Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2021.015845
Article

Impact of COVID-19 Pandemic: A Cybersecurity Perspective

Mohammed Baz[1], Hosam Alhakami[2], Alka Agrawal[3], Abdullah Baz[4] and Raees Ahmad Khan[3,*]

[1]Department of Computer Engineering, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif, 21944, Saudi Arabia
[2]Department of Computer Science, College of Computer and Information Systems, Umm Al-Qura University, Makkah, 21955, Saudi Arabia
[3]Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow, 226025, Uttar Pradesh, India
[4]Department of Computer Engineering, College of Computer and Information Systems, Umm Al-Qura University, Makkah, 21955, Saudi Arabia
[*]Corresponding Author: Raees Ahmad Khan. Email: khanraees@yahoo.com
Received: 20 November 2020; Accepted: 25 December 2020

Abstract: Inspite of the world being at a complete standstill in the wake of unprecedented health emergency of COVID-19 pandemic, people have managed to retain their digital interactions through Information Technology. Cloud networks, departmental servers, data centres, and the digital devices have ensured that businesses and industries as well as workers across the world remain associated with each other and are connected to the organizations' data. In such a scenario, the requirements placed on digital frames have increased rapidly. While this has proved to be a boon in the combat against the spread of Coronavirus, alarming increase in the instances of cyber attacks has become a major bane today. To prevent an emergence of second crisis, cybersecurity needs to be upgraded to protect the data of the users and contain the rising cyber crimes. This upgradation will be done when the impact of COVID-19 on security will be estimated. Hence this research is an attempt to gauge and analyse the impact of COVID-19 pandemic on cybersecurity. Various aspects of cybersecurity that have been affected by the pandemic have then been ranked in the descending order of severity quantitatively by the help of multi-criteria decision-making problem solving technique. Such a thorough and conclusive analysis will add to the experts' efforts in estimating the extent of the effects of COVID-19 on cybersecurity. The findings of this study will be an effective reference for designing, developing and implementing more secure mechanisms to protect the users from cyber invasions.

Keywords: Cyber security; impact of COVID-19 pandemic; decision making problems

1 Introduction

The unprecedented humanitarian crisis, COVID-19 pandemic has mobilised the people across the world in utilising the most modern approaches from data science to artificial intelligence to connect and communicate with each other [1]. In just a single month, the world became even more virtually linked and fragile than ever before. In March, the internet was suddenly used by organisations to facilitate

remote communication between the large groups of home-based workplaces that had previously needed staff to meet at a common physical location. Furthermore, home-based financial institutions' staff has a regulatory need to ensure that all communications and transactions are done on a private and highly secure infrastructure [2]. In order to preserve the supply chain for essentials, businesses also rely on digital services.

This pandemic has thus started a new trend for everyone to work from home. All of this is due to the connectivity to data, computer systems and their applications. To reassure the public and maintain order, officials rely on digital channels. They communicate rules that evolve rapidly, share critical information on mental condition, and expose the onslaught of rumours, misinformation and fraud about fake remedies. Digital networks are being used in almost all spheres of human activity nowadays. However, the ubiquitous use of virtual channels has unintentionally been the cause of rise in cyber crime. Cybercriminals have become hyperactive in the present scenario and are constantly preying upon the personal data of both the individual users and the organisations. To avoid a second crisis from arising, cybersecurity efforts need to be upgraded so as to protect the digital networks and devices [3].

Networks and devices have become infinitely more critical for organizations in the recent weeks [4]. Most of these organisations, however, were not equipped with the IT mechanisms to enable their employees to work from home. A major constraint in this league was the secure access to systems, and a secure remote access capacity. Finally, the impact of the COVID-19 pandemic is not negligible in the era of software-based applications. To achieve a thorough understanding of how much this pandemic has affected software-based applications and their security, this impact should be analysed and computed. This paper brings an approach to the same thing. The impact of COVID-19 on software systems and their industry have been identified and further classified to highlight the software systems and their applications that have been severely affected [5].

Furthermore, this paper uses a decision-making problem solving based hybrid approach of fuzzy sets theory and analytic hierarchy process for conducting a quantitative evaluation of the impact of the pandemic. Fuzzy sets are used in mathematical terms to represent imprecision and vagueness of the linguistic data. Multi-criteria decision-making approaches have important implications when used on fuzzy sets. As the pairwise comparisons between parameters are not based on measurable significance, decision-makers tend to assign intervals for the assessment of requirements in certain decision-making parameters. The benefit of fuzzy analytic hierarchy process over conventional fuzzy function is that by using pairwise comparisons and constant fuzzy sets, it fits the parameter, and measures the parameters' weights.

