Computer Systems Science & Engineering
DOI:10.32604/csse.2021.015282
Article

Tech Science Press

Safeguarding Cloud Computing Infrastructure: A Security Analysis

Mamdouh Alenezi[*]

College of Computer and Information Sciences, Prince Sultan University, Riyadh, Kingdom of Saudi Arabia
[*]Corresponding Author: Mamdouh Alenezi. Email: malenezi@psu.edu.sa

Received: 13 October 2020; Accepted: 26 November 2020

Abstract: Cloud computing is the provision of hosted resources, comprising software, hardware and processing over the World Wide Web. The advantages of rapid deployment, versatility, low expenses and scalability have led to the widespread use of cloud computing across organizations of all sizes, mostly as a component of the combination/multi-cloud infrastructure structure. While cloud storage offers significant benefits as well as cost-effective alternatives for IT management and expansion, new opportunities and challenges in the context of security vulnerabilities are emerging in this domain. Cloud security, also recognized as cloud computing security, refers to a collection of policies, regulations, systematic processes that function together to secure cloud infrastructure systems. These security procedures are designed to safeguard cloud data, to facilitate regulatory enforcement and to preserve the confidentiality of consumers, as well as to lay down encryption rules for specific devices and applications. This study presents an overview of the innovative cloud computing and security challenges that exist at different levels of cloud infrastructure. In this league, the present research work would be a significant contribution in reducing the security attacks on cloud computing so as to provide sustainable and secure services.

Keywords: Cloud computing; cloud security; cloud security issues; security attacks; intrusion

1 Introduction

Maintaining the traditional computing technology has become expensive and problematic in the present day context. Transmitting information everywhere and at any time through traditional computing is becoming extremely challenging nowadays, more so when the peripheral storage arrangement has become a significant necessity for storing personal information [1]. Outdated computing is currently incapable of accommodating the enhanced number of internet operators on sharing portals, social networking, digital broadcasting, etc. The rapid increase in the use of Internet worldwide as well as the amount of use and accessibility of resources calls for an innovative paradigm in cloud computing services. Cloud computing has been receiving intensive attention in Information and Communication Technology (ICT) world. Cloud computing is mostly associated with transferring facilities, data processing to an internally or externally, location-transparent service or provider [2].

Cloud computing has reshaped every business around the world, irrespective of the location or industry sector. From basic development tools to large databases and enterprise-grade software, the entire enterprise system is now shifting into the cloud based system. Cloud computing is actually one of the main aspects of a variety of information technology conversations, and cloud computing security is an essential prerequisite in this context [3–5]. Usually conversations concentrate on all common safety and convenience, drawbacks and specifications. However, even the most popular protection measures are not always adequate enough to safeguard the data from damage, illegal access, violation of data integrity, etc., [6–10]. There are many other essential and significant features of any information technology infrastructure which should be enforced in a much more effective manner. One of these systems is the cloud infrastructure [11–14]. This is not surprising considering that the cloud infrastructure is highly scalable, provides expanded portability and modularity for app creation, and entails low storage costs. Nevertheless, infrastructure security concerns in cloud computing is an important concern due to the hyper-connected existence of the cloud. Fig. 1 demonstrates the progress made in the provision of computer resources and platforms.

