Egyptian Informatics Journal 23 (2022) 197–214

Contents lists available at ScienceDirect

Egyptian Informatics Journal

journal homepage: www.sciencedirect.com

Full length article

Detecting Covid-19 chaos driven phishing/malicious URL attacks by a fuzzy logic and data mining based intelligence system

Syed Rameem Zahra [a], Mohammad Ahsan Chishti [b], Asif Iqbal Baba [c], Fan Wu [d,*]

[a] Department of Computer Science and Engineering, National Institute of Technology Srinagar, Kashmir, India
[b] Department of Information Technology, Central University of Kashmir, Ganderbal, Kashmir, India
[c] University of North Texas, Denton, TX, USA
[d] Department of Computer Science, Tuskegee University, Tuskegee, AL, USA

ARTICLE INFO

Article history:
Received 3 August 2021
Revised 19 October 2021
Accepted 1 December 2021
Available online 14 December 2021

Keywords:
Covid-19
Phishing
Business Email Compromise (BEC)
Ransomware
Fuzzy-Logic
Data mining
Cybercriminals
Security

ABSTRACT

With confusion and uncertainty ruling the world, 2020 created near-perfect conditions for cybercriminals. As businesses virtually eliminated in-person experiences, the COVID-19 pandemic changed the way we live and caused a mass migration to digital platforms. However, this shift also made people more vulnerable to cyber-crime. Victims are being targeted by attackers for their credentials or financial rewards, or both. This is because the Internet itself is inherently difficult to secure, and the attackers can code in a way that exploits its flaws. Once the attackers gain root access to the devices, they have complete control and can do whatever they want. Consequently, taking advantage of highly unprecedented circumstances created by the Covid-19 event, cybercriminals launched massive phishing, malware, identity theft, and ransomware attacks. Therefore, if we wish to save people from these frauds in times when millions have already been tipped into poverty and the rest are trying hard to sustain, it is imperative to curb these attacks and attackers. This paper analyses the impact of Covid-19 on various cyber-security related aspects and sketches out the timeline of Covid-19 themed cyber-attacks launched globally to identify the modus operandi of the attackers and the impact of attacks. It also offers a thoroughly researched set of mitigation strategies which can be employed to prevent the attacks in the first place. Moreover, this manuscript proposes a fuzzy logic and data mining-based intelligence system for detecting Covid-19 themed malicious URL/phishing attacks. The performance of the system has been evaluated against various malicious/phishing URLs, and it was observed that the proposed system is a viable solution to this problem.

1. Introduction

Covid-19 [1] continues to dictate the news and the cyber-security landscape throughout the world, despite efforts to contain it. It has not only claimed millions of lives but has also pushed billions into poverty by robbing them of their livelihoods [2,3]. The FUD (fear, uncertainty, and doubt) following the pandemic is something that both the good and the bad actors have noticed and use to their advantage. While the good use FUD to stay indoors and take necessary precautions to fight the virus, the bad actors prey on peoples' fear, confusion, and doubt to reap monetary and other benefits [4,5]. Due to the COVID-19 pandemic, everyone saw the whole world coming to a standstill. Some businesses closed down, and others had to adapt to the unfamiliar work-from-home and learn-from-home orders [6,7]. For containing the virus, the pandemic, also prompted various governments to impose travel bans, social distancing norms, and lockdowns. However, these metrics have a wide range of repercussions, as illustrated in Fig. 1.

Since the outbreak, there have been incidents of imposters posing as public officials (e.g., WHO) and private entities (e.g., supermarkets, airlines) [8], impersonating relief agencies (e.g., for raising funds), committing PPE fraud (use of Personal Protective

* Corresponding author.
E-mail address: fwu@tuskegee.edu (F. Wu).

Peer review under responsibility of Faculty of Computers and Information, Cairo University.

Production and hosting by Elsevier

https://doi.org/10.1016/j.eij.2021.12.003

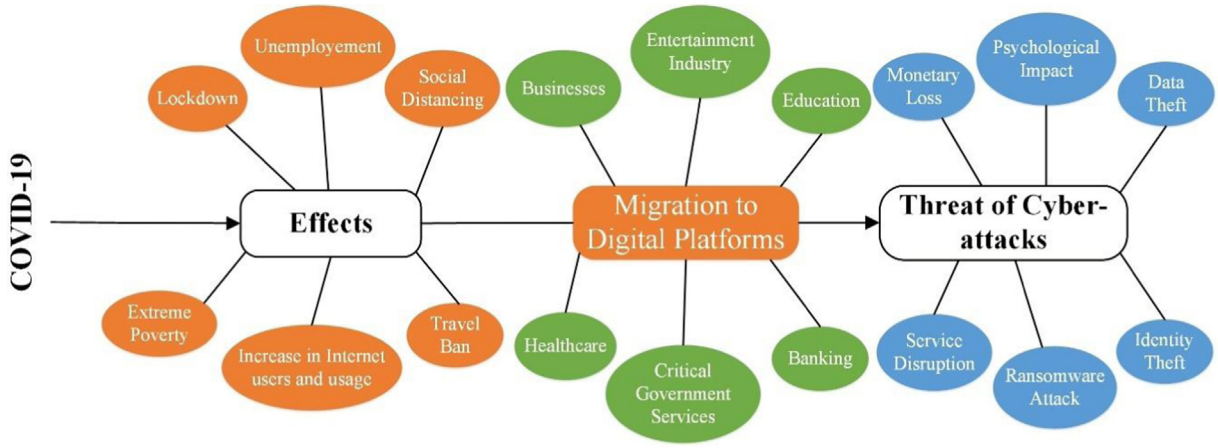

Fig. 1. Effects and repercussions of Covid-19.

Equipment), and marketing the COVID-19 cure [9]. One specific example is Singapore's minister for Home Affairs who stated that "a total of 394 frauds linked to Covid-19 were detected and victims were duped of at least SGD 1.4 million" between January and April 2020 [10]. Similarly, over 2,700 COVID-19-related fraud reports were received by the Australian Competition and Consumer Commission's Scamwatch, resulting in an estimated loss of over AUD 16,390,650 as of April 2020 [11]. Apart from imposter attacks, the world witnessed a series of other covid-19 related unparalleled cyber-attacks. Also, their number and diversity have increased significantly since the launch of Covid-19 because the cybercriminals quickly capitalised on this pandemic concept by rebranding common attack vectors.

The main contribution of this paper includes:

- An exhaustive research on how covid-19 altered the cyber-security priorities and spending. It identifies the existing loopholes in establishing security as a priority by the organizations and also sketches out how the surge in cyber-attacks forced the organizations to spend more on security.
- It analyses the trends and predicts the impact of covid-19 on the near and long-term growth of various security segments.
- An extensive survey on the surge in malicious domains, phishing attacks, Business Compromise Emails (BCE), and ransomware attacks has been done. This is because the major rise (both number and range) was seen only on these cyber-attacks during covid-19 times.
- To reveal the modus operandi of the attackers, this paper draws out a timeline of the major cyber-attacks launched by using covid-19 as a ruse in one form or the other. The timeline charts cyber-attacks in the world based on how the virus spread. It was observed that on average four major covid-19 related cyber-crime incidents occurred every month. Also, this timeline identifies malicious domains, phishing, scamming, email forging and mobile app spoofing to be the most employed social engineering techniques used during Covid-19. Ransomware, Trojans, and bots were routinely used to exploit systems and resources. This information will help in anticipating and detecting potential attacks, thereby enhancing preparedness in case of the next event.
- It was observed that during the COVID-19 pandemic, government offices, hospitals and healthcare, retail, education and Information Technology were among the most targeted essential infrastructures and industries. Also, the countries that felt the major brunt of cyber-attacks were identified in this work.
- Discusses possible mitigating measures for dealing with the identified threats. These measures are crucial to detect a breach in users' defences and prevent the attack launch.
- After recognizing that a major rise was seen in malicious domain and phishing attacks during COVID times, a system for detecting Covid-19 themed malicious URL/phishing attacks is proposed. The proposed system is based on fuzzy logic and data mining.
- The performance of the proposed system is evaluated against the state-of-the-art contemporaries.
- Lays out the foundation for future work.

To the best of our knowledge, this work is first of its kind that analyses the impact of Covid-19 on various cyber-security related aspects, outlines the timeline of Covid-19 themed cyber-attacks launched globally, discusses the impact of these attacks, offers a set of mitigation strategies which can be employed to prevent the attacks and proposes a fuzzy logic and data mining-based intelligence system for detecting Covid-19 themed malicious URL/phishing attacks. The remainder of this paper is structured as follows: To extrapolate the significance of our work, Section 2 presents a critical analysis of the most recent, and relevant state-of-art methods discussing their advantages and shortcomings from Covid-19 related cybersecurity perspective. Section 3 sketches out the attack timeline related to Covid-19. Moreover, it reflects how Covid-19 changed the priorities and amplified the need for cybersecurity. It also highlights the effect of Covid-19 on various cyber-attacks, particularly phishing and ransomware attacks. Section 4 offers the mitigation measures to these attacks for stopping the attack before gaining a foothold of the system/ user credentials. Section 5 proposes a fuzzy logic and data mining-based intelligence mechanism to handle any type of malicious/ phishing URL attacks. In section 6, we analyse the efficiency of our proposed system under the influence of various malicious links. A comparison with the available state-of-art is also shown in section 6 to indicate the stage and reliability of our work. The paper is concluded in section 7 that also highlights areas of future research.

2. Related work

As we move through this time that will have lasting effects on how we function and live, we must continue to choose objectives that allow us to concentrate on our most important goals. The question we need to address is how to protect data, processes, and connectivity regardless of where employees and third parties

are located, assuming that a distributed working model needs to become the standard, and not the exception. The objective for the security professionals is to create a beachhead there and then coattail back into the corporate network via remote teleworker connections. At present, there is a dearth of literature concerning the effect of covid-19 to cybersecurity as currently most of the security researchers are devoted on the security and privacy of the Internet of Things (IoT), Wireless Sensor Networks (WSN), Software Defined Networks (SDN) and Industrial IoT (IIoT) [12–15]. However, whatever the scanty amount of work has been done in this direction, its critical analysis is tabulated in Table 1. The parameters for critical analysis are chosen according to the need of the hour. It is observed that just a few studies consider the security aspect of Covid-19. Most of the research is focussed on contact tracing and monitoring. None of the state-of-art methods has studied the impact of covid-19 on security segments and the rise of some specific attacks in these times. To address this problem, this manuscript reviews the effect of covid-19 on various security aspects and designs a fuzzy logic and data mining-based covid-19 related malicious domain/phishing system.

3. Timeline of Covid-19 linked cybersecurity attacks and effects

A once-in-a-lifetime opportunity was presented by the Covid-19 pandemic to scammers and hackers. The cybercriminals used the impact of the virus for their gain. The cyber-crime incidents resulting from the COVID-19 pandemic pose major threats to the world's defence and economy. The following sub-sections present a timeline of the cyber-attacks as the virus spread throughout the world and highlights the effects of Covid-19 on various facets of cybersecurity.

3.1. Timeline of cyberattacks launched in 2020's Covid crises

Understanding the mechanisms, as well as the spread and reach of these threats, is vital. Table 2 sketches out the timeline of these threats, countries affected and the mechanism employed by cybercriminals.

3.2. Effect of Covid-19 on cybersecurity priorities

The COVID-19 crisis and its related constraints showed us that many of the activities before March 2020 that we considered "priorities" were not really priorities [64,65]. Like other employees, 84% of security professionals were forced to work from home, which changed their priorities. It increased their stress levels, and workloads [66]. The number of meetings attended, and the number of workshops organized by them were much larger than usual. Some companies have increased and rapidly launched new Remote Desktop Protocol (RDP) and Virtual Private Network (VPN) services in their chase to meet their employees' work-from-home needs, completely ignoring the normal internal security validation processes [67]. Thanks to the concept of the Internet of Things (IoT), working-from-home brings with it a myriad of devices that are connected to the Internet through an open and unsecured RDP port [65,68]. Displaying a worldwide four-fold growth in RDP attacks and other massive targeted attacks like FireEye, Sunburst, and SolarWinds, COVID-19 illuminated the path for the evolution of the cyber-threat landscape [65,67]. As such, it must become a priority for the technology providers to revisit their plans for accommodating the new threat landscape. Research experts believe that activities like international espionage attacks and other cybercriminal activities will see a massive surge in the year 2021 [67]. Also, resilience must be highlighted as one of the core priorities of security procedures to help organizations sustain competitiveness and drive competitive advantage.