The remainder of the manuscript is structured as follows: Section 2 addresses the cyber risks during COVID-19 pandemic. Section 3 presents the impacts of COVID-19 pandemic on cyber security. Section 4 discusses the methodology, briefly. The quantitative results are evaluated in Section 5. Section 6 deliberates upon the recommendations for practitioners. Finally, Section 7 presents the conclusion.

2 An Explosion of Cyber Risks in the Pandemic of COVID-19

The growing dependency on digital communication and the comprehensive modification to run enterprises online due to COVID-19 pandemic has unfortunately led to a significant increase in the risk of cyber-attacks. Cyber attackers have also launched a significant variety of possible hazards [6]. The perimeter security of organisations is at the risk of being violated. Organizations need continuous supervision and real-time risk assessment for breaches at both physical and digital entry points. Security risk management practitioners have to secure their organisations on a large scale, and rapidly. They must ensure that their enterprises' web services and digital networks are resilient to cyberattacks and hacking.

The information technology market is already reeling under enormous burden. In certain industries, practitioners of information technology need to expand remote working capability to include workers

who have not worked from home in the past. This includes their service partners, in some situations. In addition, most of the departments of information technology are in the midst of deploying new kinds of collaboration applications. While this mechanism is important for keeping the workers synchronised (particularly those employed in agile team members), such applications increase the hacking risk of sensitive data that currently exists in less secure remote based offices.

In order to be able to execute operations remotely, business executives, administrators and their employees need access to applications and internal resources. Since these applications and data have not historically been made available by most of the organisations over the virtual private networks or internet, practitioners are hesitant to permit access without strict access mechanisms [7]. Consequently, very few organizations are able to function remotely with their workforce on a mass basis.

It is a hard job to implement organization's security guidelines and controls on the team members, remotely. Most of the security controls have limited scalability and take considerable time to deploy. There are several organisations that permit their workers to use corporate applications without any tool or technique for controlling security by using their personal digital devices. Organizations' working continuity and incident response plans in perspective of industry are insufficient or even non-existent for managing a pandemic like COVID-19. An organizations' working continuity on such a scale was never expected or checked by cybersecurity officials.

It is well known to fraudsters that numerous businesses and their team workers have unbolted the door to hacking. The increased digital traffic and footprints are used by cybercriminals to find vulnerabilities, or to siphon-off capital. In the form of phishing emails with malicious attachments, the cybercriminals launch COVID-19 theme based attacks that drop malware to disable networks or steal data and credentials. In order to host malicious code, attackers build temporary websites or take over the compromised ones. They attract people to these websites and then drop their digital devices with malicious code.

For daily wage earners, fake web pages have also been soliciting donations with the help of email links. Viruses and identity theft malware are laden with certain links of COVID-19 patients' computational status applications. Remote working platforms have been hacked for vulnerabilities, such as video conferencing systems; recent Zoom examples in this context are a troubling norm. Cybersecurity practitioners must actively confront the threats of this modern setting. For instance, they need to make the remote employees of their organisations aware of scams quickly, and then teach them how to not fall prey to them.

The adoption of technology and resolutions that are efficient and easy to implement, for example cloud hosts, will be an important part of the success of security initiatives [8]. Security and platform services focused on the cloud markedly reduce the implementation time. They also allow organizations, depending on the threats of the moment, to rapidly enhance the scope and the range of security mechanism. With the help of remote monitoring system, security practitioners control the cloud-based security mechanism for protecting systems. In addition, controlled detection and response services focused on the cloud can be applied to remote accessible offices.

3 COVID-19 Pandemic Impacts on Cyber Security

COVID-19 pandemic has been the news all around the world for the past few weeks. The medical fraternity as well as the government and citizens across the world are collating their efforts to contain the spread of this contagion. However, even as healthcare services reinforce their resources to combat the COVID-19 emergency, they have become the victims of cyber-attacks [4–6]. In this context, the United States Department of Homeland Security (DHS), the United Kingdom's National Cyber Security Centre (NCSC) and Cybersecurity & Infrastructure Security Agency (CISA) released a joint advisory on 8 April 2020, detailing how the COVID-19 pandemic was being exploited by cybercriminals and Advanced Persistent Threat (APT) organisations [7].