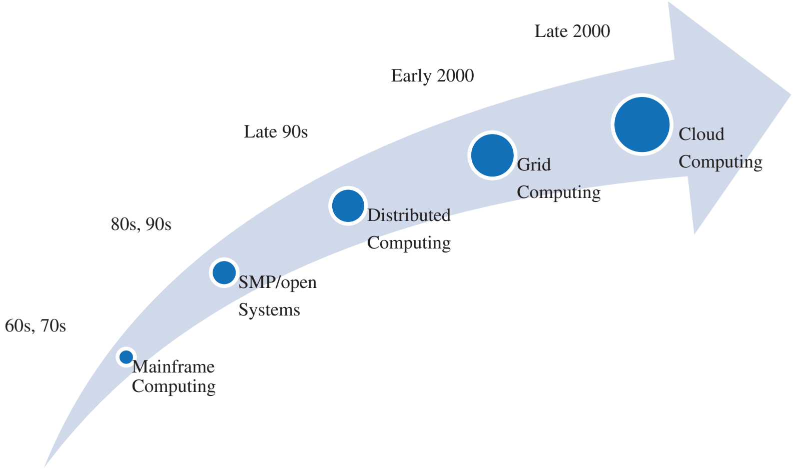

Figure 1: The evolution of computing architecture

Cloud computing is a growing Internet-based computing application that combines various infrastructure, applications and services *on-demand* and *pay-as-you-go*. The principle of this new innovation began in 1960, when telecommunications firms used a similar technology to provide point-to - point data circuits. This practice continued till 1990 after which it was substituted with the virtual private networks. But because of network traffic and for making network connectivity more effective, the cloud has been introduced between both servers and arrangement. *Amazon* has taken a crucial role in creating cloud computing through the advancement of new data centers. It was implemented in 2007 by *Google*, *IBM* and several outstanding institutions and companies [15]. Over the last few years, the cyber security research group has been focusing intently on strengthening the security and privacy of the cloud infrastructure as well as gaining the confidence of the cloud users. Conversely, the prevalence of *ad hoc* management solutions targeted at a very limited part of the overall issue makes it impossible to determine the latest technology in cloud security reasonably. The cloud computing model can only be completely utilized if the participation of the user and the cloud service provider in security measures is broadened to increase their trust [7,11].

Regardless of the various advantages of cloud computing, just 33% of businesses are committed towards strengthening cloud adoption. This was disclosed in a survey conducted by the Cloud Security Alliance (CSA). The survey included the responses of more than 200 IT and IT security executives and cited 6 key problems in the successful implementation of cloud ventures. In the light of extremely complex attacks aimed at manipulating the company's information, many IT organizations feel extremely uncomfortable with the alleged lack of influence over business data. The six key concerns that are major deterrents in the acceptance and adoption of Cloud Computing projects have been illustrated in Fig. 2.

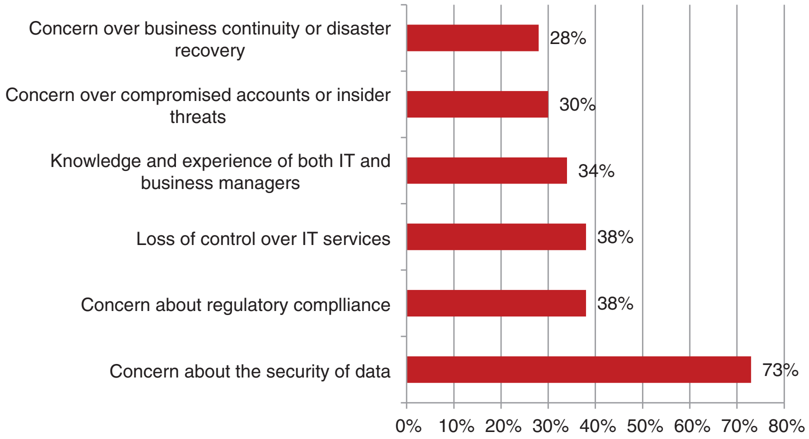

Figure 2: Top challenges holding back cloud projects (Source: CSA)

As per the Survey, *data security* is at the top of the priority list of these issues. 73 percent of the participants in the survey suggested that this is a big warning sign for them. Cloud computing providers prevent data breaches by using risk reduction techniques and strategies, including encrypting or tokenizing information, before using a cloud storage service [16].

Despite this substantial development, only a little consideration has been given to the concern of cloud security, both in literature and in implementation. Today, research involves exchanging, sharing, combining, changing knowledge, connecting applications as well as other services within and between organizations. In order to safeguard the quality and integrity of digital data, security becomes a significant and a challenging issue for achieving the three pronged targets of transparency, virtualization and delivery interconnectedness [17]. Security measures of cloud computing, particularly data security, have become highly significant. Innovative approaches to protect the cloud need to be identified and established.

The rest of this study is systematized as follows: Section 2 discusses the recent related works in the area of cloud security. Sections 3 describe the significant security concerns associated with cloud infrastructure. Section 4 provides an overview of the study. Finally, Section 5 concludes the study by enlisting the main findings of the report and recommendations.