3.3. Effect of Covid-19 on cybersecurity spending

Following the COVID-19 lockdowns, the global economy witnessed a major shrink. According to the World bank, the global economy, advanced economies, and emerging market and developing economies saw 5.2%, 7%, 2.5%, and 3.6% contractions respectively in the year 2020. Also, the per capita incomes took a 3.6% dip [69], tipping millions of people into hardship and poverty. Fig. 2 illustrates the global recession scenario for the year 2020. According to estimates, this is the worst recession since World War II., and the recent research by experts predicts that the scarring effects of COVID-19 will take a longer time to heal than any of the previous epidemics, wars, and other financial crises [70].

However, no matter what the condition of the global economy may be, the pandemic brought the worth of cybersecurity to life and made us realize that cybersecurity diligence has to be made a priority and cannot be laid as an "afterthought." It is cybersecurity that keeps businesses operational and open. As such, if we wish to save the people currently working from home from further abjection and poverty, cyber-security spending by organizations has to increase. The chart given in Fig. 2 shows the effect of COVID-19 on cyber-security spending for the quarters of 2020.

Fig. 3 orchestrates that as the world witnessed a surge in cyber-attacks, organizations started spending more on cyber-security in the fourth quarter. The security segments which require attention for saving the businesses from running into a complete debacle include, viz. Firewalls, Access Management (AM), Cloud Security, Data Security, Web Application Firewall (WAF), Secure Email Gateways (SEG), Vulnerability Assessment (VA), Security Information and Event Management (SIEM), Privileged Access Management (PAM), Integrated Risk Management Solutions (IRMS), Endpoint Protection Platforms (EPP), Identity Governance and Administration (IGA), and Application Security Testing (AST). Table 3 extrapolates Gartner's 4-year prediction on the impact of COVID-19 on these Security segments.

3.4. Effect of Covid-19 on malicious domains

History stands testimony to the fact that expert cybercriminals have never missed the opportunity to cash on any hot subject, a mega occasion, or a celebrity in their social-engineering tactics. Their approach to the Covid-19 pandemic was no different. They used the disease that killed more than 3 million people [71] (18-April-2021) as a lure. As the virus spreads globally, people are naturally searching online for the most up-to-date information about how it may affect them and what they can do to protect themselves and their loved ones. As one might expect, thousands of registered domains today contain the words like Covid-19, covid19, COVID-19, ncov, and Corona-virus.

According to the threat intelligence report by Checkpoint, the possibility of a Covid-related domain being malicious is greater than 50% [72]. Fig. 4 indicates that the instances of access to malicious Covid-19 associated URLs increased throughout the year, hitting their peak in April. While, persistent activities could be seen in May and June, the third quarter (Q3) of 2020 again shows a huge rise in these instances. Moreover, Fig. 5 shows the top ten countries whose citizens have fallen victim to these ruses in the Q3 of 2020 [73].

3.5. Effect of Covid-19 on phishing and Business email Compromise attacks

The phishing campaigns use the heightened focus on COVID-19 to spread malware, squander money, and steal user credentials

Table 1
Review of related work.

Reference	Achievements	Sector studied?	Deals with Security and Privacy concerns?	Impact of covid-19 on the growth of various cyber-attacks studied?	Cyber-attacks mitigation strategies?	Any Covid-19 related attack detection performed?
Allam et al. [10]	The report examines the coronavirus outbreak from an urban perspective.It makes recommendations for how smart city networks should collaborate to improve standardisation processes to promote data sharing in the event of outbreaks or disasters.	Healthcare	No	No	No	No
Cho et al. [16]	Identifies the privacy implications of various contact tracing apps developed for covid-19.Suggests solutions to ensure privacy in these apps.	Healthcare	Yes	No	Yes	No
Carli et al. [17]	Utilizes Bluetooth enabled communication channel using asymmetric cryptography for sending messages.Ensures Privacy.	Cyber-Security	Yes	No	No	No
Gupta et al. [18]	Uses Wi-Fi datasets to observe individuals' proximity to positive cases in an organization while maintaining their privacy.	Cyber-security and healthcare	Yes	No	No	No
Yang et al. [19]	Identifies the relevance of containment measures taken by China for covid-19.	Prediction and diagnosis	No	No	No	No
Pirouz et al. [20]	Investigated the impact of weather on the number of Covid-19 cases using binary classification. Confirmed that with relative humidity and max temperature, No. of cases increase.	Prediction and diagnosis	No	No	No	No
Kumar et al. [21]	Reviews modern technologies for tackling Covid-19.	Not Applicable	No	No	No	No
Hakak et al. [22]	Reviews some of the dangerous cyber-attacks linked to COVID-19.	Cyber-Security	Yes	Yes	Yes	No
Wynants et al. [23]	Offers suggestions on how to improve prediction and diagnosis models.Identifies the two most reliable models.	Prediction and diagnosis	No	No	No	No
Javaid et al. [24]	Identifies useful technologies of Industry 4.0 that can aid in the proper control and management of the COVID-19 pandemic.	Healthcare	No	No	No	No
Khan et al. [25]	Identifies the top ten cyber-threats that have occurred or could occur during the COVID-19 pandemic.	Cyber-Security	Yes	Yes	No	No
Wang et al. [26]	Identifies the technologies that are being employed for fight against COVID-19 and explores the cyber-security risks linked to these technologies	Cyber-Security	Yes	Yes	Yes	No
Chigada et al. [27]	Examines the economic impact of cybercrimes during COVID-19.Identifies prevalent cybersecurity risks and security vulnerabilities in information systems during COVID-19.	Cyber-Security	Yes	Yes	Yes	No
Ferreira et al. [28]	Identifies COVID-19′s implications on cyber-security and healthcare	Cyber-security and healthcare	Yes	Yes	No	No
Ahmed et al. [29]	Suggests some security measures that can be used to protect personal and corporate data from cyber criminals during COVID-19	Cyber-Security	Yes	Yes	Yes	No
Tran [30]	Presents guidelines for attack defense in case of phishing and other cyber-security threats that are prevalent during COVID-19.	Cyber-Security	Yes	Yes	Yes	No
This Study	Discussed throughout the manuscript.	Cyber-Security	Yes	Yes	Yes	Yes

[74]. Phishing scams have been with us since the mid-90 s, and every time, the attackers have cashed on key calendar dates (e.g., tax day,) and times of uncertainty. The fact that an attacker only requires a small percentage of clicks to make financial or other gains is highly worrying. Following the rise in the number of infected people, the anxiety surrounding the pandemic is also spreading exponentially, which is exactly what malware developers are preying on [75,76]. The coronavirus created fodder for phishing attacks as the scammers could fetch fast and massive rewards just by sending phishing emails to millions of victims wanting to apply for funding assistance from the state, their employers,

banks, and other sources [77]. Using such an approach, in hopes of compromising as many individuals as possible, cybercriminals cast a less targeted but broader net. The Reports say that there has been a 667% increase in the number of successful email attacks since February 2020 [74,77,78] and a 220% increase in phishing attacks compared to the average yearly increase during other global pandemic times [79]. Though most of the phishing attacks are activated when victims click on links sent to them through emails, other types of phishing attack, called the "pharming attack," compromises the Domain Name Server (DNS) or the victim's device itself to take it to the phishing website.

Table 2
Timeline of cyberattacks launched in 2020′s Covid crises.

Type of cyber-attack	Focussed on	Launched on	Countries affected	Attack description
Phishing Malware [31]	Data theft	January 06, 2020	China	China accused Vietnam of launching a "Metaljack" phishing attack against district offices of China's Wuhan.
Smishing campaigns [32]	Money and credential squandering	January 19, 2020	All	Global incidents of SMS-based phishing attacks were reported.
Phishing Malware [33]	Money	January 28, 2020	Japan, China	"Emotet" malware was distributed via a "safety measure" email.
Phishing [34]	Stealing credentials	January 28, 2020	United States of America	Link in an email giving information about infected cases in the victim's area takes it to a website stealing its credentials.
Pharming [35]	Medical groups data	February 06, 2020	China	China accused India of launching a pharming campaign on its medical groups.
Ransomware [36]	Money	February 09, 2020	China	CXK-NMSL ransomware was spread through Covid-19 themed emails.
Phishing [37]	Data theft	February 10, 2020	All	Initial cases of "AZORult" malware identified.
Ransomware [38]	Money	February 13, 2020	China	Covid-19 themed emails led to the distribution of Dharma/ Crysis ransomware.
Phishing [38]	Credentials, money	March 02, 2020	Italy	"Trickbot" launched via email.
Phishing [38]	Credentials, money	March 04, 2020	All	"MBR Wiper" distributed in the cloak of contact tracing information.
Phishing [38]	Credentials	March 08, 2020	USA	A malware called "Formbook" was spread in the mask of parcel shipment advice.
Ransomware [38]	Money	March 10, 2020	USA	"Netwalker" ransomware infected systems in the district hospital of Illinois
Phishing [37]	Data theft	March 10, 2020	Spain	Victims lured in the name of Covid-19 remedy given by Israeli scientists.
Malware [36]	Data theft	March 12, 2020	Libya	A mobile application named "Corona live 1.1" giving information about deaths, and active covid-19 related cases was a Trojan stealing user data.
Phishing Malware [35]	Data theft	March 12, 2020	Mongolia	Mongolia accused China of using e-mails from the Mongolian Ministry for spreading malware "virgin panda."
Phishing Malware [35]	Laser-focussed on money	March 13, 2020	Philippines	Citizens attacked by the "REMCOS" malware.
Malicious domain [36]	Data theft	March 20, 2020	All	The developers of the website www.antivirus-covid19.site claimed it to be created by the scientists of Harvard University to act as an anti-virus against real Covid. Instead, it installed a malware "Blacknet-rat" on the systems trying to access it.
Smishing, Pharming [33]	Money, data	March 24, 2020	UK	SMS about free school meals took victims to website stealing payment credentials
Malware [35]	Data theft	April 10, 2020	Czech Republic	Attacks on hospitals in the Czech republic.
Ransomware [39]	Money, data	May 01, 2020	USA	"Maze" ransomware was launched at Asheville Plastic Surgery Institute.
Business Email Compromise [39]	Healthcare Data	May 05, 2020	USA	Three employees from BJC healthcare, St Louis, received emails that led to the breach of patient data.
Undetected [39]	Data theft	May 07, 2020	Japan	A data breach attack on the largest telecom company in Japan which made its entry through NTT based in Singapore
Ransomware [40]	Money	June 01, 2020	USA	The University of California paid a whopping 1.14 million USD in ransom for the release of its data held by "netwalker" hackers.
Ransomware [40]	Money	June 07, 2020	Japan	The car-maker Honda's internal systems were hacked, restricting access to emails, and computers. "Ekans" ransomware was identified as the main culprit here.
Undetected [39]	Data theft	June 16, 2020	England	An attack made the website of Care New England shutdown.
Malware [40]	Data theft	June 19, 2020	Australia	Malware attacks were reported through various sectors throughout Australia. China was accused.
Phishing [41]	Data, Money	July 01, 2020	Russia	The Twitter account of Russia's foreign minister was hacked, and the information was sold for 66 Bitcoins on the dark-web.
Ransomware [41]	Money, data theft	July 01, 2020	UK	Orange telecommunication company was targeted by "Nefilim" ransomware.
Ransomware [42]	Money	July 19, 2020	USA	The University of Utah was forced to pay a ransom of $457000 to regain control of its data.
Ransomware [41]	Data theft	July 24, 2020	Spain	Adif, the Spanish railway company, lost 800 GB of data to a data breach attack.
Phishing [42]	Credentials	August 06, 2020	USA	A security firm named "SANS" got 28,000 of its records compromised in a phishing attack.
Ransomware [42]	Money	August 24, 2020	Canada	A residential properties company called "Brookfield" was attacked by a group named "Darkside."
Ransomware [43]	Money	September 01, 2020	The Middle East and North Africa	High Profile "Eking," "Emotet," and "wastedLocker" attacks were launched on government organizations.