This advisory tackled concerns such as the compromise between phishing, malware and communication networks (e.g., Zoom, Microsoft Teams). By designing and implementing new economic policies, policymakers are reconsidering ways to ensure that their countries are prosperous. Nevertheless, as the world focuses on the health and economic challenges presented by COVID-19, this crisis is inevitably being capitalised on by cybercriminals around the world [8]. In this paper, the authors attempt to examine the impact of various scenarios due to the COVID-19 pandemic. The adverse effects of the pandemic on the software industry have been summarized in Fig. 1 and description of each impact is termed as follows:

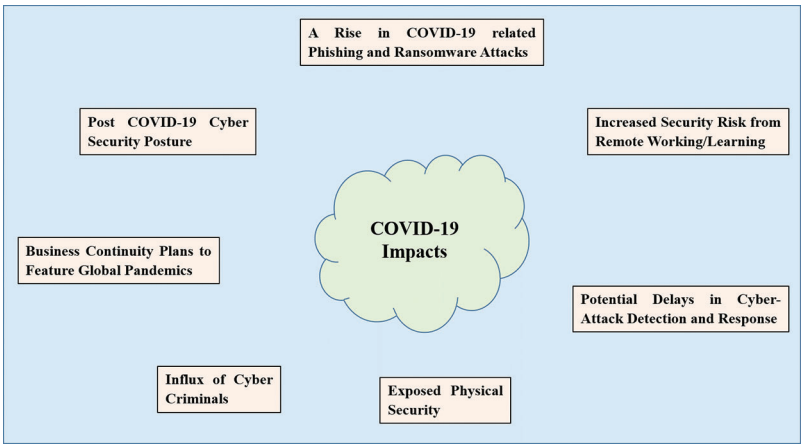

Figure 1: Different cyber security issues

3.1 Impact-1: A Rise in COVID 19 Related Phishing and Ransomware Attacks

Authors also noticed an increase in phishing attacks, malspams and ransomware attacks from a study released by [4] the Cyber Intelligence Centre. The study cites that the attackers use COVID-19 as a lure to impersonate brands and thereby deceive employees and customers. More contaminated personal computers and phones are likely to result from this. Not only are organisations threatened, but the end users who download applications related to COVID-19 are often fooled into installing ransomware disguised as legitimate applications. Organizations should take preventive measures by advising their employees and customers to be more attentive and careful, especially while perusing COVID-19 related links, emails or documents. Organizations should ensure the functionality of their identification and warning capabilities while keeping an eye on the impact of having several remote employees.

3.2 Impact-2: Increased Security Risk from Remote Working/Learning

Company Virtual Private Network (VPN) servers have now become a lifeline for businesses/schools with many workers working from home and students' virtually learning, and their security and availability will be a big focus in the future [5]. There is a risk that the unpreparedness of an enterprise could lead to security misconfiguration in VPNs, thus exposing confidential information on the internet, and therefore exposing the computers to Denial of Service (DoS) attacks. In addition, certain people can use personal computers to conduct official tasks that may also pose a great deal of danger to the organisations. Organizations should guarantee that VPN services are secure and effective, as these services promise to be far more scrutinised. In addition, it is important to warn the workers against using personal computers for official purposes.

3.3 Impact-3: Potential Delays in Cyber-Attack Detection and Response

Due to the COVID-19 pandemic, the functioning of several security teams is likely to be compromised, making it difficult to identify malicious activities and even more difficult to respond to these activities [4]. It can also be a problem to upgrade patches on devices if the security teams are not operational. Security defences in place should be assessed by the organisations and the use of co-sourcing with external consultants should be explored, particularly for areas where key human risks have been identified.

3.4 Impact-4: Exposed Physical Security

This can be explained by the example of some companies in Nigeria's implementation of "work from home" policies, where reliable power supply and fast internet access may be a privilege in some quarters. Hence, the workers employed in such companies have to depend upon the public spaces to use power and free internet facilities [5]. The computer equipment and sensitive information that the device holds can be unwittingly exposed to theft or harm by this behaviour. Thus, the organizations are encouraged to raise awareness among their workers about information security. Working in public spaces should be limited and organisations should use technologies that in the event of theft or injury, ensure that sensitive information remains safe on such devices.

