Andrade, and A.M. da Silva. Artificial intelligence-based antivirus in order to detect malware preventively. *Progress in Artificial Intelligence*, 10(1):1–22, March 2021.

[60] Z.A. Hamed, I.M. Ahmed, and S.Y. Ameen. Protecting Windows OS Against Local Threats Without Using Antivirus. *International Journal of Advanced Science and Technology*, 29(12s):64–70, May 2020.

[61] J. Delaney. The Effectiveness of Antivirus Software - ProQuest, August 2020. `https://www.proquest.com/openview/d3ff27e1e773c8dd36e7746e64567702/1?pq-origsite=gscholar&cbl=44156` [Online; Accessed on May 10, 2022].

[62] R.W. Scholz, R. Czichos, P. Parycek, and T.J. Lampoltshammer. Organizational vulnerability of digital threats: A first validation of an assessment method. *European Journal of Operational Research*, 282(2):627–643, April 2020.

[63] I. Zografopoulos, J. Ospina, X. Liu, and C. Konstantinou. Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies. *IEEE Access*, 9:29775–29818, February 2021.

[64] I. Homoliak, S. Venugopalan, D. Reijsbergen, Q. Hum, R. Schumi, and P. Szalachowski. The Security Reference Architecture for Blockchains: Toward a Standardized Model for Studying Vulnerabilities, Threats, and Defenses. *IEEE Communications Surveys & Tutorials*, 23(1):341–390, October 2021.

[65] A. Hassan, H.M. Abdullah, U. Farooq, A. Shahzad, R. Muhammad, A.F. Haider, and A.U. Rehman. A Wirelessly Controlled Robot-based Smart Irrigation System by Exploiting Arduino. *Journal of Robotics and Control (JRC)*, 2(1):29–34, January 2021.

[66] H.F. Alqahtani, J.A. Albuainain, B.G. Almutiri, S.K. Alansari, G.B. AL-awwad, N.N Alqahtani, S.M.

Masaad, and R.A. Tabeidi. Automated smart locker for college. In *Proc. of the 3rd International Conference on Computer Applications & Information Security (ICCAIS'20), Riyadh, Saudi Arabia*, pages 1–6. IEEE, March 2020.

[67] Y. Chen, F.M. Zahedi, A. Abbasi, and D. Dobolyi. Trust calibration of automated security IT artifacts: A multi-domain study of phishing-website detection tools. *Information & Management*, 58(1):103394, January 2021.

[68] O.A. Waraga, M. Bettayeb, Q. Nasir, and M.A Talib. Design and implementation of automated IoT security testbed. *Computers & Security*, 88:101648, January 2020.

[69] V. Ravi, S. Kp, M. Alazab, S. Sriram, and K. Simran. A Comprehensive Tutorial and Survey of Applications of Deep Learning for Cyber Security. Technical Report 10.36227/techrxiv.11473377.v1, TechRxiv, 2020.

[70] S. Rathore and J.H. Park. A Blockchain-Based Deep Learning Approach for Cyber Security in Next Generation Industrial Cyber-Physical Systems. *IEEE Transactions on Industrial Informatics*, 17(8):5522–5532, August 2021.

[71] D. Chen, P. Wawrzynski, and Z. Lv. Cyber security in smart cities: A review of deep learning-based applications and case studies. *Sustainable Cities and Society*, 66:102655, March 2021.

[72] M.A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, 50:102419, February 2020.

[73] S.C. Sundaramurthy, M. Wesch, X. Ou, J. McHugh, S.R. Rajagopalan, and A. Bardas. Humans are dynamic. our tools should be too. innovations from the anthropological study of security operations centers. *IEEE Internet Computing*, pages 1–1, June 2017.

[74] C. Feng, S. Wu, and N. Liu. A user-centric machine learning framework for cyber security operations center. In *Proc. of the 2017 IEEE International Conference on Intelligence and Security Informatics (ISI'17), Beijing, China*, pages 173–175. IEEE, July 2017.