(*continued on next page*)

Table 2 (*continued*)

Type of cyber-attack	Focussed on	Launched on	Countries affected	Attack description
Ransomware [44]	Money, data theft	September 07, 2020	Pakistan	"Netwalker" ransomware was launched on Pakistan's biggest power supplier "K-electric." A ransom of $3.85 million was demanded.
Phishing [45]	Data theft	September 10, 2020	NATO member and cooperating countries	Russian hackers have been attacking government departments in NATO countries. The NATO training material was used as a phishing scheme lure that contains the malware that created a permanent backdoor on target machines.
Ransomware [46]	Data theft	September 28, 2020	France	On the servers of the French container transport and shipping company CMA CGM, ransomware "Ragnar Locker" was released.
Malware [47]	Data theft	October 01, 2020	Russia, India, Ukraine, Kazakhstan, Kyrgyzstan, and Malaysia	US home security officials claimed that cyber-attacks were being launched by Chinese hackers on various entities in these countries.
Phishing [48]	Data theft	October 04, 2020	Turkey, Azerbaijan	Greek hackers have disfigured the website of the Turkish parliament and 150 websites of the Azerbaijani Government in support of Armenia.
Malware [49]	Data theft	October 05, 2020	Africa, Asia, and Europe	A Chinese-speaking hacking group attacked diplomatic institutions and NGOs using "MosaicRegressor"- Italian hacking tool provider HackingTeam's code-adapted malware.
Cyber Espionage [50]	Data theft	October 06, 2020	Azerbaijan	An unnamed intelligence agency launched a cyber-espionage operation targeting Azerbaijani government agencies in the middle of the worsening dispute between Armenia and Azerbaijan over the territories of Nagorno-Karabakh.
Cyber Espionage [51]	Data theft	October 21, 2020	Iraq, Kuwait, Turkey, and the UAE	Iranian hackers attacked government institutions and telecommunications operators.
Phishing [52]	Research documents and data	Throughout October 2020	Sweden, Netherlands, Canada, the UK, Australia, Singapore, the U.S, and Denmark.	An Iranian hacking group, "Silent Librarian," targeted the universities in these nations.
Phishing [53]	Data theft	November 06, 2020	Southeast Asia	Vietnamese hacker group "OceanLotus" created fake websites and Facebook pages to spread malware to target victims.
Hacking [54]	Data theft	November 13, 2020	South Korea, India, France, Canada, and the U.S.	Microsoft claims Russia's "Fancy Bear" and North Korea's "Lazarus," "Cerium" hacking groups attacked COVID-19 vaccine producer pharmaceutical companies.
Malware [55]	Data, Money	November 15, 2020	India, Bangladesh, and Singapore	Blackberry's security team identified a hacker-for-hire group targeting financial organizations in these countries using the "Sombra" malware.
Phishing [56]	Data theft	November 27, 2020	UK	North Korean hackers targeted COVID-19 vaccine manufacturer AstraZeneca, by posing as recruiters and providing false offers to employees, including malware.
Ransomware [57]	Data, Money	November 29, 2020	Mexico	A Foxconn-owned Mexican facility was targeted by a "DopplePaymer" ransomware attack which led to the encryption of 1,200 servers, 20–30 TB of backups being erased, and the theft of 100 GB of encrypted data. Also, a ransom of $34 million was demanded.
Spear Phishing [58]	Data theft	December 01, 2020	All	According to a recent intelligence report from IBM Security X-Force, bad actors are impersonating biomedical researchers and threatening business executives involved in the sub-zero storage and transportation, needed by AstraZeneca, Moderna, Pfizer, and others to deliver vaccines in a worldwide spear-phishing campaign.
Ransomware [59]	Data, Money	December 03, 2020	Israel	The Israeli insurance firm Shirbit was attacked by the "Blackshadow" hacker group, seeking nearly $1 million in Bitcoin. After making their demands, the hackers released some confidential personal information and threatened to expose it more if they did not obtain payment.
Cyber Espionage [60]	Data theft	December 03, 2020	USA	Russian hackers who infiltrated the tech vendor "SolarWinds" and abused their access to track internal processes have violated several U. S. entities and private businesses.
Hacking [61]	Data theft	December 06, 2020	Israel	Iranian hackers got access to the data of more than 40 Israeli firms. The hackers obtained access to a logistics management software developer and used their links to steal data from customers.
Spear Phishing [62]	Data theft	December 23, 2020	Persian Gulf, European Union, and the USA	Iranian hacker group "Charming Kittens" launched a major Christmas-themed spear-phishing attack, targeting think tanks, research groups, scholars, journalists, and activists.
Vulnerability-exploitation [63]	Data theft	January 10, 2021	New-Zealand	Unidentified hackers infiltrated one of New Zealand's central bank's data centres.

Although, it was observed that during 2020, the attackers were laser-focussed on the money. For reference, between the first and second quarters of 2020, events involving payment and invoice frauds rose by 112%. If a phishing attack is successful, it can affect an organization in ways that are more than economical. Fig. 6 illustrates the side-effects of a successful phishing attack.

The Barracuda researchers found three types of phishing scams based on Covid-19 themes, viz. Business Email Compromise (BEC), brand impersonation, and scamming. In April 2020, 18 million covid-19 related compromise emails were received by Gmail daily [80]. Table 4 highlights the important details about phishing attacks launched in the times of the Covid-19 pandemic.

3.6. Effect of Covid-19 on Ransomware attacks

Ransomware restricts the access of users to their files, devices, or entire networks. The attackers ask their victims to pay a ransom

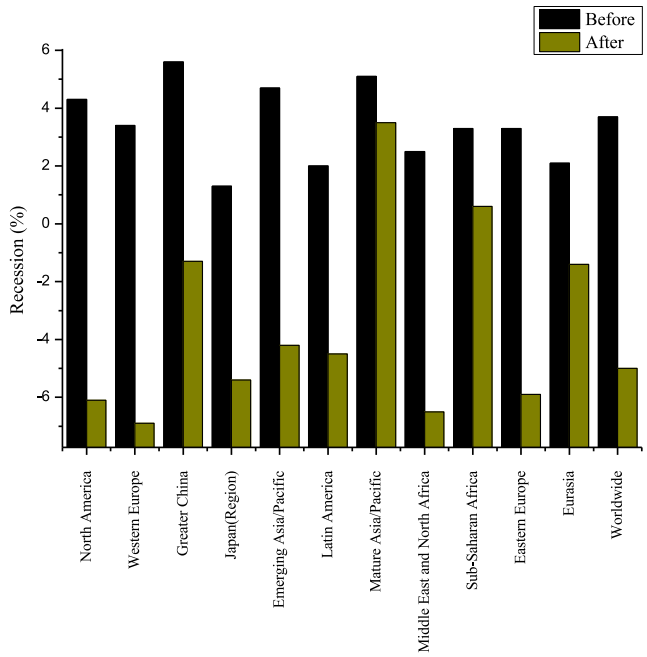

Fig. 2. Global Recession Scenario.

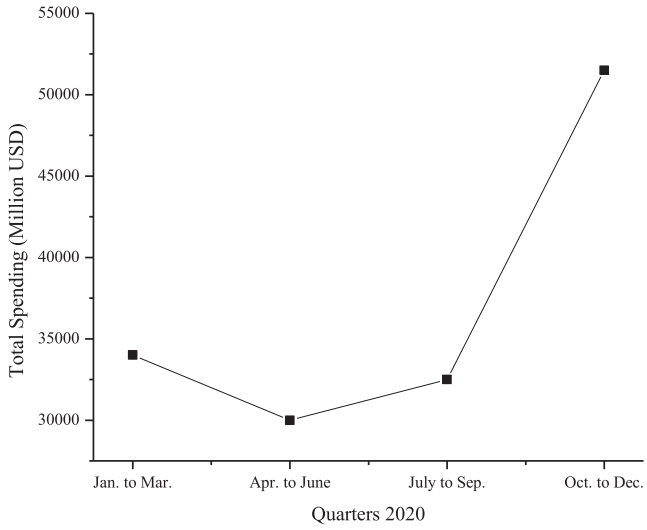

Fig. 3. Security Spending Forecast By Gartner.

to regain possession of their data. They also intimidate the victims of harsh consequences like auctioning their data, selling it on the dark-web, etc., if they fail to pay up. The COVID-19 pandemic has made industries like hospitals, colleges, government offices, etc., more scared of losing access to their systems and hence more motivated to pay the ransom [81,82]. The year 2020 created history as the first death was recorded because of a ransomware attack on German Dusseldorf university hospital [81]. The attack caused the patient to be re-routed to a hospital that was 30 Km away from the nearest Dusseldorf hospital. The hospital's internal servers were all locked up, and thus, they were unable to receive her.

Cybercriminals are completely exploiting the Covid-19 situation, which is evident by the 350 million USD lost on ransoms in year 2020 [83]. This displays a 311% rise in ransomware payments from the year 2019 [83]. Fig. 7 shows the top 5 countries impacted by ransomware attacks in the third quarter of the year 2020. The most affected industries were healthcare, education, retail, and Information Technology [84]. In the timeline of cyber-attacks, it is evident that ransomware attacks are on the rise during the pandemic.

4. Possible mitigation measures

Knowing and understanding cybercriminals' abilities is critical as we enter a new era marked by increasing attack sophistication and the threat of new catastrophic attacks. The following preventive actions and mitigation measures must be taken to detect a breach in your defences and stop the attacker in its tracks (Fig. 8).

- User awareness: To prevent any type of attack, it is crucial that users must be made aware of their vulnerabilities, and they must know how to identify trusted and legitimate sources. They must know what happens when certain permissions are given to third-party applications. At this time, users should avoid using public wi-fi spots, and at all times, people should take back-up of their critical data and never share their account details and other credentials via phone or email.
- Check outbound connections: We monitor what comes in (using firewalls, etc.) but neglect to do the same for outbound connections. When any malware infects a device, it must reconnect to its command-and-control centre in order to carry out the attack. If we are successful in preventing this connection, ransomware will be unable to gain traction in the first place. Hence, any questionable activity must be recorded and examined.
- Raise flags on scam calls and messages: To save innocent people from smishing and spam calls, VoIP service providers can help to enhance user awareness and reduce spam call/message threats by actively blocking possibly treacherous numbers.

The design and implementation of artificial intelligence-based anti-spam detectors is another viable mitigating approach (AI). We can construct an AI-based bot that can answer calls (instead of users) and evaluate if an incoming call is spam or not using data from past pandemics.

- Cross-border collaboration: During pandemics, such as the current COVID-19 outbreak, we require collaborative efforts from various countries and governments. To address cyber risks associated with pandemics, the international community must exert effort and take countermeasures, including the establishment of an international task force to facilitate the sharing of current cyber threat intelligence (e.g., attack vectors and methodologies).

To finance mitigation activities, the community and international organisations' support should be sought. For instance, financial assistance from organisations such as the International Monetary Fund (IMF) can be utilised to develop cyber threat mitigation techniques and expertise [16].

- Identify misleading news: We are living in a time when fake news spreads faster than wildfire. Identifying fake, ambiguous or partially accurate news can be a difficult job. The responsibility should be taken up in collaboration by the social, computer, and healthcare scientists to design techniques for identifying covid-19 related fake/misleading news.

Table 3
Impact of covid-19 on the growth of various security segments.

Security Segment	Near Term Effect on Growth(2020–2021)	Long Term Effect on Growth (2022–2023)
Firewalls	**Downward** growth.Existing capabilities will be improved.Network Security will be sweated.	**Downward** growth will continue.
AM	**No Effect.**Given AM's role in securing remote assets, it should be able to weather the effect of Covid-19.	**Increase.**Once the market enters the recovery phase, the growth drivers of AM will remain intact.
Cloud Security	**No Effect.**Large organizations will continue to buy these services and hence will dissipate the near effect of Covid.	Interest in cloud security will stay intense**;** enterprises of all sizes will make it the base of their projects.Overall growth will **Increase.**
Data Security	**No Effect.**Companies working with encrypted data, tokenization, digital rights management, etc., will weather the effect of Covid on the data security segment.	It will continue to rise ahead in the strongest position.**Increased** growth will be witnessed in this segment.
WAF	**No Effect.**Working from the home situation will demand WAF services.	**Increase.**Gartner believes that by 2023, almost 30% of web applications and APIs will be secured by cloud WAAP services, including WAF, services, protection from botnets, DDoS, etc.
SEG	**Downward** growth.Business Email Compromise (BEC) will pose a threat. Movement from email to cloud-based services will continue.	**No Effect.**The email will continue to be the best choice for phishing and BEC attacks.Vendors will grab this opportunity to sell their products.
VA	**Downward** growth.At this point, the VA market is mature. Newer technologies are being added to this, but their effect on the market will perhaps be seen in late 2021.	**Upward** growth.The interest in newer technologies will see a surge.The movement to cloud-based solutions will continue.
SIEM	**Downward** growth trend.The demand for SIEM projects was strong before Covid, but they take a long time to start up and run. As such, SIEM projects will be pushed back in the times of Covid because the projects that guarantee a quicker return on investment will be favoured.	**No Effect.**The inception of eXtended Detection and Response (XDR) products will pose a competition to the SIEM market by providing built-in automation along with alert-incident correlation.
PAM	**No Effect.**Remote working will require PAM services in place.	**Increase.**The emerging PAM technologies like behavioural analytics, privileged session monitoring, cloud privilege management, remote client access, etc., will be in high demand.
IRMS	**Downward** growth.Because of the market's economic pullback, this segment shall also see a pullback.	**Increase.**The growth will resume once the market recovers.
EPP	**No Effect.**Any device that wants remote access must be configured by EPP.	**Increase.**Resumption of growth will happen, and End-point Detection and Response (EDR) capability will be integrated with EPP.
IGA	**Downward** growth.IGA comes with a complicated installation process, labour costs, and heavy service investments (almost 150% of what has to be spent on software licenses, 3-year support, and maintenance).In the current world scenario where cash is the king, IGA project investments will be help-up.	**Increase.**Once businesses recover, the IGA penetration will see a rise.
AST	**Downward** growth.To cut the additional costs, most businesses will try to get their work done by using the already available application security testing tools.	**Increase.**The buyers will be forced to return to this market because heavier reliance will be put on online transactions.