3.5 Impact-5: Influx of Cybercriminals

Globally, organizations are downsizing their workforce to cope with the effects of COVID-19. Most of the professionals have also lost their means of livelihood due to the numerous restrictions of movement by governments across the world. This move would likely encourage the growth of cyber criminals as idle people with internet access who have lost their jobs from the effects of COVID-19 may see an opportunity to make a living out of this pandemic. Organisations considering laying off staff should enforce proper exit plans. Also, we encourage all who have lost their jobs or currently being restricted to a location to consider taking this period to learn a new profitable skill and undertake online courses.

3.6 Impact-6: Business Continuity Plans (BCP) to Feature Global Pandemics

Most companies have business continuity plans, but the impact of a global pandemic like COVID-19 has not been taken into account in many BCPs [7]. Organizations need to re-visit their Business Continuity Program and Incident Response Plans with the widespread impact of COVID-19, in particular, to include such exigencies that impact several countries and vital supply chain components at the same time. An updated risk assessment should be carried out on the essential processes to determine the different options to ensure that these processes can still be managed at an appropriate level, and the failures can be dealt with.

3.7 Impact-7: Post COVID-19 Cyber Security Posture

With some analysts predicting a recession as one of the after-impacts of the pandemic, the COVID-19 pandemic has placed a major strain on the global economy [7,8]. In such a scenario, to cut down on their economic losses, the organisations are downsizing by cutting off business lines. This also includes cybersecurity operations that are perceived to be non-critical. However in the long run, this short-term practice may prove to be "penny wise and pound foolish," as this would further increase the impact of attacks on the organisation. Organizations are recommended to upgrade their BCPs and remote working policies/practices when prioritising cybersecurity during the re-strategization phase after COVID-19.

All in all, with new job models, new cybersecurity challenges, new planned legislation, personal hygiene and so on, COVID-19 will change our lives forever. The fight against COVID-19 is not only for the business, workers or clients, but a collective effort from everyone. It is also obvious that companies will need to reconsider their cyber risk management measures post COVID-19. This paper proposes to rank these effects of COVID-19 as per their severity levels. Fuzzy AHP is used for estimation as the technique for this prioritisation.

4 Methodology Followed

Protecting the systems from hackers in advance is a modern technique for optimal security from the attacks and hackers [9,10]. This estimated protection would come from prioritising the consequences of the pandemic of COVID-19. Multi-Criteria Community Decision Making (MCGDM) problems are therefore widely identified in practise in order to meet the goals according to the customers' expectations and the responsiveness of the data. There are several methods in literature which can be used to solve these problems [11–13]. AHP is a better strategy for evaluating the positive and negative attributes of the variables than any of the other MCDA methods.

However, the inherent uncertainties and imprecision that the decision-makers face in analysing the sensitivity of the objective data cannot be resolved by AHP alone. The researchers of this study found that the experts merge the Fuzzy definition with AHP because this enables a more accurate analysis of the real world problems [14,15].

Fuzzy AHP is a powerful method for evaluating difficult decision making contexts as this methodology gives specific graded target rates that determine each complicated problem. AHP has therefore been used to prioritise results through decision-making problem solving method [16]. The Fuzzy AHP focuses on the Fuzzy Numerical Interval of Triangular Fuzzy Numbers to maximise the effectiveness of the Fuzzy AHP approach for a more feasible view. These numbers are introduced to decide the weights of interpretative components. The AHP method uses only the pair-wise review matrix to resolve the inaccuracy of multi-criteria decision labelling challenges [17].

The model projected here makes it possible to use triangular fuzzy figures to define linguistic parameters and integrate fuzzy procedures with AHP. First step is to recognize the problem and identify its attributes. This has been done in the previous section of this work where the effects of COVID-19 pandemic were analysed.

50 domain experts were taken and impacts were discussed with them in order to gather the information for the study. Data is gathered and examined from their perspectives. The tree structure for Fuzzy AHP is shown in Fig. 1. The next stage is to build the Triangular Fuzzy Number (TFN) from the Tree Hierarchy. With the support of one factor's impact on the other factor, a pair-wise evaluation of each category of specified goal plays a key role.

Professionals translate this further by linguistic principles through specific figures and TFN. TFN, which ranges from *0 to 1* [14,15], is also used in this research paper. The mathematical versatility of the triangular fuzzy participation functions which can communicate with fuzzy data [16] is the reason for using the TFN. Furthermore, linguistic factors are classified as *equally significant, weakly significant*, and so on. Accurate statistics are graded as *1,2, …… 9*. As per the scale given to the variables that affect the scores in a numerical way, the experts awarded the points. The next step is to create the fuzzy comparison matrix according to the flow chart represented in Fig. 2.

