IET Communications

Research Article

IET Journals
The Institution of Engineering and Technology

Cyber security threats, challenges and defence mechanisms in cloud computing

ISSN 1751-8628
Received on 10th January 2019
Revised 20th October 2019
Accepted on 4th February 2020
E-First on 19th March 2020
doi: 10.1049/iet-com.2019.0040
www.ietdl.org

Abdullah Aljumah[1], *Tariq Ahamed Ahanger*[1] ✉

[1]*College of Computer Engineering and Sciences, Prince Sattam Bin Abdulaziz University, Al-Kharj 16278, Saudi Arabia*

✉ *E-mail: t.ahanger@psau.edu.sa*

Abstract: With the advent of computers and their widespread use, cloud computing has been identified as one of the major emerging components of computer technology. The benefits of cloud computing, in the form of processing power and computing resources connected via the internet, have not only bolstered business and personal operations of users but have also led to severe security and privacy threats that require adaptation into cloud computing systems. In light of this, the present study explores the various threats to cloud computing, in addition to outlining defence mechanisms against these threats. It was found that there is a major threat concerning data breaches because of the lack of management understanding of the use of cloud computing services and their defence mechanisms. Furthermore, there can be an abuse of cloud computing services that, in turn, affect not only sensitive data pertaining to the organisation but also the personal identity and information of the user.

1 Introduction

1.1 Cloud computing and its security aspects: an overview

Cloud computing is a model that enables global and on-demand access to a network of shared computing resources that can be provisioned and made available through a cloud service provider [1]. This environment supports high scalability, flexibility, and multi-tenancy [2]. A basic cloud computing environment is represented in Fig. 1, where users can access the cloud from any supporting device from any part of the world.

Security is a true challenge for cloud architecture, where the software, hardware, and infrastructure are maintained and operated by a third party. This third party sells such services and resources to the user [3]. There are numerous ways in which cloud computing technologies are implemented (using diverse architectures, services, and models) and operated (with a plethora of technologies, software, and applications), making it a substantial security challenge. Maintaining security is among the major responsibilities of the service provider [4, 5]. Cloud service providers are required to ensure that integrity, reliability, and confidentiality of data is not compromised [6]. Another aspect of security is to maintain the anonymity of the user and to protect the data's location. Service providers are required to employ a security mechanism that offers adequate data and resource protection as well as to mitigate malicious external threats [7, 8].

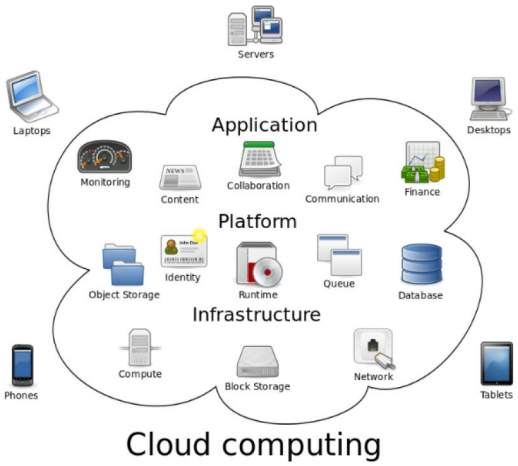

Fig. 1 *Basic cloud structure [1]*

2 Need for the study

Almost every aspect of modern network or data storage is associated with cloud computing technology. Maintaining reliability and continuous access to services and data provided by the cloud is a high-priority requirement. Security and privacy issues associated with the cloud environment are among the major challenges that hinder the acceptance and distribution of cloud computing technology. The well-known threats connected to cloud security are data loss, hacking phishing, botnet, and many more [9]. Along with these common security concerns, this multi-tenancy platform pooling distributed computing resources has introduced novel security challenges that add to the existing ones [1]. Thus, this study analyses the security threats and defence mechanisms used to mitigate such threats in the cloud computing environment. This study scrutinises security threats associated with the cloud computing environment along with outlining threat-mitigating mechanisms.

3 Literature review

3.1 Threats to cloud computing

Although cloud computing is an advancement of several existing web services, it faces numerous similar and dissimilar security threats associated with other services on the web. Some of the major threats to cloud computing are presented in Fig. 2 and discussed here. Table 1 provides a brief empirical review of the threats to cloud computing.

3.1.1 Data breaches: In cloud computing, data from diverse users and organisations is stored in the cloud environment, and any breach into this environment is a potential attack on the data from all cloud users. Thus, the data stored, processed, or shared in the cloud environment is a target of very high value. This includes breaches due to human negligence or error, targeted malicious attacks, vulnerabilities associated with cloud applications, and other shortcomings of security policies in threat detection, vulnerability mitigation, security intelligence, and many more [11,15].