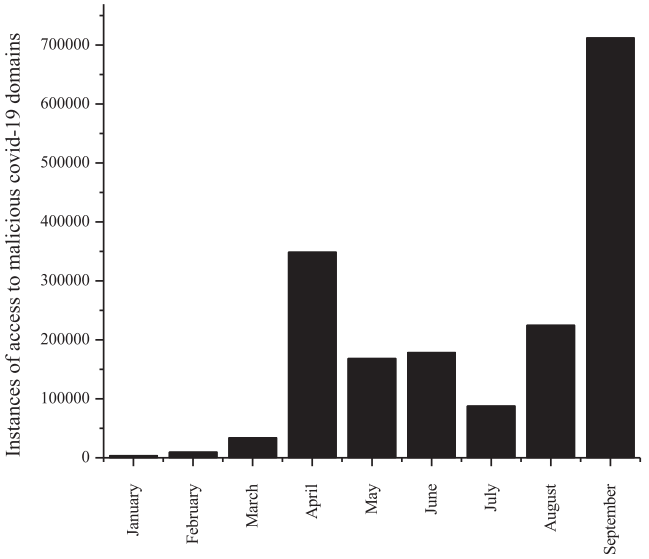

Fig. 4. Instances of access to malicious covid-19 domains for the year 2020.

- Constantly patch your network: It is always preferable to make it more difficult for an attacker to succeed by closing any vulnerabilities and misconfigurations that could be used to breach your network. Devices must be updated with the most recent security updates on a regular basis.
- Grave analysis of the network by professionals: If the data is extremely valuable, firms should have cybersecurity professionals do periodic scans of their networks. While the global pandemic and its widespread ripple effect can seem to be full of nothing but doom and gloom, a silver lining is that many positions in the cybersecurity sector will open up as a result. As IT quickly secures and scales its network to meet new demands, the teams are heavily taxed. For many companies, the move to work-from-home has involved repurposing their cybersecurity personnel to manage IT functions, and vice versa. At this point, there is a global shortage of 3.12 million cybersecurity professionals, according to (ISC) 2020 [85]; this workforce, therefore, needs to expand rapidly every year to meet the increasing demand for skilled staff and also to mitigate the potential threats.

According to a survey, 70% of attacks on companies were partly attributed to the cybersecurity skills shortage [86]. Clearly, there is a tremendous need for qualified cybersecurity specialists – perhaps the biggest that has ever been due to current circumstances. As the idea of remote work becomes a standard and infrastructures more widely spread, the need for IT professionals with timely security expertise and awareness will only increase.

Indeed, positions such as data scientists, cyber-savvy law enforcement agents, or threat hunters will grow in need. The Network Operations Center (NOC) and Security Operations Center (SOC) teams having to invert their networks to move the majority of end-users from operating inside the conventional perimeters to connecting from home offices now is also one of the main challenges. Network-wide exposure and power have been decreased,

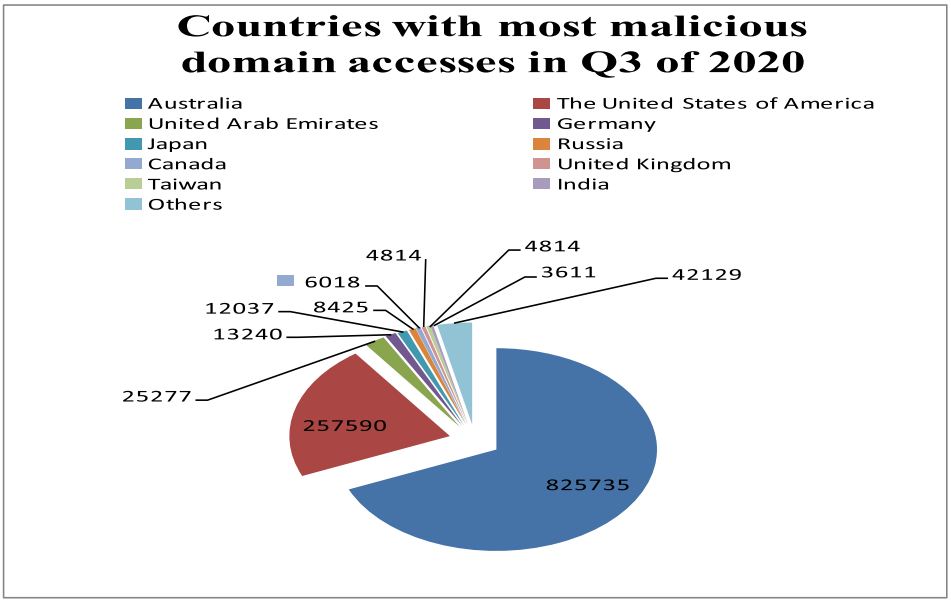

Fig. 5. Countries with the most malicious domain accesses in Q3 of 2020.

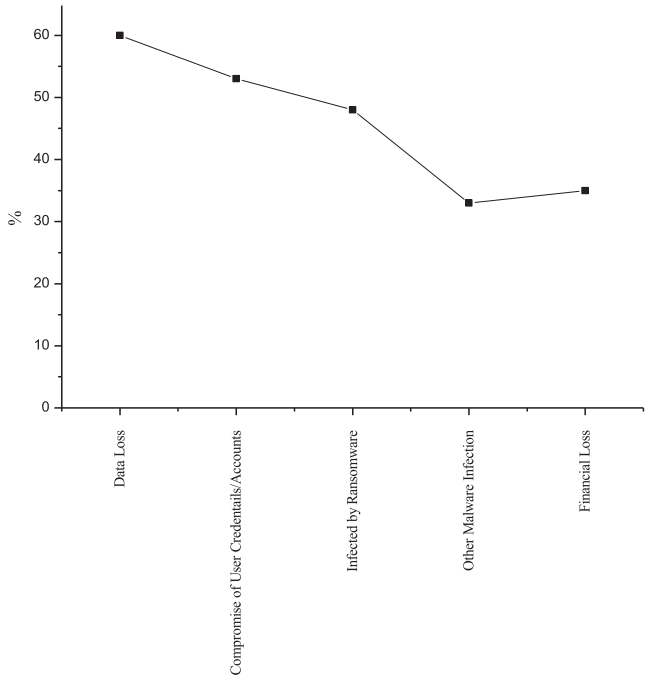

Fig. 6. Side-Effects of a Successful Phishing Attack.

exposing companies to threats that just a few months ago did not exist. Unfortunately, the expanded corporate network now incorporates notoriously unpatched and unprotected home networks. Understanding these complex patterns is important for security teams charged with detecting threats and properly protecting networks which only increases the need for filling the skill gap.

5. Materials and methods

5.1. Collection of dataset

Malicious data was obtained from the domains tools dataset, and legal data was obtained from WhoisDS (publicly available list). Domain tool data set has been used in earlier studies as it gives threat information about a new and existing domain. It rates domains in the range of 70–100, indicating an existing or approaching threat. We also collected legal domain names from WhoisDS between the periods of February 15, 2021, to February 27, 2021. We then sieved the dataset for keywords like "COV-19," "COVID-19," "Coronavirus," and "Carronavirus." It was found that approximately 25,000 COVID-19 related domains were requested in this period globally.

Once filtering was done, the domain names obtained from WhoisDS were matched with 1,54,292 malicious COVID-19 related entries present in the domain tools dataset. We considered any URL not present in both datasets as non-dangerous. 5173 such domains were obtained. A total of 6321 COVID-19 related malicious domains were identified. This input of 6321 malicious and 5173 legal domains was fed to the fuzzy logic and data mining-based intelligence engine, that is discussed in detail in the following subsection.

5.2. Covid-19 related attack detection intelligence architecture

In this subsection, we propose a fuzzy logic and data mining-based intelligence architecture that will help in detecting the malicious URL/ phishing attacks in the case that after taking all the necessary precautions, an attacker has gained access to your system and compromised the network or the device. It is to be noted here that although we designed the architecture to cover only malicious URL's and phishing attacks, we in no way claim that these are the only two threats in the time of Covid-19, but that they are on an extreme rise and there is a huge urgency to curb them.

To quantify and qualify any of the malicious COVID-19 related URLs, emails, and other malware, we propose the use of fuzzy logic. Fuzzy logic has been used in research for decades to integrate inputs into computer models for a various purposes. Boolean logic accepts input as true or false. Fuzzy logic is the logic of uncertain and imprecise reasoning [68]. Whenever, there is uncertainty and imprecision, precise logic cannot be used. In fuzzy logic, it is possible to describe partial membership in sets to calculate the result. The goal of fuzzy logic is to create a computational paradigm that is based on how humans think because in the real world, most classes of objects do not have clearly defined membership criteria.

Table 4
Phishing Attack Statistics under the Impact of Covid-19 [79,80]

Delivery Method used	Subject lines used in Q2-Q4 of 2020	Malicious attachments used in Q3-Q4 of 2020	Most Phished Industries in 2020	Most impersonated brands in Q2-Q4 of 2020
• Emails: 96% • Websites: 3% • Text messages (Smishing), and • Ttelephone calls (vishing): 1%	• Covid-19 in your area? Please confirm your address. • Coronavirus (ncov) safety measures. • Click here for Covi-19 vaccination details. • Twitter: Security alert: new or unusual Twitter login. • Fake cures for Covid-19. • Donate to these charitable organizations. • Amazon: Action Required | Your Amazon Prime Membership has been declined. • Zoom: Scheduled Meeting Error. • Google Pay: Payment sent. • High Risk: New confirmed cases in your area! • RingCentral is coming! • Workday: Reminder: Important Security Upgrade Required	• Windows executable files: 74% • Script files: 11% • Office files: 5% • Archive documents: 4% • PDF files: 2% • Java documents: 2% • Batch files: 2% • Shortcuts: greater than1% • Android executable files: greater than1%	• E-commerce • Health • Education • Business services • Manufacturing	• Microsoft (comprises 43% of all the brand phishing attempts) • DHL: 18% • LinkedIn: 6% • Rakuten: 4% • IKEA: 3% • Google: 2% • Paypal: 2% • Chase: 2% • Yahoo: 1%

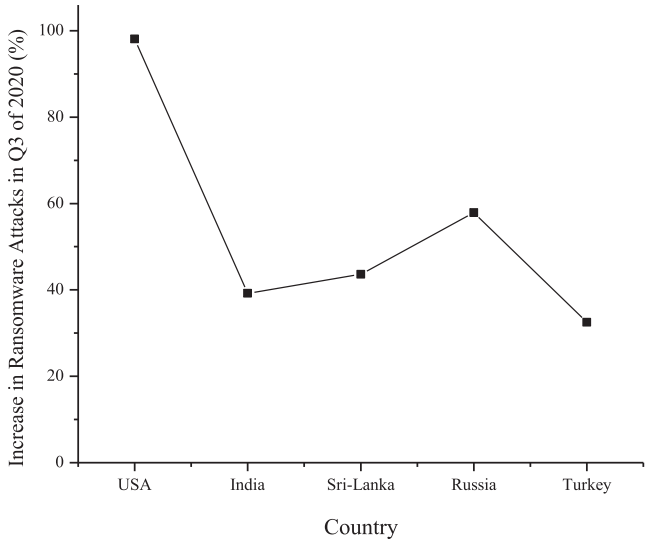

Fig. 7. Countries Affected the Most By Ransomware Attacks In Q3 Of 2020.