The approach used in this paper is derived from [17]. The next step is the transformation of the fuzzified values into their degrees and the resolution of their own values. The next move is to check if the CR is below *1 or not*. The values are defuzzified if CR concludes less than 1, and the final results are determined, otherwise the pair-wise matrices are reconstructed and calculations are performed again if the CR is less than 1.

Final results of the weights of all the attributes help to determine the attribute with the highest priority, and the attribute with the least priority. Here, the attributes are COVID-19 results, hence the highest and the lowest impact is determined at the end. The steps for evaluating the priority are outlined in the next section.

5 Quantitative Assessment

The Fuzzy AHP method [10–14] was used in this article to test the efficacy of the proposed model. The Fuzzy AHP approach is used as a tool to determine the extent of a given impact from a range of impacts and

is ideal for precise decisions [15]. The authors have used this method to test the pandemic's most prioritized impacts. This form of classification and decision provides potential researchers with a novel and useful concept. The authors have previously used this technique [13] and obtained data from various experts to carry out the Fuzzy-AHP methodology. Using fuzzy AHP membership features, the responses were collected and then compiled.

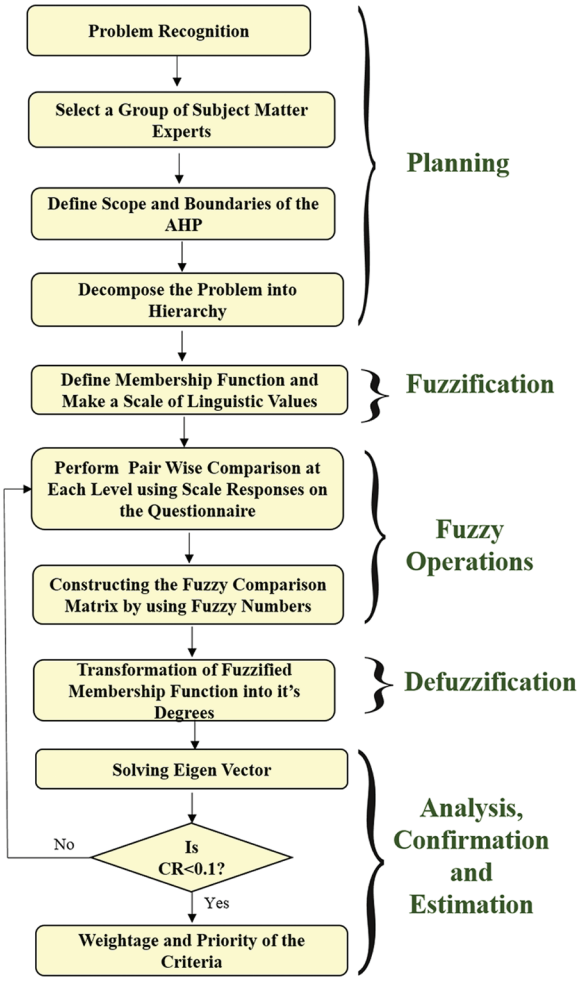

Figure 2: Flow chart of fuzzy AHP method

We chose the most prioritised impacts for the pandemic based on the membership functions. Thereafter, the aggregated fuzzy comparison matrix was prepared with the aid of the equations [14]. In the form of triangular fuzzy numbers [15], Tab. 1 displays the fuzzy pair-wise comparison matrix. The authors followed [16] the procedures to test the Consistency Ratio (CR) of the matrix. This paper used the alpha cut method [17] for the defuzzification procedure. The defuzzified pair-wise comparison matrix is represented in Tab. 2. The group's final weights are shown in Tab. 3. Finally, Fig. 3 displays the complete weights and priorities of the models.

Different methodologies have been used in different pandemics. This empirical investigation specifically used Fuzzy AHP for prioritizing the impacts and concluded that the most severely affected attribute was **Potential delays in cyber-attack detection and response.** According to the quantitative assessment in

Tabs. 1–3 and Fig. 3, the impact 7 obtained the highest priority with a weight of 0.25650, and the CR value of 0.0333. In addition, prioritization of the models in the descending order is: *I3 > I5 > I6 > I4 > I7 > I2 > I1*. Impact 3 (**Potential delays in cyber-attack detection and response***)* has obtained the highest weight (0.25650), Impact 5 (I6) obtained the second highest rank and weight (0.17290), whereas the Impact 1 (I1) obtained the lowest rank and weights (0.07330). By the obtained ranks and weights, the authors assigned the ranks to the impacts being used in minimizing the spread of COVID-19.