2 Related Works

The Cloud security model has been addressed by both the practitioners from the industry as well as the research scientists. There are many international and national conferences workshops that concentrate solely on cloud security. In addition, there are numerous articles in the international and national journals that are specifically premised on cloud protection. Moreover, several authors have published their work in cloud security area. Some of the recent studies have been discussed below:

Almorsy et al. [8] have conducted a thorough review of the topic of cloud security. They looked at the problem from a cloud design perspective, the cloud's features viewpoint, cloud participants perspective, as well as cloud service delivery structures perspective. Depending on their review, they developed a thorough description of the cloud security issue and the important aspects that should be protected by any suggested security solution.

Singh & Chatterjee [9] addressed the essential functionality of cloud computing, security problems, threats and potential strategies. In addition, they outlined a range of important cloud-related subjects, including cloud architecture structure, service and implementation model, cloud technology, cloud security principles, threats , and attacks. A variety of open research questions related to cloud protection were also addressed in their paper.

Kalaiprasath et al. [10] performed a thorough study to analyse the possible risks to cloud customers and to define enforcement models and security standards that must be in place to mitigate these risks. They established the ontology of cloud security measures, threats and enforcement. They have also created an application which categorizes the security risks faced by cloud consumers and dynamically defines the high level of security and enforcement policy controls that must be triggered for each incident. The application also shows current cloud providers which endorse these security measures.

Ardagna et al. [11] provided a study that concentrated on the interaction between cloud security and cloud security assurance. Second, they presented a summary of the latest technology of cloud security. They also introduced the concept of cloud security assurance and examined its rising impact on cloud security strategies. Ultimately, they provided a set of strategies for the creation of next level cloud security and cloud products.

Iqbal et al. [12] provided the classification of cloud security breaches and possible mitigation methods with the goal of providing an in-depth awareness of security requirements of the cloud setting. They also emphasized upon the significance of threat identification and prevention as a service.

Coppolino et al. [13] presented a thorough overview of the significant threats that obstruct wide-scale implementation of cloud services and a privilege to review the technologies presently being offered by large providers. Their paper also addressed the future research advices of cloud - based security research, taking a glimpse of key research patterns and the most certified strategies. Their research was conducted on the best range of proprietary and Open Source cloud services.

Tabrizchi & Rafsanjani [14] examined the various elements of cloud computing, and also the security and privacy concerns facing these structures. In addition, their work provided a new category of the latest security solutions that function in this field. Additionally, their survey identified different forms of security threats that are affecting cloud storage services and also addressed open concerns and possible future approaches. Their research focused on the awareness of the security issues faced by cloud administrators, such as the cloud service providers, data owners, and cloud users.

3 Security Concerns with Cloud Infrastructure

SaaS, PaaS, IaaS are the increasingly developing terms in the field of cloud computing [6,17–19]. ‘Saas,’ ‘PaaS’ and ‘IaaS’ are some of the most frequently used acronyms in the cloud market, and with appropriate reason. These three words differentiate between the principal cloud based service models: ‘*Software as a Service*,’ ‘*Platform as a Service*,’ and ‘*Infrastructure as a Service*.’ Although cloud computing can satisfy practically any IT needs conceivable, these categories are important to show the function that a specific cloud service plays and how that service fulfills its purpose. In other terms, SaaS, PaaS, and IaaS are the three primary cloud computing concepts. According to [20] cloud service providers and customers are responsible for confidentiality and protection in cloud computing system, but their level of commitment for various delivery models can vary. Service Infrastructure (IaaS) acts as the base layer for certain delivery models, and the absence of protection in this layer impacts the other delivery models. In IaaS, while the clients are essential for safeguarding operating systems, software and information, the protection of consumers' data is a major responsibility of cloud service providers. In Platform as a service (PaaS), clients are responsible for securing applications which designers build and maintain on platforms, while operators are responsible for the safety of application components and working environments from each other. In SaaS, cloud service providers, especially public cloud suppliers, are more responsible than clients for improving application security and managing effective data transformation. Data breaches, technology security flaws and accessibility are critical problems that can lead to regulatory and personal liability in the SaaS model.

Cloud computing poses a range of interesting security problems and challenges. Data can be processed in the cloud database with a third-party provider and accessed through the internet. This suggests that the visibility and control of the data is restricted. It also poses the issue of how this can be adequately secured [21]. It is imperative that everyone recognizes their respective positions and the security concerns inherent in cloud computing. Cloud service providers regard cloud protection risks as mutual liabilities. The cloud infrastructure security can be observed, evaluated and executed as per its constructing levels such as the network, host and application levels [19]. Fig. 3 shows the different levels of cloud infrastructure.