This translates to the idea that any attribute is intrinsically abstract. Tall, short, warm, and cold, for example, are all subjective terms, as one person's definition of these terms may be substantially different from another's. This implies that people interpret observations differently. To bridge the gap between the ambiguities of different understandings, fuzzy logic can be used.

We prefer to use the fuzzy logic approach as no distinctive boundaries exist between the legitimate and illegitimate classes in phishing URLs. The significance of fuzzy logic in phishing detection stems from the use of linguistic variables to point-out the possibility of a URL being malicious based on important phishing feature flags and linguistic variables to express phishing signs. The system is designed keeping in mind that false negatives should be very less as it is important to let the user obtain genuine COVID-19 related information from legitimate sites. The system should neither barge the user from a legal COVID-19 related site nor send important emails containing COVID-19 related keywords into spam.

Data mining is a technique for extracting implicit, previously undiscovered, and possibly beneficial information from big data sets. Data mining algorithms forecast patterns that can be used to identify phishing web pages. The proposed approach for detecting phishing and malicious domain attacks makes use of both fuzzy logic and data mining. Fig. 9 identifies the building blocks of a fuzzy logic-based rule system.

5.2.1. Intelligent fuzzy inference system components

The proposed intelligent fuzzy inference system is composed of three layers and six segments. The general framework of our system is given in Fig. 10. We have divided the features among 3 layers based on their type. For example, in the layer URL authenticity, we have verified the authenticity of the URL based on IP address, unusual URL request, unusual anchor, atypical DNS record and atypical URL. The study of these features helps in identifying an unusual URL, indicating unusual web browsing activity caused by initial access, persistence, C&C, or exfiltration. In a strategic web compromise, targeted users may receive emails with unusual URLs for trusted websites.

In layer 2, encryption and JavaScript and source code related features are analyzed. JavaScript has recently become the most popular attack construction language. By analyzing the combination of listed 5 features, most of the malicious JavaScript based attacks can be identified [68]. Similarly, an attack that attempts to manipulate or forge HTTP cookies is called cookie poisoning. Depending on the attack, cookie poisoning can lead to session hijacking, sensitive data exposure, or account takeover. In layer 2, one of the studied features is the unusual cookie. Likewise, the other features have been added to include every type of malicious intent.

In layer 3, we have studied the content and style of page, features of address bar and other human-social criteria. The features listed in these components are self-explanatory. For example, one of the chosen features is presence of symbols like '@'. If '@'is present in a URL, it ignores the string to the left. The right-side string is used to retrieve the page. As such, the URL in the address bar may look valid because of its limited space, but actually go to a different page. Similarly, a legitimate website doesn't contain hyphens, but an illegitimate one does. Also, an illegitimate website may contain more than one underscore and many dots. For Covid-related phishing/malicious URL attacks, we noticed the use of obfuscated covid-19 related keywords in the URL's, viz. covid, COVID, Corona, etc. Also, words like "Secure," "Confirm," "Vaccine," "Free," "Account" were frequently seen in covid-19 related phishing websites.

The proposed system has assigned weights to segments as concluded from various phishing experiments, data mining classification and associate rule mechanism, anti-phishing tools studies, phishing surveys, and quizzes. The phishing possibility is given by the equation:

Fig. 8. Possible Covid-19 related cyber-attack mitigation measures.

$\Upsilon_{phishing}$ = {0.3 × Crisp URL authenticity} Layer 1 + {(0.1 × crisp encryption) + (0.2 × crisp java script and source code)} Layer 2 + {(0.1 × crisp content and style of page) + (0.2 × crisp address bar) + (0.1 × crisp human social factor)} Layer 3.

5.2.1.1. Fuzzification. The framework mentioned here uses fuzzy logic modelling to determine the probability of website phishing based on 30 features that define a forged website. The features have been extracted from the most relevant state-of-art methods and help in the best understanding of the URL.

The primary advantage set by using fuzzy logic systems is use of linguistic labels to symbolize key factors. In the fuzzification stage, for each phishing characteristic indicator, Large, Small, and Average linguistic labels are consigned. The inputs' appropriate ranges are taken into account and distributed into fuzzy sets.

The length of a URL address, for example, will vary from 'small' to 'large,' with other values in between. We are unable to establish exact class boundaries. As shown in Fig. 11, every phishing indicator has linguistic values of Small (0–5), Average (3–7), and Large (5–10), while the Degree of phishing Attack (DOA) has linguistic values of Very Low (25–55), Medium (50–85), High (75–100). The triangular and trapezoidal membership functions are not probability values but grade-a subjective judgements. A triangular membership function is defined by a lower limit a, upper limit b and a value m where $a < m < b$, i.e.,

$$\mu_A(x) = \begin{cases} 0x \le a | x \ge b \\ \frac{x-a}{m-a} a < x \le m \\ \frac{b-x}{b-m} m < x < b \end{cases}$$

Here, $\mu_A(x)$ is a membership grade and not a probability value. It determines how much an element × in A is part of the fuzzy set. The value of all characteristic inputs' range from zero to ten, while the output values range from zero to hundred.

5.2.1.2. Development of fuzzy rule base. This stage generated fuzzy rules. When experts are constructing fuzzy logic models, they define fuzzy rules for use in the logic models. As a result, the mod-

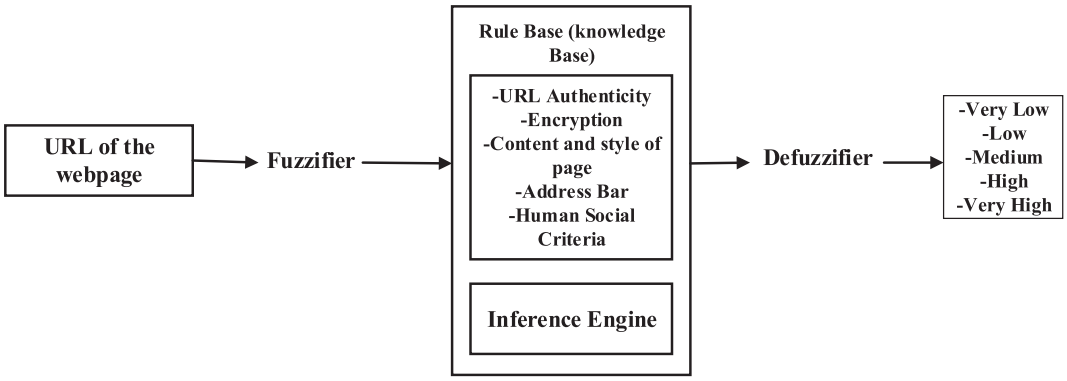

Fig. 9. Building blocks of fuzzy-logic based inference system.

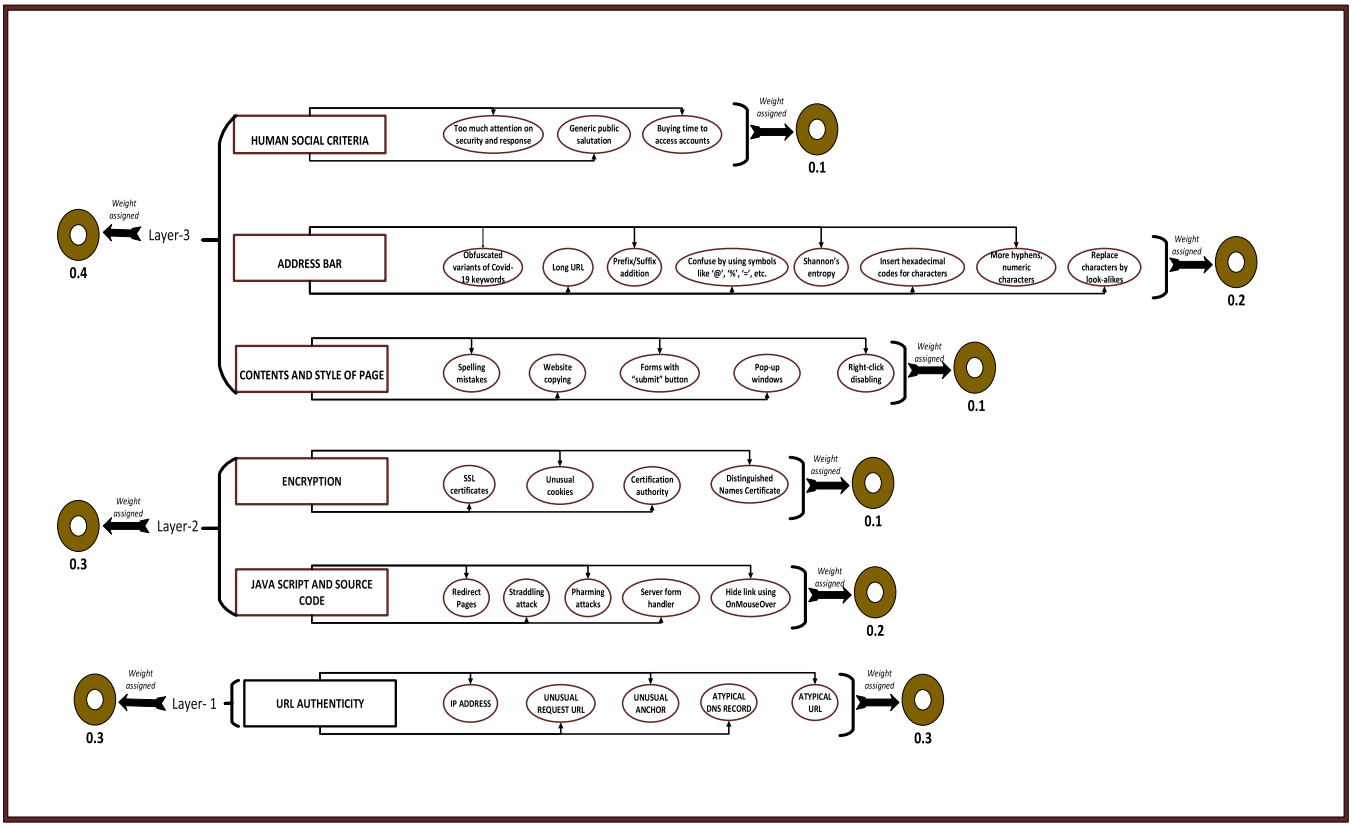

Fig. 10. Proposed Intelligent Fuzzy logic and data mining-based Inference System.

el's accuracy is dependent on their knowledge. A data mining classification-based strategy was employed to eliminate this problem and automate the rule development procedure. Phishing URLs and authentic URLs were utilised in this step. In total, 30 features were extracted for each of the URLs previously given. In order to define the fuzzy membership class, we used the fuzzy membership functions defined for each of these attributes individually. As soon as that was done, the data set was changed to a.arff version. This file was entered into WEKA, a data mining software program, for analysis. JRip, J48, and PART classification algorithms were used to develop the fuzzy rules.

Since there are five components for layer one segment, i.e., URL authenticity, fuzzy rule base (shown in Table 5), will contain a total of 3^5 entries. The consequent part of the rule speaks about the degree of attack and classifies it into three classes, viz. low, medium, and high. The fuzzy rule base for layer two containing two segments viz. encryption and JavaScript & source code and nine components, and layer 3 containing three components and sixteen components is given in Table 5.

5.2.1.3. Defuzzification. We fuse the results obtained from three layers into a final phishing possibility. Rule evaluation is defuzzified using Mamdani method [87]. An AND operator is used to combine these fuzzy rules. The disjunction operator is used when the firing of multiple rules (antecedents) result in the same result. The DoA value is computed by averaging the centroids of gravity of each member function. That is,

$$DOA = \sum_{x=a}^{b} \mu_A(x) \times x / \sum_{x=a}^{b} \mu_A(x)$$

The overall degree of phishing attacks is shown in Table 6. It contains 3^5 entries, and the degree of attack here is classified into five classes, viz. very low, low, medium, high, and very high.

5.2.1.4. Implementation of the model. The jFuzzyLogic library was used to create the fuzzy model. It is a free and open-source Java library that implements industry standards for the development of fuzzy systems. IEC 61131-part 7 Fuzzy control language (FCL) specification is implemented by jFuzzyLogic. Because FCL is designed as a "control language," the fundamental notion is a "control block" with some input and output variables.

First, the "FUNCTION" block is defined while constructing a fuzzy model. A second step is to define input and output variables. The Fuzzification of each input variable is defined in the "FUZZIFY" block. The linguistic terms are defined in each block. There are two parts to each term: a name and a membership function. Finally, output variables are dufuzzified to produce a "genuine" output number. Defuzzifiers have been defined in the "DEFUZZIFY" blocks. In every "DEFUZZIFY" block, linguistic terms were defined in the same way as those in "FUZZIFY" blocks. A Left-most-Maximum (LM) approach was utilized for defuzzification. The "RULE" block is the model's final part. Here, we have stored all the fuzzy rules.