Table 1: Aggregated fuzzy comparison matrix

Impacts	I1	I2	I3	I4	I5	I6	I7
I1	1.00000, 1.00000, 1.00000	0.68980, 0.88600, 1.10020	0.22550, 0.27620, 0.35740	0.30510, 0.38920, 0.56090	1.00000, 1.37410, 1.71180	0.56100, 0.83600, 1.07810	0.30400, 0.37660, 0.47230
I2	–	1.00000, 1.00000, 1.00000	0.30300, 0.42080, 0.60520	0.19160, 0.23030, 0.30010	0.51380, 0.79590, 1.20320	0.69500, 0.95020, 1.34570	1.14860, 1.43850, 1.69620
I3	–	–	1.00000, 1.00000, 1.00000	1.19280, 1.58260, 2.14970	1.07810, 1.59900, 2.11300	0.82060, 1.11180, 1.61500	0.56700, 0.71320, 0.87390
I4	–	–	–	1.00000, 1.00000, 1.00000	0.32300, 0.44800, 0.60510	0.25840, 0.31720, 0.41680	0.66610, 1.05640, 1.54270
I5	–	–	–	–	1.00000, 1.00000, 1.00000	1.34790, 1.81800, 2.38590	1.41310, 1.96510, 2.48200
I6	–	–	–	–	–	1.00000, 1.00000, 1.00000	0.85400, 1.10870, 1.45320
I7	–	–	–	–	–	–	1.00000, 1.00000, 1.00000

Table 2: Defuzzified pair-wise comparison matrix

Impacts	I1	I2	I3	I4	I5	I6	I7
I1	1.00000	0.89050	0.28390	0.41110	1.36510	0.82780	0.38240
I2	1.12300	1.00000	0.43750	0.23810	0.82720	0.98530	1.35780
I3	3.52240	2.28570	1.00000	1.62690	1.59730	1.16480	0.71680
I4	2.43250	4.19990	0.61470	1.00000	0.45610	0.32740	1.08040
I5	0.73250	1.20890	0.62610	2.19250	1.00000	1.84250	1.95640
I6	1.20800	1.01490	0.85850	3.05440	0.54270	1.00000	1.13120
I7	2.61510	0.73650	1.39510	0.92560	0.51110	0.88400	1.00000
							CR = 0.0056045

Table 3: Overall weight and ranks of the impacts

COVID-19 Impacts	Weights	Ranks
Impact-1 (I1)	0.089873	7
Impact-2 (I2)	0.101343	6
Impact-3 (I3)	0.194164	1
Impact-4 (I4)	0.150007	4
Impact-5 (I5)	0.172048	2
Impact-6 (I6)	0.156259	3
Impact-7 (I7)	0.136306	5