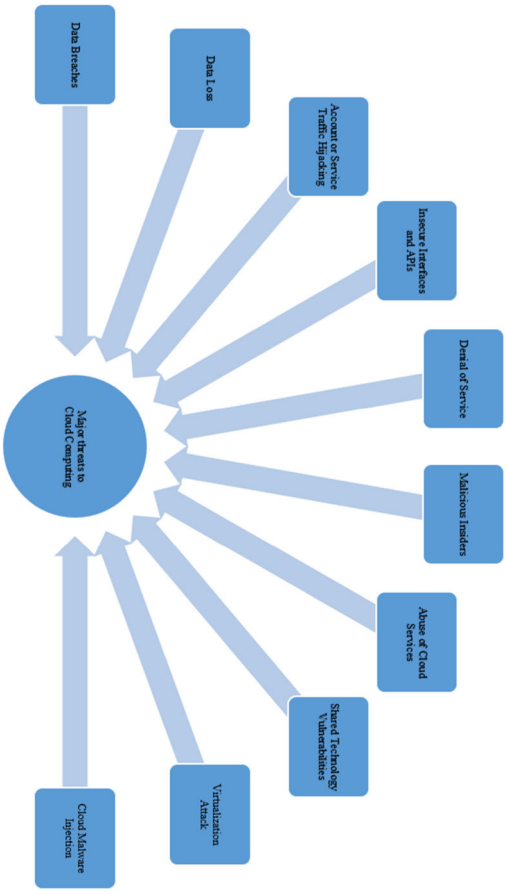

Fig. 2 *Major threats in cloud computing*

3.1.2 Data loss: Among the major risks associated with using the cloud, the loss of data is the prominent one. There are several ways that data can be compromised, including the deletion and alteration of the original content. Loss of data due to a virus or malware affecting hardware, backup storage, and data recovery are fatal in the cloud environment. The loss of data can also occur due to natural disasters, power failure, human error, and hard drive failure [2, 16].

3.1.3 Account or service traffic hijacking: Hacking of sensitive information related to accounts and services by cybercriminals or hackers has the same risks faced by countless other web services. Private information, such as financial records, pictures, credit card numbers, and more can be broadcasted, used, or sold by hackers [3, 17–20]. This threat also entails a man-in-the-middle attack, social engineering manipulations, eavesdropping on activities, and malware/spyware invasion [10, 15].

3.1.4 Insecure interfaces and application programme interfaces (APIs): Insecure interfaces, APIs, and virtual machines (VMs) are also a potential threat to the cloud computing environment. APIs, VMs, and other software interfaces are used by the user to gain access to cloud services [21, 22]. These points of contact are central components as they provide activity monitoring, management, and provisioning [23]. Thus, security flaws at these points lead to false access controls, illegal authentication, breach of encryption etc. These risks arise due to feeble API credentials, failure in key management, bugs in the operating system (OS), unpatched software, and hypervisor bugs [11, 24].

3.1.5 Denial of service (DoS): Under a DoS attack, the network is flooded with spam by the attacker, which creates useless traffic with the aim of exhausting resources [18, 25]. This situation can further lead to the unavailability of resources and services to authentic users [26]. This attack can occur due to weak network security architecture, vulnerable applications, insecure network protocol etc. [4, 16].

3.1.6 Malicious insiders: Security threats can also be internal to the cloud environment, and these are a bit harder to prevent. Any sensitive information can be copied to a storage device by any insider/employee having administrative access [21, 22]. The information can be stolen by any former disgruntled employee, system administrator, business partner, or third-party contractor [27]. Such risks can be limited by conducting proper background checks and limiting access to confidential data [2].

3.1.7 Abuse of cloud services: The cloud provides its users with an illusion of limitless computing capability, network resources, and storage capacity. Spammers, malicious code writers, hackers, and other cyber criminals can nefariously use such capabilities for password or encryption key cracking, bottlenecking the network, hosting malicious data, and many more [28]. This threat can arise due to a lack of proper monitoring and service level agreement in the cloud environment [10, 11].

3.1.8 Shared technology vulnerabilities: Cloud computing is a scalable technology for sharing infrastructure, technology, and resources. This multi-tenant platform uses a hypervisor to facilitate access to the guest OSs [29]. However, there are licensing and restriction shortcomings with hypervisors that can allow an inappropriate level of access and control to intruders. This threat can also arise due to vulnerabilities associated with VMs and third-party switching [11].

3.1.9 Virtualisation attack: Built-in virtualisation architecture necessitates individually constituted hardware and the best virtualisation is programmed with the lay on architecture [30]. With anomalies and adversaries in present-day OSs, vulnerabilities can be initiated to maliciously govern the host OS. As soon as the aggressor has the ability to regulate the host OS, the hypervisor is principally marked as an anomaly [31]. Thus, the command directorial rights of the hypervisor will permit the aggressor to execute any malevolent actions on any of the VMs accommodated by the hypervisor.