To use the built phishing site detection methodology, a Chrome Web Browser Extension was created. When a user enters a URL, the developed model extracts the ten URL properties stated above and feeds those values into the developed phishing detection model. The fuzzy model will determine if the URL is a phishing URL or a real URL based on the extracted value. If the URL is valid, the Browser Plugin Icon will change green to show this. If the URL is flagged as phishing, the browser plugin icon will turn red to reflect this. In addition, a warning banner will be displayed in the browser. As a

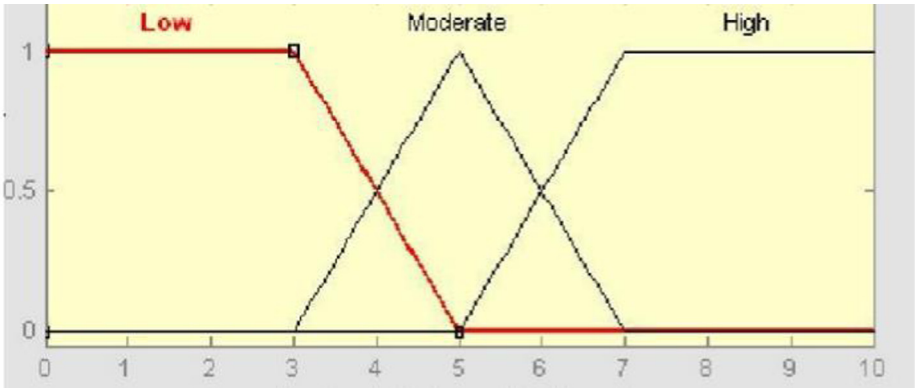

Fig. 11. Membership function μ for phishing indicators (long URL address).

Table 5
Fuzzy Rule Base.

Fuzzy Rule Base for Layer one segments	**Antecedent part of the rule**	**IP address**	Small	Small	Small	Average	Large	Small	Large	Small	Small	Small
		Unusual request URL	Small	Small	Small	Small	Average	Large	Average	Small	Small	Average
		Unusual Anchor	Small	Small	Small	Large	Small	Small	Large	Small	Average	Average
		Atypical DNS Record	Small	Small	Average	Average	Small	Small	Large	Average	Average	Small
		Atypical URL	Small	Average	Average	Large	Small	Average	Small	Large	Large	Large
	Consequent part of the rule	**Degree of Phishing Attack**	Low	Low	Medium	High	Medium	Medium	High	Medium	High	
Fuzzy rule base for layer two segments	**Antecedent part of the rule**	**Encryption**	Less	Less	Less	Medium	Medium	Medium	High	High	HighHigh	
		Java script and source code	Good	Doubtful	Malicious	Good	Doubtful	Malicious	Good	Doubtful	Malicious	
	Consequent part of the rule	**Degree of Phishing Attack**	Less	Less	High	Less	Medium	Medium	Medium	Medium	High	
Fuzzy rule base for layer three segments	**Antecedent part of the rule**	**Contents and style of page**	Good	Good	Good	Doubtful	Doubtful	Doubtful	Malicious	Malicious	Malicious	
		Address bar	Good	Doubtful	Malicious	Good	Doubtful	Malicious	Good	Doubtful	Malicious	
		Human Social Criteria	Good	Malicious	Malicious	Good	Doubtful	Doubtful	Good	Doubtful	Malicious	
	Consequent part of the rule	**Degree of Phishing Attack**	Less	Medium	High	Less	Medium	Medium	Less	Medium	High	

result, the user gets warned about the phishing site. The user can then be more cautious not to submit personal information such as usernames, passwords, credit card details, etc., information found on these websites. A browser extension is a group of files. It includes the files manifest.json, content.js, background.js, styles.css, and jquery-3.2.1.min.js. The manifest.json file contains the extension's primary information such as name, version, scripts, default icons, and so on. The web server calls the phishing detection programs in the content.js file, and the styles.css file contains the extension's fundamental styling.

The URL of the site is taken from the browser address bar in the chrome extension's content script. The data will then be sent to the web service. The URL characteristics will be collected from the web service. The feature is then supplied into the Phishing detection model. The model will determine whether the provided URL is a phishing URL or a legal URL. The result of the phishing detection model will then be returned to the web service, and the result of the web service will be returned to the web browser. The chrome extension will notify the user about the status of the URL based on the returned value. If the URL is real, the phishing indicator icon will become green; if the URL is phishing, the phishing indicator icon will turn red, and a warning banner will be displayed, as shown in Fig. 12.

6. Performance analysis

In this section, we have checked the applicability of our proposed system on COVID-19 related malicious URLs and phishing attempts. We used 5173 legal domains linked to COVID-19 (obtained from the WhoisDS dataset) and 6321 malicious COVID-19 related domains (extracted from the domain tools dataset). It must also be noted that Fuzzy logic-based techniques offer the advantage of being memory efficient and having a fast inference speed. However, implementation is more involved and complex than heuristic-based methods.

Table 6
Overall possibility of an attack.

Antecedent part of the rule			Consequent part of the rule
Layer 1	**Layer 2**	**Layer 3**	**Degree of Attack**
Good	Good	Good	Very low
Good	Good	Doubtful	Low
Good	Good	Malicious	Medium
Good	Doubtful	Good	Medium
Good	Doubtful	Doubtful	High
Good	Doubtful	Malicious	High
Good	Malicious	Good	Medium
Good	Malicious	Doubtful	High
Good	Malicious	Malicious	Very High
Doubtful	Good	Good	Low
Doubtful	Good	Doubtful	Medium
Doubtful	Good	Malicious	High
Doubtful	Doubtful	Good	Medium
Doubtful	Doubtful	Doubtful	Medium
Doubtful	Doubtful	Malicious	High
Doubtful	Malicious	Good	High
Doubtful	Malicious	Doubtful	High
Doubtful	Malicious	Malicious	Very High
Malicious	Good	Good	Medium
Malicious	Good	Doubtful	Medium
Malicious	Good	Malicious	High
Malicious	Doubtful	Good	Medium
Malicious	Doubtful	Doubtful	Medium
Malicious	Doubtful	Malicious	High
Malicious	Malicious	Good	High
Malicious	Malicious	Doubtful	Very High
Malicious	Malicious	Malicious	Very High

6.1. Fuzzy rule evaluation

The rules are evaluated using tenfold cross-validation. The dataset is separated into ten groups, with nine of the ten components utilized to train the classifier. The data acquired throughout the training phase is then used to test the tenth group. This is repeated ten times. Each of the groups would have been used as either training or testing data at the end of the training and testing phase. This strategy assures that the training and test data are distinct. Table 7 indicates the accuracy obtained for various classification algorithms using Weka tool.

6.2. Results

The parameters chosen for analyzing the performance of our system under the influence of malicious URL/phishing attacks are given in Table 8.

The working of the proposed system for some input sets is depicted in Table 9. It is seen from Table 9 that a doubtful website has a 50% degree of attack possibility when layer 1 gives a malicious flag for ten inputs and other layers give zero. Similar results were obtained when all the three layers gave doubtful (five) flags for the URL. From Table 9, we conclude that a heavy guarantee is given as the website being fishy when layers 1 and 2 give out average DOA and Layer 3 gives high (ten) DOA. Table 9 also indicates that even if one feature sees a website as fishy, it might still be legitimate and safe to use.

These results in Table 9 orchestrate that even when some of the characteristics of a URL are not blatantly wrong, it can still be fishy based on some other characteristics. For this reason, we chose not to use machine learning methods because the curse of dimensionality creeps in when one tries to use multiple features. The essence of the fuzzification process is that it gives the phishing possibility of URLs in the range of 14.2% to 87.3% instead in the full 1–100%

Table 7
Accuracy of classification algorithms.

Classification Algorithm	Accuracy Percentage
jRip	97.38
J48	97.56
PART	98.88

Table 8
Parameters for performance analysis.

Parameter	Definition	Calculation
True Positive Rate (TPR)/ Sensitivity/ Recall	No. of malicious URL's that system correctly detects as malicious.	$\frac{TP}{TP+FN} \times 100$
True Negative Rate (TNR)/ Specificity	No. of non-malicious URL's that system correctly detects as normal.	$\frac{TN}{TN+FP} \times 100$
False Positive Rate (FPR)	No. of legitimate URL's falsely detected as malicious.	$\frac{FP}{FP+TN} \times 100$
False Negative Rate (FNR)	No. of malicious URL's falsely detected as normal.	$\frac{FN}{FN+TP} \times 100$
Precision	No. of genuine records that were retrieved to the total number of genuine records.	$\frac{TP}{TP+FP} \times 100$
Detection Accuracy	Percentage of attacks detected by the system.	$\frac{TP+TN}{TP+TN+FP+FN} \times 100$

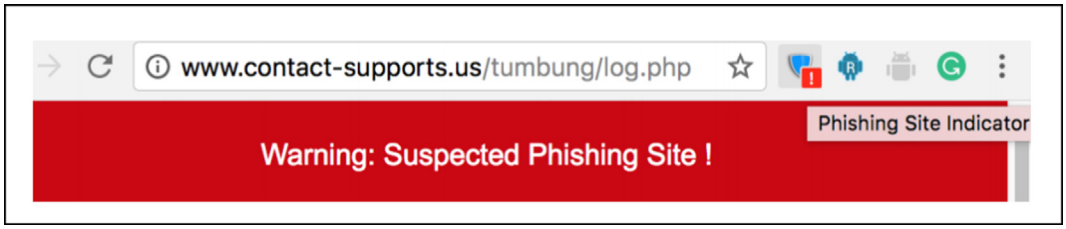

Fig. 12. Warning banner in chrome extension for phishing URLs.

Table 9
URL's possibility of phishing.

Maximum input (ten) for layer 1 and lowest (zero) for layers 2 and 3	Layer 1		Ten	Ten	Ten	Ten	Ten
	Layer 2	Encryption	Zero	Zero	Zero	Zero	Zero
		Java Script and Source Code	Zero	Zero	Zero	Zero	Zero
		Contents and Style of page	Zero	Zero	Zero	Zero	Zero
	Layer 3	Address bar	Zero	Zero	Zero	Zero	Zero
		Human social factor	Zero	Zero	Zero	Zero	Zero
	URL's possibility of phishing (%)		50%				
Average (Five) input for layer 1 & 2 and maximum (ten) input for layer 3	Layer 1		Five	Five	Five	Five	Five
	Layer 2	Encryption	Five	Five	Five	Five	Five
		Java Script and Source Code	Five	Five	Five	Five	Five
		Contents and Style of page	Ten	Ten	Ten	Ten	Ten
	Layer 3	Address bar	Ten	Ten	Ten	Ten	Ten
		Human social factor	Ten	Ten	Ten	Ten	Ten
	URL's possibility of phishing (%)		68%				
Average (five) input for layer 1 and zero input for layer 2 and 3	Layer 1		Five	Five	Five	Five	Five
	Layer 2	Encryption	Zero	Zero	Zero	Zero	Zero
		Java Script and Source Code	Zero	Zero	Zero	Zero	Zero
		Contents and Style of page	Zero	Zero	Zero	Zero	Zero
	Layer 3	Address bar	Zero	Zero	Zero	Zero	Zero
		Human social factor	Zero	Zero	Zero	Zero	Zero
	URL's possibility of phishing (%)		37%				

Table 10
Performance of our system.

Parameter	Performance in our system
True Positive Rate (TPR)/ Sensitivity/ Recall	5030 (97.23%)
True Negative Rate (TNR)/ Specificity	6257 (98.98%)
False Positive Rate (FPR)	64 (1.01%)
False Negative Rate (FNR)	143 (2.76%)
Precision	91.72%
Detection Accuracy	98.19%

range. For the 5173 legitimate sites and 6321 malicious sites, the overall results obtained are tabulated in Table 10. Moreover, the average time to identify if a URL was malicious or not was equal to 1017 ms.

In the case of phishing attacks related to COVID-19, the reduction of false positives and false negatives is as important as accuracy or true positives. Our system gives an overall detection accuracy is 98.19%, a False Positive Rate (FPR) of 1.01%, and from 6321 malicious COVID-19 related domains, it called 452 domains as Falsely Negative, i.e., it only gave a False Negative Rate of 2.76%. Therefore, it allows the users to obtain crucial covid-19 related information while at the same time blocking the phishing/-malicious ones.