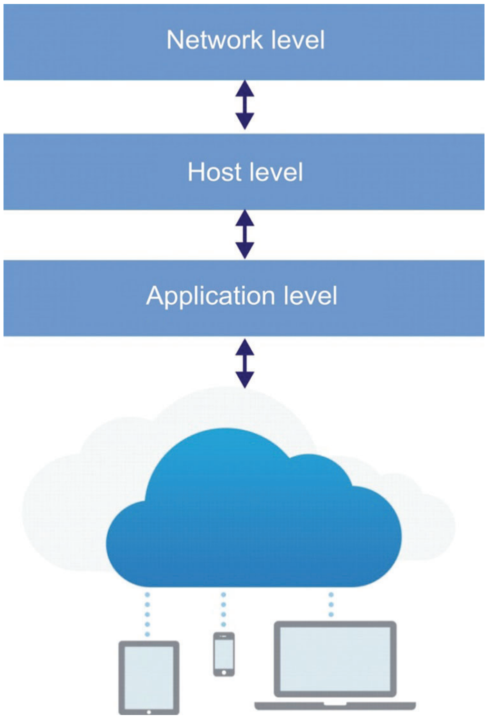

Figure 3: Overview of cloud infrastructure

3.1 Network Level Security

Every data transferred on the network must be safe. Powerful network traffic encryption methods such as *Secure Socket Layer (SSL)* as well as *Transport Layer Security (TLS)* may be used to avoid disclosure of confidential data. Many other primary protection features such as *data security, data integrity, user authentication, privacy protection, web server security, virtual machines accessibility, compatibility, recovery, and privacy violations* should be thoroughly researched in order to maintain the smooth and consistent functioning of the cloud. Throughout this use scenario, there can be four major risk factors such as (a) Ensure authenticity and privacy of the communication-in-transit entity to and from the cloud service provider; (b) Ensure proper network access (authentication, authorization and auditing) of any service used by the cloud service provider; (c) Ensure the availability of Internet-based services in a cloud platform used by an organization or delegated to an organization by the cloud service providers and (d) Replacing the existing network field and domain third party system.

3.2 Host Level Security

Host Security explains how the server is designed to avoid threats, minimize the effect of a devastating attack on the entire process, and respond to threats whenever they emerge. When evaluating the host security and managing risk, consideration should be given to cloud computing service delivery models such as SaaS, PaaS, and IaaS and public, private, and hybrid implementation models. The host security duties for SaaS and PaaS services are shifted to the cloud infrastructure provider. IaaS clients are mainly capable for safeguarding hosts supported in the cloud system.

3.3 Application Level Security

Research suggests that so many sites are protected at the level of the network although there may be security vulnerabilities at the level of the application which may give unauthorized users the access to data. Software and hardware tools may be used for protection for applications. Throughout this way, adversaries would not be able to manipulate and alter these programs. SQL injection, Secret key manipulation, XSS attacks are examples of security concerns to the application level that arise from unauthorized use of the implementations.

Thus, to summate, the challenges of cloud infrastructure security and cloud storage lie in the description and implementation of security implications that every party involved in the process provides. The following Tab. 1 shows the level-wise common cloud threat and corresponding mitigation strategy.

4 Discussion

Cloud computing is an evolving concept which includes every basic elements of computer technology like the end-user devices, communications systems, access monitoring systems, as well as cloud infrastructures. In particular, with the advent of innovative trends including the 5 G Network, Internet of Things (IoT), and green infrastructure, the function of cloud computing would be extra critical for collecting and analyzing more data than ever before. The complexity of the new business world has introduced a wide range of threats and security issues. In recent times, due to the lack of information on *how much* and *where the workflow* resides, it is becoming increasingly difficult to track and mitigate the growing potential risks. Till they are able to detect the threats, the security organizations have to contend with the problem of replication of data, lack of command of access to data and safety to comply with regulatory requirements without even a clear image of the cloud computing infrastructure. The information and cloud infrastructure should be secure against unidentified / malicious activities in all cloud architectures to achieve robust cloud protection. Many studies are being carried out to resolve security issues in a cloud infrastructure. However, for a stable cloud computing there are several open problems which need to be resolved. Security concerns in association with cloud communication, network, and protection of data, application and online services are among the conventional issues at the start of cloud technology. Innovative protection problems arise from multi-tenancy, application development and shared pool infrastructure. Several tools and facilities are accessible in a cloud computing system, but resource protection relies on the availability and quality of the service. The security of the device is an open question in the cloud technology.