[75] D.F. Mirilla, C.C Tappert, R.I Frank, and L. Tao. A proposed dynamic security operations center management framework for reducing task disengagement. In *Proc. of Student-Faculty Research Day, CSIS, Pace University, New York, NY, USA*, pages D6–1–D6–8, May 2018.

[76] D. MegÃas, M. Kuribayashi, A. Rosales, K. Cabaj, and W. Mazurczyk. Architecture of a fake news detection system combining digital watermarking, signal processing, and machine learning. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, 13(1):33–55, March 2022.

[77] G. Ali, N. Ahmad, Y. Cao, S. Khan, H. Cruickshank, E.A. Qazi, and A. Ali. xdbauth: Blockchain based cross domain authentication and authorization framework for internet of things. *IEEE Access*, 8:58800–58816, March 2020.

[78] M. Tahir, M. Sardaraz, S. Muhammad, and M.S. Khan. A lightweight authentication and authorization framework for blockchain-enabled iot network in health-informatics. *Sustainability*, 12(17):6960, August 2020.

[79] Z. Kirsch and M. Chow. Quantum computing: The risk to existing encryption methods, December 2015. `https://www.cs.tufts.edu/comp/116/archive/fall2015/zkirsch.pdf` [Online; Accessed on May 10, 2022].

[80] M. Leitner, M. Frank, G. Langner, M. Landauer, F. Skopik, and et. al. Enabling exercises, education and research with a comprehensive cyber range. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, 12(4):37–61, December 2021.

[81] S. Agarwal. A new composite fractal function and its application in image encryption. *Journal of Imaging*, 6(7):70, July 2020.

[82] S.K. Abd-El-Hafiz, A.G. Radwan, S.H.A Haleem, and M.L. Barakat. A fractal-based image encryption system. *IET Image Processing*, 8(12):742–752, December 2014.

[83] S. Agarwal. Image encryption techniques using fractal function: A review. *International Journal of Computer Science and Information Technology*, 9(2):53–68, April 2017.

[84] S. Manfredi, M. Ceccato, G. Sciarretta, and S. Ranise. Empirical validation on the usability of security reports for patching tls misconfigurations: User- and case-studies on actionable mitigations. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, 13(1):56–86,

March 2022.

[85] M. Yousif, C. Hewage, and L. Nawaf. Iot technologies during and beyond covid-19: a comprehensive review. *Future Internet*, 13(5):105, April 2021.

[86] A. Alshamrani, S. Myneni, A. Chowdhary, and D. Huang. A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities. *IEEE Communications Surveys Tutorials*, 21(2):1851–1877, January 2019.

[87] S. Singh, P.K. Sharma, S.Y. Moon, D. Moon, and J.H. Park. A comprehensive study on APT attacks and countermeasures for future networks and communications: challenges and solutions. *The Journal of Supercomputing*, 75(8):4543–4574, August 2019.

[88] K. Okereafor and O. Adelaiye. Randomized cyber attack simulation model: A cybersecurity mitigation proposal for post covid-19 digital era. *International Journal of Recent Engineering Research and Development (IJRERD)*, 5(07):61–72, July 2020.

[89] A.K. Alhwaitat, S. Manaseer, and M. Alsyyed. A survey of digital forensic methods under advanced persistent threat in fog computing environment. *Journal of Theoretical and Applied Information Technology*, 97(18):4934–4954, September 2019.

[90] J. Navarro, V. Legrand, S. Lagraa, J. François, A. Lahmadi, G.D. Santis, O. Festor, N. Lammari, F. Hamdi, A. Deruyver, Q. Goux, M. Allard, and P. Parrend. Huma: A multi-layer framework for threat analysis in a heterogeneous log environment. In *Proc. of the 10th International Symposium on Foundations and Practice of Security (FIPS'17), Nancy, France*, volume 10723 of *Lecture Notes in Computer Science*, pages 144–159. Springer-Cham, October 2017.

[91] P.K. Sharma, S.Y. Moon, D. Moon, and J.H. Park. DFA-AD: a distributed framework architecture for the detection of advanced persistent threats. *Cluster Computing*, 20(1):597–609, March 2017.