6.3. Comparison with state-of-art

Figs. 13 and 14 compare the detection accuracies and recall of our system with various contemporaries, and it is observed that it gives far better results. It also has to be noted here that we could not find any work in the literature that took covid-19 related phishing attacks into consideration. Hence, the comparison has been made with less suitable state-of-art methods. The comparison has been drawn with URLNet [88], Texception [89], Triple Network [90], and Monte Carlo [91]. [91] is the most recent deep learning-based implementation. Our system has the advantage of using data mining and fuzzy logic combination that takes every factor into consideration.

7. Conclusion and future

The drastic shift to working remotely has created a tempting opportunity for scammers. Security teams have observed a large spike in cyber-attacks directly linked to this move. The ultimate

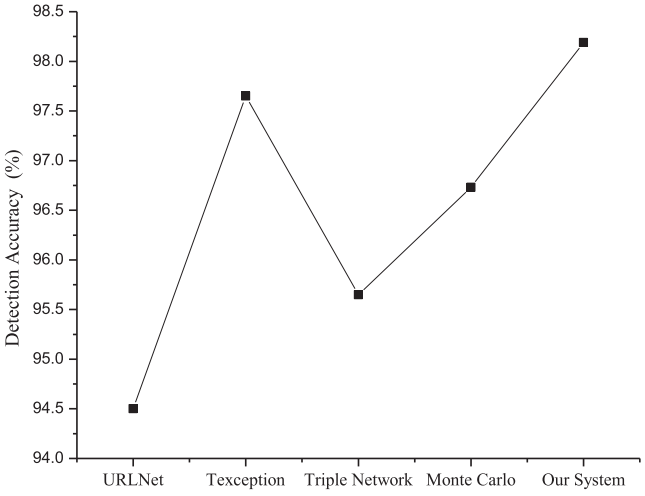

Fig. 13. Comparison of Detection Accuracies with State-of-art detection methods.

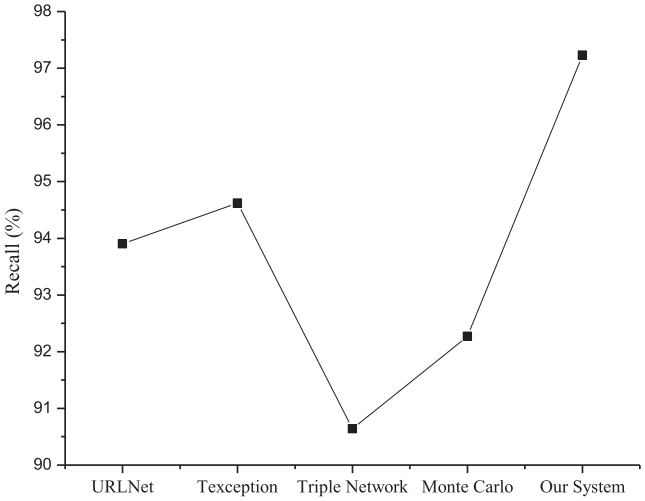

Fig. 14. Comparison of Recall with State-of-art detection methods.

opportunists that the cybercriminals are, instead of making the situation go to waste, capitalised on it with the resilience that companies wish they possessed. This paper highlights the effect of the Covid-19 pandemic on cyber security's spending, priorities, and other aspects. It also sketches out a timeline of Covid-19 related attack incidents from January 2020 to February 2021 to help security professionals understand the criminal psyche and their modus operandi. The paper proposes a well-defined set of mitigation strategies that could be taken up to stop the attack before it gains any traction. Moreover, to deal with the covid-19 related malicious/ phishing URL scams, a first of its kind fuzzy logic and data mining-based intelligence system was designed. With the three layers, six segments, and 30 components working in sync with each other, it is able to identify all the launched attacks with an accuracy of 98.19%. Evaluation results indicate the viability of our approach.

Unfortunately, Covid-19 has resulted in a significant increase in diverse cyber-attacks around the world. Cyber criminals have taken advantage of the current scenario and are targeting businesses, hospitals, pharmaceutical industries and manufacturing firms, as well as government agencies. A comprehensive examination of the cyber-attacks, their signatures and impacts, is the need of the hour. The immediate future scope is to identify more attacks that are taking advantage of the pandemic situation, and include them in our fuzzy logic and data mining-based intelligence system. Another future prospect would be to reduce false alarms even further. Also, our study found that a loose direct and inverse correlation exists between attacks and events. Additional investigation is required to examine this relationship to see whether a predictive model can be used to validate it. Cyber-attack case reports are plentiful worldwide, and further research will demonstrate that the issue is a real one.

Conflicts of Interest

The authors declare that they have no conflicts of interest

Acknowledgements

The work was partially supported by National Science Foundation grants \#1761735, \#1723586, and \#1663350. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the funding agencies.

References

[1] Melin, Patricia, et al. "Multiple ensemble neural network models with fuzzy response aggregation for predicting COVID-19 time series: the case of Mexico." *Healthcare*. Vol. 8. No. 2. Multidisciplinary Digital Publishing Institute, 2020.

[2] Sun T, Wang Y. Modeling COVID-19 epidemic in Heilongjiang province, China. Chaos, Solitons Fractals 2020;138:109949.

[3] Castillo O, Melin P. Forecasting of COVID-19 time series for countries in the world based on a hybrid approach combining the fractal dimension and fuzzy logic. Chaos, Solitons Fractals 2020;140:110242.

[4] Castillo, Oscar, and Patricia Melin. "A novel method for a covid-19 classification of countries based on an intelligent fuzzy fractal approach." *Healthcare*. Vol. 9. No. 2. Multidisciplinary Digital Publishing Institute, 2021.

[5] Melin P et al. Analysis of spatial spread relationships of coronavirus (COVID-19) pandemic in the world using self organizing maps. Chaos, Solitons Fractals 2020;138:109917.

[6] A. Bartik, M. Bertrand, Z. Cullen, E. Glaese, M. Luca, C. Stanton. *The impact of COVID-19 on small business outcomes and expectations*. [online]. Available: https://www.pnas.org/content/117/30/17656. Accessed: December 24, 2020.

[7] Melin P, Castillo O. Spatial and Temporal Spread of the COVID-19 Pandemic Using Self Organizing Neural Networks and a Fuzzy Fractal Approach. Sustainability 2021;13(15):8295.

[8] Threat Intelligence Team. *Cybercriminals impersonate World Health Organization to distribute fake coronavirus e-book*. [online]. Available:https://blog.malwarebytes.com/social-engineering/2020/03/cybercriminals-impersonate-world-health-organization-to-distribute-fake-coronavirus-e-book/. Accessed: December 20, 2020.

[9] Europol. *Pandemic Profiteering*. [online]. *Available:* https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis. Accessed: December 21, 2020.

[10] Allam, Zaheer, and David S. Jones. "On the coronavirus (COVID-19) outbreak and the smart city network: universal data sharing standards coupled with artificial intelligence (AI) to benefit urban health monitoring and management." *Healthcare*. Vol. 8. No. 1. Multidisciplinary Digital Publishing Institute, 2020.

[11] Nunes-Vaz R. Visualising the doubling time of COVID-19 allows comparison of the success of containment measures. Global Biosecurity 2020;1:3.

[12] Numan M et al. "A systematic review on clone node detection in static wireless sensor networks." *IEEE*. Access 2020;8:65450–61.

[13] Zahra SR, Chishti MA. Ransomware and internet of things: A new security nightmare. 2019 9th international conference on cloud computing, data science & engineering (confluence), 2019.

[14] Rafique W et al. Complementing IoT services through software defined networking and edge computing: A comprehensive survey. IEEE Commun Surv Tutorials 2020;22(3):1761–804.

[15] Khan WZ et al. Industrial internet of things: Recent advances, enabling technologies and open challenges. Comput Electr Eng 2020;81:106522.

[16] Cho, Hyunghoon, Daphne Ippolito, and Yun William Yu. "Contact tracing mobile apps for COVID-19: Privacy considerations and related trade-offs." *arXiv preprint arXiv:2003.11511* (2020).

[17] Carli De, Alessandro, et al. WeTrace–a privacy-preserving mobile COVID-19 tracing approach and application. arXiv preprint arXiv:2004.08812, 2020.

[18] Gupta P et al. Quest: Practical and oblivious mitigation strategies for COVID-19 using WiFi datasets. arXiv preprint arXiv:2005.02510, 2020.

[19] Yang Z et al. Modified SEIR and AI prediction of the epidemics trend of COVID-19 in China under public health interventions. Journal of thoracic disease 2020;12(3):165.

[20] Pirouz B et al. Investigating a serious challenge in the sustainable development process: analysis of confirmed cases of COVID-19 (new type of coronavirus) through a binary classification using artificial intelligence and regression analysis. Sustainability 2020;12(6):2427.

[21] Kumar A, Gupta PK, Srivastava A. A review of modern technologies for tackling COVID-19 pandemic. Diabetes & Metabolic Syndrome: Clinical Research & Reviews 2020;14(4):569–73.

[22] Hakak S et al. "Have you been a victim of COVID-19-related cyber incidents? Survey, taxonomy, and mitigation strategies. IEEE Access 2020;8:124134–44.

[23] Wynants, Laure, et al. "Prediction models for diagnosis and prognosis of covid-19: systematic review and critical appraisal." *bmj* 369 (2020).

[24] Javaid M et al. Industry 4.0 technologies and their applications in fighting COVID-19 pandemic. Diabetes & Metabolic Syndrome: Clinical Research & Reviews 2020;14(4):419–22.

[25] Khan NA, Brohi SN, Zaman N. "Ten deadly cyber security threats amid COVID-19 pandemic." TechRxiv. Preprint. 2020. , https://doi.org/10.36227/techrxiv.12278792.v1.

[26] Wang L, Alexander CA. "Cyber security during the COVID-19 pandemic. AIMS Electronics and Electrical Engineering 2021;5(2):146–57.

[27] Chigada J, Madzinga R. Cyberattacks and threats during COVID-19: A systematic literature review. South African Journal of Information Management 2021;23(1):1–11.

[28] Ferreira A, Cruz-Correia R. COVID-19 and cybersecurity: finally, an opportunity to disrupt? Jmirx med 2021;2(2):e21069.

[29] Ahmed J, Tushar Q. Covid-19 Pandemic: A New Era Of Cyber Security Threat And Holistic Approach To Overcome. 2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE), 2020.

[30] Tran C. Recommendations for ordinary users from mitigating phishing and cybercrime risks during COVID-19 pandemic. arXiv 2006;11929:2020, v1.

[31] S.Henderson, G. Roncone, S.Jones, J. Hultquist, B. Read. *Vietnamese Threat Actors APT32 Targeting Wuhan Government and Chinese Ministry of Emergency Management in Latest Example of COVID-19 Related Espionage*. Available: https://www.fireeye.com/blog/threat-research/2020/04/apt32-targeting-chinese-government-in-covid-19-related-espionage.html. Accessed: February 22, 2021.

[32] Aon. *Social Engineering Attacks And COVID-19*. Available: https://www.aon.com/cyber-solutions/thinking/social-engineering-attacks-and-covid-19/ Accessed: February 22, 2021.

[33] LaptrinhX. *Threat Intel | Cyber Attacks Leveraging the COVID-19/CoronaVirus Pandemic*. [online]. Available: https://laptrinhx.com/threat-intel-cyber-attacks-leveraging-the-covid-19-coronavirus-pandemic-2768112524/. Accessed: February 23, 2021.

[34] M. Vergelis. *Coronavirus phishing*. [online]. Available: https://www.kaspersky.com/blog/coronavirus-phishing/32395/. Accessed: February 23, 2021.

[35] S. Patranobis. *Indian hackers targeting Chinese medical institutes amid coronavirus outbreak, says report*. [online]. Available: https://www.hindustantimes.com/world-news/indian-hackers-targetting-chinese-medical-institutes-amid-coronavirus-outbreak-says-report/story-piDHQeY4UfTVy8BWa2GG3O.html. Accessed: February 24, 2021.

[36] N. A. Khan, S. N. Brohi, and N. Zaman. *Ten deadly cyber security threats amid COVID-19 pandemic*. [online]. Available: https://doi.org/10.36227/techrxiv.12278792.v1

[37] A. Pilkey. *Coronavirus email attacks evolving as outbreak spreads*. [online]. Available: https://blog.f-secure.com/coronavirus-email-attacks-evolving-as-outbreak-spreads/. Accessed: February 26, 2021.

[38] Lallie HS et al. Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers and Security 2021;105.