Several businesses do not understand the cloud security awareness gap. They underestimate the security challenges prevailing today which are highly susceptible to cloud account breach and data leakage, resulting in significant financial loses. Investing in cloud cyber protection solutions that exploit automation and AI for minimal human capital is a straightforward way of automating data safety and upholding the principles of data management. Automation of the collection and simulation with behavior analytics of the current network data not only enables the detection and classification of possible threats by organizations but also improves their effectiveness.

Table 1: Level-wise common cloud threat and mitigation

Cloud Security Level	Threat	Mitigation
Network Level	DDoS attack	Execute an appropriate network infrastructure according to IT security strategy and reduce the amount of ICMP and SYN packets on router interfaces.
	DNS attack	Domain name system security Extensions (DNSSEC) decreases the impact of DNS threats
	IP based attack	Clear old ARP addresses from cache
	Snooping attack	Installing anti-virus software enforcing security controls and procedures.
	Man-in-the–middle attacks	Providing a good encryption feature prevents unauthorized people from breaching the network.
Host Level	Session hijacking	Cookie must be evaded, or regular Cookie Cleaning is compulsory
	Hyperjacking	Security organization of the hypervisor should be reserved separately from regular traffic
	Backdoor attack	Implement firewall and robust network monitoring
	VM attack	Operational security procedures need to be followed
Application Level	SQL injection	Use of Prepared Statements, Stored Procedures Enforce Least Privilege
	Secret key manipulation	Avoid putting parameters into a query string
	XSS attacks	On entry, monitor input. When user feedback is obtained, filter, based on what is required or true input as specifically as appropriate.

5 Conclusion

Taking into consideration the many advantages that cloud computing provides to individuals or organizations, it is reasonable to conclude that cloud computing has quickly become a revolutionary technology. Cloud computing helps the society to deal with future issues such as big data management, information security and quality assurance. In addition, new innovations such as Artificial Intelligence, decentralized ledger technology, and several other innovations are becoming accessible as cloud computing services. In spite of these benefits, the cloud is often sensitive to plenty of security problems. Thus security is a big issue and must be the elemental concern in implementation of the cloud. To achieve the goal of providing stable cloud infrastructure, developers must fix certain security problems. The consumers and the providers are already well aware of these potential risks. The key objective of this study was to highlight all the potential security problems in the cloud computing infrastructure as well as to deliver an effective resolution for such problems. This paper has endeavored to demonstrate numerous security issues, weaknesses, threats and risks at different levels of cloud infrastructure which hinder the deployment of cloud computing. These security problems are caused by different features of the cloud. A simplified interpretation of these concerns has been provided here to improve the effectiveness in identifying the security vulnerabilities of the cloud computing system, and for developing efficacious preventive measures for these. The study collates a set of recorded strategies, measures and methods that must be used to minimize risks and threats for seamless and secure use of cloud computing services.

Acknowledgement: The authors are thankful to Prince Sultan University, Saudi Arabia, for providing the fund to carry out this work.

Funding Statement: This work is funded by Prince Sultan University, Riyadh, the Kingdom of Saudi Arabia.

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

References

[1] M. Zarour, M. T. J. Ansari, M. Alenezi, A. K. Sarkar, M. Faizan *et al.,* "Evaluating the impact of blockchain models for secure and trustworthy electronic healthcare records," *IEEE Access*, vol. 8, no. 8, pp. 157959–157973, 2020.

[2] D. Owens, "Securing elasticity in the cloud," *Communications of the ACM*, vol. 53, no. 6, pp. 46–51, 2010.

[3] W. Y. Chang, H. A. Amara and J. F. Sanford, "Transforming enterprise cloud services," Springer, 2010. [Online]. Available: https://www.springer.com/gp/book/9789048198450. Last Visit Nov 17, 2020.

[4] M. T. J. Ansari and D. Pandey, "Risks, security, and privacy for HIV/AIDS data: Big data perspective," *Big Data Analytics in HIV/AIDS Research, IGI Global*, vol. 5, no. 6, pp. 117–139, 2018.