3.1.10 Cloud malware injection: Cloud malware injection attacks (CMIAs) are executed to gain access to the operator's data, which is stored and processed in the cloud [32]. Some of the most widely practiced CMIA threats are cross-site scripting attacks and structured query language (SQL) injection attacks. Such attacks are possible due to vulnerable cloud service providers such as the OpenStack cloud platform [33]. With the assistance of a malevolent cypher, adversaries can easily deliver scrambled information from a buffer by misusing a design flaw in present day mainframes [34]. See Table 1, which reviews the threats to cloud computing.

3.2 Defence mechanisms for threats to cloud computing: an empirical review

This section provides a short empirical review of the defence mechanisms for countering threats to cloud computing, which is presented in Table 2.

4 Research methodology

This study scrutinises the security threats associated with the cloud computing environment. Along with this, the existing threat mitigating mechanisms used in the cloud environment are also discussed. This work follows a descriptive and explanatory study approach that includes a survey analysis methodology. A descriptive approach is useful for describing the research phenomenon, situation, or group of individuals [36]. Furthermore, this approach aides the researcher in identifying the existing reality in regard to the theme of the study while the explanatory approach detects the significant variables that explain the aim of the study [36]. Therefore, the explanatory approach will detect security threats associated with the cloud computing environment and measures to overcome these threats.

Table 1 Brief empirical review for threats in cloud computing

Author name and year	Aim of paper	Findings
Sharma *et al.* 2019 [2]	this study had audited security for data storage in cloud computing	this study uniquely combined random masking and public key-homomorphic authenticator for privacy preservation of public data in the cloud. The proposed scheme was highly efficient and provably secure.
Saha *et al.* [3]	this study had compared three cloud service models to investigate cloud security threats and risks in the cloud environment	this study identified security flaws and vulnerabilities in the cloud, namely abuse of cloud resources, data breaches, and external security attacks as well as had proposed countermeasures for these security breaches
Ahmat 2015 [10]	this study had discussed key evolving threats for cloud services	this study addressed security risks such as hacking of information, insider attack, lack of adherence to security standards, data loss and segregation privacy concerns and more
Suryateja 2018 [11]	this study aimed to provide an overview of various threats and vulnerabilities in cloud computing	this study evaluated security risks in cloud computing such as data breaches or losses, DoS, weak authentication management, lack of due diligence, advanced insistent threats, insufficient security measures, ransomware, spectre etc.
Senyo *et al.*, 2018 [12]	aimed at synthesising the present literature to counsel that why an additional holistic approach of data security management is required in a management context	the study addresses the following issues 1. the study suggests that management role should be considered in information security management 2. it provides a holistic perspective on cloud computing analysis over the years. This data has found out areas that require additional analysis efforts such as the use of frameworks and methodologies 3. it provides insights into application domains that have used cloud computing and those who will use the cloud in the coming time. Intrinsically practitioners in these domains will use this data to revamp their business processes so as to acquire the advantage of cloud computing. Lastly, this study provides the inspiration towards a more robust understanding of cloud computing moreover as future analysis efforts
Khan and Al-Yasiri 2018 [13]	the study aimed to discuss major issues of cloud computing which include confidentiality, integrity, and availability	the study identifies 18 present and future, security problems, which affect various features of cloud computing. In this process of identification, this study found mitigation techniques to avoid such security problems. A security guide is developed that allows companies and institutions to be aware of security challenges, vulnerabilities, and techniques to elude them.
Parekh and Sridaran (2018) [14]	the study aimed to evaluate the requirements for cloud security and proposed a viable solution, which would eradicate major potential threats	this study mainly emphasise scrambling of data on cloud computing and aims at finding a solution for data security implementing second-level encryption and scrambling of data

4.1 Procedure of data collection and analysis

In consideration of the quantitative research approach, the primary source of data collection was a survey questionnaire. The questionnaire was conducted in a semi-structured format where the important questions were Likert questions. Additionally, an open-ended question was put forward to explore the mechanisms that can secure content in using cloud computing services. The questionnaire was administered to the employees of five cloud computing service providers in Delhi.

4.2 Sample size and participants

The questionnaire was targeted to collect the responses from 157 employees of five cloud computing service providers in Delhi using a simple random sampling method.

4.3 Measurement instrument and measures

The measurement instrument was a survey questionnaire that had a demographic and inferential part, which helped to determine the threats and defence mechanisms of cloud computing in their respective organisations.