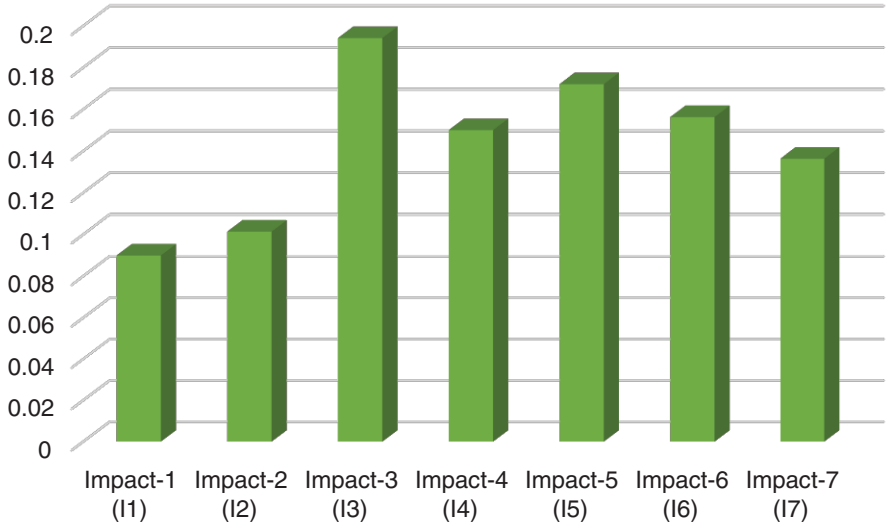

Figure 3: Priorities of the COVID-19 impacts

6 Recommendations for Practitioners

It's important to note that COVID-19, with a time period measured in weeks or months, is supposed to be temporary. But for IT and cybersecurity staff, this could exacerbate an already complicated landscape. They need to take into account the aftermath as they invest, build and carry out new capabilities throughout the crisis. The proposed research paper analyses the impacts of the pandemic during and after this time. In this work, seven most critical impacts were considered and prioritised by using the technique of Fuzzy-AHP. There are some recommendations for practitioners after the prioritisation of the impacts that could help safeguard the software business ecosystem during this COVID-19 pandemic.

- **Some organizations will need to move to new operating models.** Cybersecurity and IT rights would need a thorough analysis and immediate handling to address the bottlenecks that exist in providing secure mechanisms for employees who work from home/or are remotely connected. Remote control and assistance of staff would become important. And cybersecurity experts must maintain strict systems and access scrutiny for employees transitioning from home to office before permitting the modified system to associate with the network again.
- **Companies will need to reset their security systems to ensure there are no outliers.** It will be important to restart both physical and digital systems, to search for any digital holes in the fence.

In order to allow remote work, device and data access rights approved during the pandemic would require auditing to decide if they should be withdrawn or modified. For holes, foul routes or false identities, IT structures would need to be examined. The explanation is that cyber criminals may have discovered ways to gain access to otherwise hardened services.

- **New cyber risks that appeared during the pandemic must be understood.** Security specialists, for example, would need to scrutinise the digital capacities of vital business functions, ensuring that during a lockout they can withstand cyber-attacks. To maintain sustainability during a health crisis, they will investigate vital supply chains, including digital supply chains.
- **Corporate IT security architectures should be reassessed.** This contains access tools, support requirements for mass-scale remote access and security authentication mechanisms based on risk/context.
- **Advanced technology must be deployed.** Advanced abilities enabled by next-generation technology such as artificial intelligence, big data and machine learning must be included in threat detection and response capabilities. These are required, without human interventions, to identify and reply to adverse behaviour at machine speed. In addition, the companies may want to examine protection against cyber-attack damages suffered during a pandemic scenario.

The lessons they learned during the crisis would also need to be shared by the security officials. That will support them in making effective countermeasures for a pandemic like calamity in future. The experts need to recalibrate security solutions, especially in the context of provision, scalability, remote management capabilities and cloud-based availability. They should also collaborate with the trusted stakeholders proactively in preparing for dynamic scalability, provision of the services and solutions. Planning requires both imaginative and detailed initiatives. In order to adopt innovative approaches and consider new operating technologies, leaders face a growing imperative. Automation will, in particular, offer operational efficiencies and minimise dependency on human interventions.

7 Conclusions

A new age in cyber security has been ushered in by the pandemic. Critical players in the economic recovery will be security practitioners who lift their game and consumer's security, technologies and data of their businesses from novel or enhanced threats of extra advanced cyber criminals. Computer protection is a complex challenge since multiple features are involved. The present pandemic situation and the debate in this paper clearly describe the need for efficient impact analysis in this digital era. In a software or software development process, all practitioners want an organised orientation to facilitate efficient security. Using MCDM procedures, this report analyses the impact and offers a table of prioritised impact analysis. The outcomes of the final table can be used by any practitioner to establish guidelines for fraudsters to secure apps and mobile applications in this pandemic. In the list of seven impacts, the most prioritised impact is possible delays in cyber-attack detection and response. Impact five, the influx of cybercriminals, is the second most impactful insecurity.

Companies will also be required to optimise budgets and accelerate their digital transformations as they adjust to the *new normal* post-crisis. By leveraging the emerging technologies and service models transformed to do more with less, security leaders would have to embrace these initiatives. It is important to conduct these in the most cost-effective way. Additional Computational modelling is an efficient method that helps by complete efforts to estimate main transmission parameters. Automated instruments, decision analysis, Fuzzy-AHP for computation and dynamic analysis, which play an important role in pandemic management, are also included in the proposed prioritisation model. To monitor the distribution of COVID-19, the Fuzzy-AHP tool is used to prioritise the available results. The project has the following practical/scientific utilities:

- The results of the above calculation show that the impact of possible delays in the detection and response of cyber-attacks is highest among the seven impacts mentioned in the above report.
- The suggested project offers a structured framework for listing the most severely affected impact analysis during and after the pandemic of COVID-19.
- The proposed study may assist the developers and software engineers in developing guidelines for the data security of their staff and users.