[5] M. Bilal, L. O. Oyedele, J. Qadir, K. Munir, S. O. Ajayi *et al.,* "Big data in the construction industry: A review of present status, opportunities, and future trends," *Advanced Engineering Informatics*, vol. 30, no. 3, pp. 500–521, 2016.

[6] K. Jamsa, "Cloud computing: SaaS, PaaS, IaaS, virtualization, business models, mobile, security and more," Jones & Bartlett Publishers, 2012. [Online]. Available: https://books.google.co.in/books/about/Cloud_Computing.html?id=msFk8DPZ7noC&redir_esc=y. Last Visit Nov 17, 2020.

[7] M. T. J. Ansari and D. Pandey, "An integration of threat modeling with attack pattern and misuse case for effective security requirement elicitation," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 3, pp. 15–23, 2017.

[8] M. Almorsy, J. Grundy and I. Müller, "An analysis of the cloud computing security problem." arXiv preprint arXiv: 1609.01107, 2016.

[9] A. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey," *Journal of Network and Computer Applications*, vol. 79, no. 5, pp. 88–115, 2017.

[10] R. Kalaiprasath, R. Elankaviand and D. R. Udayakumar, "Cloud security and compliance-A semantic approach in end to end security," *International Journal of Mechanical Engineering and Technology*, vol. 8, no. 5, pp. 987–994, 2017.

[11] C. A. Ardagna, R. Asal, E. Damiani and Q. H. Vu, "From security to assurance in the cloud: A survey," *ACM Computing Surveys*, vol. 48, no. 1, pp. 1–50, 2015.

[12] S. Iqbal, M. L. M. Kiah, B. Dhaghighi, M. Hussain, S. Khan *et al.,* "On cloud security attacks: A taxonomy and intrusion detection and prevention as a service," *Journal of Network and Computer Applications*, vol. 74, no. 5, pp. 98–120, 2016.

[13] L. Coppolino, S. D'Antonio, G. Mazzeo and L. Romano, "Cloud security: Emerging threats and current solutions," *Computers & Electrical Engineering*, vol. 59, no. 6, pp. 126–140, 2017.

[14] H. Tabrizchi and Rafsanjani, "A survey on security challenges in cloud computing: Issues, threats, and solutions," *Journal of Supercomputing*, vol. 5, no. 6, pp. 1–40, 2020.

[15] M. S. V. Janakiram, “Cloud computing strategist,” *Demystifying the Cloud an Introduction to Cloud Computing, Version 1*, 2010. [Online]. Available: https://www.scribd.com/document/92333549/Demystifying-the-Cloud-eBook. Last Visit Nov 17, 2020.

[16] McAfee, 6 Cloud security issues that businesses experience, 2020. [Online]. Available: https://www.mcafee.com/blogs/enterprise/cloud-security/6-cloud-security-issues-that-businesses-experience/. Last Visit Nov 17, 2020.

[17] M. T. J. Ansari, D. Pandey and M. Alenezi, “STORE: Security threat oriented requirements engineering methodology,” *Journal of King Saud University-Computer and Information Sciences*, pp. 1–18, Article in Press, 2018.

[18] M. T. J. Ansari, F. A. Al-Zahrani, D. Pandey and A. Agrawal, “A fuzzy TOPSIS based analysis toward selection of effective security requirements engineering approach for trustworthy healthcare software development,” *BMC Medical Informatics and Decision Making*, vol. 20, no. 1, pp. 1–13, 2020.

[19] T. Mather, S. Kumaraswamy and S. Latif, “Cloud security and privacy: An enterprise perspective on risks and compliance,” O’Reilly Media, Inc., 2009. [Online]. Available: https://sites.google.com/site/nandur63anggrek42/FteRFD6287SISOTMAK1225. Last Visit Nov 17, 2020.

[20] H. Takabi, J. B. Joshi and G. J. Ahn, “Security and privacy challenges in cloud computing environments,” *IEEE Security & Privacy*, vol. 8, no. 6, pp. 24–31, 2010.

[21] R. Kumar, M. Alenezi, M. T. J. Ansari, B. Gupta, A. Agrawal *et al.,* “Evaluating the impact of malware analysis techniques for securing web applications through a decision-making framework under fuzzy environment,” *International Journal of Intelligent Engineering and Systems*, vol. 13, no. 6, pp. 94–109, 2020.