[92] T.B. Brown, B. Mann, N. Ryder, M. Subbiah, J.D. Kaplan, and et. al. Language Models are Few-Shot Learners. *Advances in neural information processing systems*, 33:1877–1901, July 2020.

[93] O. Gillath, T. Ai, M.S. Branicky, S. Keshmiri, R.B. Davison, and R. Spaulding. Attachment and trust in artificial intelligence. *Computers in Human Behavior*, 115:106607, February 2021.

[94] M. Brundage, S. Avin, J. Wang, H. Belfield, G. Krueger, and et. al. Toward Trustworthy AI Development: Mechanisms for Supporting Verifiable Claims. *arXiv:2004.07213 [cs]*, page 80, April 2020.

[95] Y. Siriwardhana, P. Porambage, M. Liyanage, and M. Ylianttila. AI and 6G Security: Opportunities and Challenges. In *Proc. of the 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit'21), Porto, Portugal*, pages 616–621. IEEE, June 2021.

[96] K. Salah, M.H.U Rehman, N. Nizamuddin, and A. Al-FuqahaS. Blockchain for AI: Review and Open Research Challenges. *IEEE Access*, 7:10127–10149, January 2019.

Author Biography

Arjun Choudhary has been an Assistant Professor with the Department of Cyber Security, Sardar Patel University of Police. He is Deputy Director at the Centre of Cyber Security, Sardar Patel University of Police, Security and Criminal Justice. His current research interests include Cloud Computing, Web apps, and Digital Forensics. He has organized various international and national training programs for Law Enforcement Agencies. He also has (co-)authored many journal/conference papers and book chapters.

Gaurav Choudhary received a Ph.D. in Information Security Engineering from Soonchunhyang University, South Korea. He has done a Master of Technology in Cyber Security from the Sardar Patel University of Police and received a Chancellor Gold Medal for Academic Excellence. He is presently working as a Security Researcher at DTU Compute, Department of Applied Mathematics and Computer Science, Technical University of Denmark (DTU). Prior to joining DTU, he has also worked as an Assistant Professor in the School of Computer Science, University of Petroleum and Energy Studies (UPES), and School of Computer Science and Engineering (SCSE) at VIT Bhopal University. His current research interests include Threat Intelligence, IoT and CPS Security, Cyber Security, Vulnerability Assessment, 5G Security, Drone Security, and Cryptography. He has authored or co-authored many reputed SCI journal/conference papers and book chapters.

Kapil Pareek received the B.Tech degree in Computer Science and Engineering from Rajasthan Technical University in 2019 and the Master Degree in Cyber Security from Sardar Patel University of Police Security and Criminal Justice in 2021. He is currently working as security analyst in Juspay Technologies Private Limited, Bangalore. His areas of research are threat analysis, network security, vulnerability management and deep learning.

Chetanya Kunndra received the B.Tech degree in Computer Science and Engineering from Guru Gobind Singh Indraprastha University, Delhi, India in 2020 and is currently pursuing M.Tech from Sardar Patel University of Police, Rajasthan, India. His current research interests revolve around Industrial control systems, Malwares, Network security and ML based security solutions.

Jatin Luthra is currently pursuing his B.Tech degree in the department of Communication and Computer Engineering from The LNM Institute of Information Technology, Rajasthan, India. His areas of interest are Cyber Security, Cloud Security, Machine Learning and Artificial Intelligence.

Nicola Dragoni is Professor in Secure Pervasive Computing at DTU Compute, Technical University of Denmark, where he also serves as Head of the DTU Center for Digital Security (DIGISEC) and Deputy Head of the DTU Compute's PhD School. Nicola Dragoni received the M.Sc. (cum laude) and Ph.D. degrees in computer science from the University of Bologna, Italy. His main research interests center around pervasive computing and security, with latest focus on Internet-of-Things, Fog/Edge computing and mobile systems. He has co-authored 130+ peer-reviewed scientific papers in international journals and conference proceedings. He has edited 3 journal special issues and 1 book. He has been active in a number of national and international projects.