Acknowledgement: Taif University Research Supporting Project number (TURSP-2020/239), Taif University, Taif, Saudi Arabia.

Funding Statement: Funding for this study is received from the Taif University Research Supporting Projects at Taif University, Kingdom of Saudi Arabia under Grant No. TURSP-2020/239.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] J. G. Ronquillo, J. W. Erik, K. Cwikla, R. Szymanski and C. Levy, "Health IT, hacking, and cybersecurity: National trends in data breaches of protected health information," *JAMIA Open*, vol. 1, no. 1, pp. 15–19, 2018.

[2] K. Sahu and R. Shree, "Stability: Abstract roadmap of security," *American International Journal of Research in Science, Engineering & Mathematics*, vol. 2, no. 9, pp. 183–186, 2015.

[3] J. Davis, "The 10 biggest healthcare data breaches of 2019, so far." Xtelligent Healthcare Media, LLC. 2019. [Online]. Available: https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2019-so-far.

[4] McKinsey & Company, "COVID-19 Crisis Shifts Cybersecurity Priorities and Budgets." 2020. [Online]. Available: https://www.mckinsey.com/business-functions/risk/our-insights/covid-19-crisis-shifts-cybersecurity-priorities-and-budgets#.

[5] TCS Worldwide, "How COVID-19 is Dramatically Changing Cybersecurity." 2020. [Online]. Available: https://www.tcs.com/perspectives/articles/how-covid-19-is-dramatically-changing-cybersecurity.

[6] OrangeCyberDefense, "A Biological Hazard Goes Digital." 2020. [Online]. Available: https://orangecyberdefense.com/global/white-papers/covid-19-a-biological-hazard-goes-digital/.

[7] Deloitte, "COVID-19's Impact on Cybersecurity," 2020. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/ng/Documents/risk/ng-COVID-19-Impact-on-Cybersecurity-24032020.pdf.

[8] K. Sahu, R. Shree and R. Kumar, "Risk management perspective in SDLC," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 4, no. 3, pp. 1247–1251, 2014.

[9] R. Kumar, S. A. Khan and R. A. Khan, "Analytical network process for software security: A design perspective," *CSI Transactions on ICT*, vol. 4, no. 2, pp. 255–258, 2016.

[10] K. Sahu and R. K. Srivastava, "Soft computing approach for prediction of software reliability," *ICIC Express Letters*, vol. 12, no. 12, pp. 1213–1222, 2018.

[11] R. Kumar, S. A. Khan and R. A. Khan, "Durability challenges in software engineering," *Crosstalk*, vol. 29, no. 5, pp. 29–31, 2016.

[12] K. Sahu and R. K. Srivastava, "Needs and importance of reliability prediction: An industrial perspective," *Information Sciences Letters*, vol. 9, no. 1, pp. 33–37, 2020.

[13] S. A. Khan, M. Alenezi, A. Agrawal, R. Kumar and R. A. Khan, "Evaluating performance of software durability through an integrated fuzzy-based symmetrical method of ANP and TOPSIS," *Symmetry*, vol. 12, no. 4, pp. 1–15, 2020.

[14] K. Sahu and R. K. Srivastava, "Revisiting software reliability," *Advances in Intelligent Systems and Computing*, Singapore, Springer, vol. 808, pp. 221–235, 2019.

[15] R. Kumar, S. A. Khan, A. Agrawal and R. A. Khan, "Measuring the security attributes through fuzzy analytic hierarchy process: Durability perspective," *ICIC Express Letters-An International Journal of Research and Surveys*, vol. 12, no. 6, pp. 615–620, 2018.

[16] K. Sahu and R. Shree, "Helpful and defending actions in software risk management: A security viewpoint," *Integrated Journal of British*, vol. 4, pp. 1–7, 2015.

[17] A. Agrawal, M. Alenezi, S. A. Khan, R. Kumar and R. A. Khan, "Multi-level fuzzy system for usable-security assessment," *Journal of King Saud University-Computer and Information Sciences*, pp. 1–9, 2019.