[39] A.Wolf. *The Top 5 Cyberattacks of May 2020.* [online]. Available: https://arcticwolf.com/resources/blog/top-5-cyberattacks-of-may-2020. Accessed: February 11, 2021.

[40] A.Wolf. *The Top 5 Cyberattacks of May 2020.* [online]. Available: https://arcticwolf.com/resources/blog/top-5-cyberattacks-of-june-2020. Accessed: February 13, 2021.

[41] L.Irwin. *Cyber attacks and data breaches in review: July 2020.* [online]. Available: https://www.itgovernance.eu/blog/en/cyber-attacks-and-data-breaches-in-review-july-2020. Accessed: February 17, 2021.

[42] A.Wolf. *The Top 5 Cyberattacks of August 2020.* [online]. Available: https://arcticwolf.com/resources/blog/top-cyberattacks-of-august-2020. Accessed: February 19, 2021.

[43] M. Heinemeyer. *Ransomware-as-a-Service: Eking targets government organization.* [online]. Available: https://www.darktrace.com/en/blog/ransomware-as-a-service-eking-targets-government-organization/. Accessed: February 21, 2021.

[44] A. Bizga. *Pakistan's Largest Power Supplier Hit by Netwalker Ransomware.* [online]. Available: https://hotforsecurity.bitdefender.com/blog/pakistans-largest-power-supplier-hit-by-netwalker-ransomware-24105.html. Accessed: February 22, 2021.

[45] A.Kharpal. *Russian hackers target Nato, military secrets.* [online]. Available: https://www.cnbc.com/2014/10/28/russian-hackers-target-nato-military-secrets.html. Accessed: February 23, 2021.

[46] Resilience360.Ransomware attack on french carrier CMA CGM disrupts shipping operations. [online]. Available: https://www.resilience360.dhl.com/news/ransomware-attack-on-french-carrier-cma-cgm-disrupts-shipping-operations/. Accessed: February 25, 2021.

[47] S.Vavra. *DOD, DHS expose hacking campaign in Russia, Ukraine, India, Malaysia.* [online]. Available: https://www.cyberscoop.com/dod-dhs-cyber-command-cisa-hacking-russia-ukraine-india-malaysia/. Accessed: February 27, 2021.

[48] Wion. *Greek hackers bring down over 150 Azerbaijani government websites as sign of support for Armenia.* [online]. Available: https://www.wionews.com/world/greek-hackers-bring-down-over-150-azerbaijani-government-websites-as-sign-of-support-for-armenia-332409. Accessed: February 27, 2021.

[49] C. Cimpanu. *Chinese hacker group spotted using a UEFI bootkit in the wild.* [online]. Available: https://www.zdnet.com/article/chinese-hacker-group-spotted-using-a-uefi-bootkit-in-the-wild/. Accessed: February 28, 2021.

[50] S.Lyngaas. *Spies hacked Azerbaijan government officials as Nagorno-Karabakh conflict escalated, researchers say*. [online]. Available: https://www.cyberscoop.com/nagorno-karabakh-azerbaijan-armenia-espionage-talos-hackers/. Accessed: February 28, 2021.

[51] S. Lyngaas. *'MuddyWater' spies suspected in attacks against Middle East governments, telecoms.* [online]. Available: https://www.cyberscoop.com/muddywater-iran-symantec-middle-east/. Accessed: February 28, 2021.

[52] A.Asokan. *Iranian Hacking Group Again Targets Universities.* [online]. Available: https://www.bankinfosecurity.com/iranian-hacking-group-again-targets-universities-a-15182. Accessed: March 01, 2021.

[53] S. Vavra. *Vietnamese hacking group OceanLotus uses imitation news sites to spread malware.* [online]. Available: https://www.cyberscoop.com/vietnam-hacking-oceanlotus-apt32-fake-news/. Accessed: February 16, 2021.

[54] Z. Whittaker. *Microsoft says hackers backed by Russia and North Korea targeted COVID-19 vaccine makers.* [online]. Available: https://techcrunch.com/2020/11/13/microsoft-russia-north-korea-hackers-coronavirus-vaccine/. Accessed: February 18, 2021.

[55] C. Cimpanu. *BlackBerry discovers new hacker-for-hire mercenary group.* Available: https://www.zdnet.com/article/blackberry-discovers-new-costaricto-hacker-for-hire-group/. Accessed: February 19, 2021.

[56] J. Stubbs. *Suspected North Korean hackers targeted COVID vaccine maker AstraZeneca.* [online]. Available: https://www.reuters.com/article/us-healthcare-coronavirus-astrazeneca-no-idUSKBN2871A2. Accessed: February 19, 2021.

[57] A. Hope. *DoppelPaymer Ransomware Attack Disrupts Foxconn's Operations in the Americas, Hackers Delete Terabytes of Data, Demand $34 Million.* [online]. Available: https://www.cpomagazine.com/cyber-security/doppelpaymer-ransomware-attack-disrupts-foxconns-operations-in-the-americas-hackers-delete-terabytes-of-data-demand-34-million/. Accessed: February 20, 2021.

[58] M. Miliard. *Hackers taking aim at crucial COVID-19 vaccine 'cold chain,' says IBM.* [online]. Available: https://www.healthcareitnews.com/news/hackers-taking-aim-crucial-covid-19-vaccine-cold-chain-says-ibm. Accessed: February 20, 2021.

[59] T. Joffri. *Shirbit hackers demand almost $1 million in ransom money to stop leaks.* [online]. Available: https://www.jpost.com/israel-news/shirbit-hackers-demand-almost-1-million-in-ransom-money-to-stop-leaks-650995. Accessed: February 22, 2021.

[60] The New York Times. *Scope of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit.* [online]. Available: https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html. Accessed: February 23, 2021.

[61] S. Winer. *Cyberattack hits Israeli companies, with Iran reportedly the likely culprit.* Available: https://www.timesofisrael.com/israels-supply-chain-targeted-in-massive-cyberattack/. Accessed: February 24, 2021.

[62] C. Cimpanu. *Iranian cyberspies behind major Christmas SMS spear-phishing campaign.* [online]. Available: https://www.zdnet.com/article/iranian-cyberspies-behind-major-christmas-sms-spear-phishing-campaign/. Accessed: February 25, 2021.

[63] NBC news. *New Zealand central bank says data system hacked, sensitive information potentially accessed*. [online]. Available: https://www.nbcnews.com/news/weird-news/new-zealand-central-bank-says-data-system-hacked-sensitive-information-n1253652. Accessed: February 25, 2021.

[64] V. Anant, J. Caso, and A. Schwarz. *COVID-19 crisis shifts cybersecurity priorities and budgets.* [online]. Available: https://www.mckinsey.com/business-functions/risk/our-insights/covid-19-crisis-shifts-cybersecurity-priorities-and-budgets#. Accessed: December 22, 2020.

[65] M. Solomon. *Emerging Threats During Times of Crisis: Insights from Airbus Cybersecurity's Phil Jones.* [online]. Available: https://www.securityweek.com/emerging-threats-during-times-crisis-insights-airbus-cybersecuritys-phil-jones. Accessed: December 21, 2020.

[66] Helpnetsecurity. *The COVID-19 pandemic and its impact on cybersecurity.* [online]. Available: Available: https://www.helpnetsecurity.com/2020/08/03/pandemic-impact-cybersecurity/. Accessed: December 24, 2020.

[67] S. Quadros. *RDP Attacks on the Rise During COVID-19 Pandemic.* [online]. Available: https://securityboulevard.com/2021/01/rdp-attacks-on-the-rise-during-covid-19-pandemic/. Accessed: January 9, 2021.

[68] Zahra SR, Chishti MA. Fuzzy logic and fog based secure architecture for internet of things (FLFSIoT). J Ambient Intell Hum Comput 2020:1–25.

[69] The World Bank. *COVID-19 to Plunge Global Economy into Worst Recession since World War II.* [online]. Available: https://www.worldbank.org/en/news/press-release/2020/06/08/covid-19-to-plunge-global-economy-into-worst-recession-since-world-war-ii. Accessed: January 10, 2021.

[70] N. M. Fuentes, I. Moder. *The scarring effects of COVID-19 on the global economy.* [online]. Available: https://voxeu.org/article/scarring-effects-covid-19-global-economy. Accessed: February 8, 2021.

[71] Worldometer. *Coronavirus Death Toll.* [online]. Avaialble: https://www.worldometers.info/coronavirus/coronavirus-death-toll/ Accessed: April 18, 2021.

[72] Checkpoint. *Coronavirus-themed domains 50% more likely to be malicious than other domains.* [online]. Available: https://blog.checkpoint.com/2020/03/05/update-coronavirus-themed-domains-50-more-likely-to-be-malicious-than-other-domains/. Accessed: December 29, 2020.

[73] TrendMicro. *Developing Story: COVID-19 Used in Malicious Campaigns.* [online]. Available: https://www.trendmicro.com/vinfo/in/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains. Accessed: December 31, 2020.

[74] The Economic Times. *COVID-19-related phishing attacks up by 667%.*[online]. Available: https://ciso.economictimes.indiatimes.com/news/covid-19-related-phishing-attacks-up-by-667-report/74839322. Accessed: January 01, 2021.

[75] L. Whitney. *How a successful phishing attack can hurt your organization.* [online]. Available: https://www.techrepublic.com/article/how-a-successful-phishing-attack-can-hurt-your-organization/. Accessed: February 11, 2021.

[76] K. Mathai. *How fear of pandemic became fodder for phishing attacks.* [online]. Available: https://timesofindia.indiatimes.com/india/how-fear-of-covid-pandemic-became-fodder-for-phishing-attacks/articleshow/76810580.cms. Accessed: February 01, 2021.

[77] Pranggono B, Arabo A. COVID-19 pandemic cybersecurity issues. Internet Technology Letters 2020.

[78] M. Rosenthal. *Must-Know Phishing Statistics: Updated 2021.* Available: https://www.tessian.com/blog/phishing-statistics-2020/. Accessed: February 11, 2021.

[79] D. Warburton. *2020 Phishing and Fraud Report.* [online]. Available: https://www.f5.com/labs/articles/threat-intelligence/2020-phishing-and-fraud-report. Accessed: January 15, 2021.

[80] J. Arghire. *Google Sees Increase in COVID-19 Phishing in Brazil, India, UK.* [online]. Available: https://www.securityweek.com/google-sees-increase-covid-19-phishing-brazil-india-uk. Accessed: January 18, 2021.

[81] C. Cimpanu. *First death reported following a ransomware attack on a German hospital.* [online].Available: https://www.zdnet.com/article/first-death-reported-following-a-ransomware-attack-on-a-german-hospital/. Accessed: January 25, 2021.

[82] J. Firch. *10 Cyber Security Trends You Can't Ignore In 2021.* [online]. Available: https://purplesec.us/cyber-security-trends-2021/. Accessed January 19, 2021.

[83] C. Cimpanu. *Ransomware gangs made at least $350 million in 2020.* [online]. Available: https://www.zdnet.com/article/ransomware-gangs-made-at-least-350-million-in-2020/. Accessed: February 05, 2021.

[84] Cisomag. *Ransomware Attacks in 2020! These are 4 Most Affected Sectors.* [online]. Available: https://cisomag.eccouncil.org/ransomware-attacks-in-2020-these-are-4-most-affected-sectors/. Accessed: February 16, 2021.

[85] Global Security Mag. *Global cybersecurity industry faces a workforce gap of 3.12 million in 2020.* [online]. Available: https://www.globalsecuritymag.com/Global-cybersecurity-industry,20201215,106241.html. Accessed: March 02, 2021.

[86] McAfee. *Hacking the skills shortage.* [online]. Available: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf. Accessed: March 02, 2021.

[87] M. Liu, D. Chen and C. Wu. "The continuity of Mamdani method," International Conference on Machine Learning and Cybernetics,Page(s): 1680 - 1682 vol.3, 2002.

[88] Le, Hung, et al. "URLNet: Learning a URL representation with deep learning for malicious URL detection." *arXiv preprint arXiv:1802.03162* (2018).
[89] Tajaddodianfar F, Stokes JW, Gururajan A. Texception: A character/word-level deep learning model for phishing URL detection. ICASSP 2020–2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2020.
[90] Bu S-J, Cho S-B. Integrating Deep Learning with First-Order Logic Programmed Constraints for Zero-Day Phishing Attack Detection. ICASSP 2021–2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2021.
[91] Novoselov S et al. Triplet Loss Based Cosine Similarity Metric Learning for Text-independent Speaker Recognition. Interspeech. 2018.