The demographic section included information on age, gender, educational background, personal income, and work department. However, the inferential section comprised questions determining the threats and defence mechanisms to their cloud computing services. The questions in relation to determining the threats to using cloud computing services were based on a five-point Likert scale: strongly disagree, disagree, neutral, agree, and strongly agree. With this scale, the respondents' perspectives about different threats to cloud computing services were identified. Additionally, an open-ended question was put forward to explore the defence mechanisms that can secure the content in cloud computing services. The data collected were then statistically analysed using frequency analysis to attain the count statistics for description in order to understand how many respondents replied to a particular query. The collected data were numerically coded using MS Excel, which was then imported to the Statistical Package for Social Science version 21 for both descriptive and inferential analysis.

5 Data analysis and interpretation

5.1 Demographic profile

Out of the 157 respondents, 77% of the respondents were male and the rest were female. About 47% of the respondents belonged to the age group of 30–40 years. Furthermore, in terms of educational qualification, 50% of the respondents were graduates. There were mixed responses as to the monthly income of the respondents. About 36% of the respondents were earning Rs. 20,000–25,000. Lastly, in regard to the work department of the respondents, 38% of the respondents were from the information technology (IT) department. Overall, it is indicated from the survey that the respondents were from a middle-age group level and earned a fair monthly income. Additionally, these respondents were fairly educated and mostly from the IT department (Fig. 3).

Table 2 Empirical review for defence mechanisms for threats of cloud computing

Author and year	Findings	Defence mechanisms
Potey and Sharma (2013) [24]	this study highlighted and categorised various security risks associated with the cloud environment. Risks, threats, and vulnerabilities associated with the cloud were surveyed. Additionally, potential countermeasures for these threats were discussed here.	this study provided remediation for all the discussed threats, such as the prohibition on sharing account credentials, use of back-up and retention strategies, strong API access control, blackout monitoring to name a few
Mahalkari *et al.* (2016) [35]	a detailed analysis of existing security issues and their remedial solutions used by many cloud service providers was presented in this study. This investigation had taken a layered approach to security concerns and defence mechanism for the vulnerable areas in the cloud architecture. However, this study had not included performance and overhead concerns in the investigation.	this study proposed a multi-layered cloud security approach called defence-in-depth.
Jyothis and Krishna (2014) [9]	this study compares various mitigation methods used for reducing the underlying security issues in the cloud computing environment. It had also analysed automatic defensive security mechanisms for both known and unknown malware security concerns.	a new method was proposed in this study for detecting intrusions in the distributed cloud architecture
Dey *et al.* (2019) [5]	the authors identified five major security and privacy features namely, integrity, confidentiality, accountability, availability, accountability, and preservability. Links between these attributes shed light on the vulnerabilities exploited by the attackers. This study also discussed threat models and existing defence strategies in the cloud environment.	this study discussed early detection, monitoring at control platform and service level, continuous system patching and more
Bhadauria and Sanyal (2012) [16]	along with discussing multifarious security and privacy issues in a cloud environment, this study also addresses issues related to server failures resulting in a DoS. This study had analysed various unresolved risks threatening cloud computing technology diffusion and adoption impacting its numerous stake-holders. This study provided security solutions for three basic cloud architecture namely, basic security, network level security, and application level security.	an adaptable approach was proposed for early threat detection that had two main components for blocking malwares and URL filtering. It had also proposed the use of multi factor authentication, IPSec, homomorphic token and such.
Iyengar and Iyengar (2015) [15]	this study proposed a layered load balancing approach for scrutinising the incoming traffic requests at different layers of cloud architecture to mitigate any attack. This model emphasised on detecting threats earlier to ensure the availability of the services. The proposed method had a high-success rate in detecting overload threats at the earlier layers of the architecture through constant monitoring and strict security protocol.	an Effective Layered Load Balance (ELB) mechanism was proposed in this study. It acted as a traffic range perception, authenticity prediction, restrain request management, overload diminishment, and instantaneous load balancing.

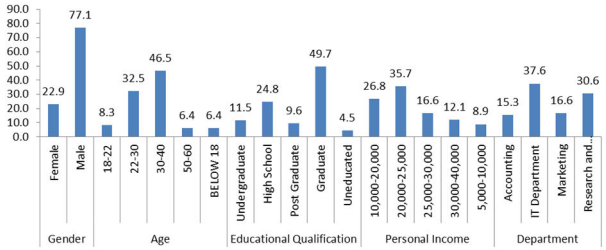

Fig. 3 *Demographic analysis*

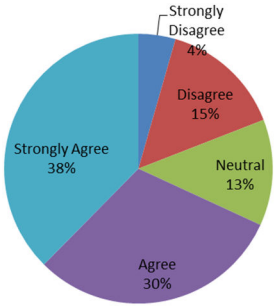

Fig. 4 *Benefits of cloud computing for business operations*

5.2 General background

Furthermore, this research also gathered general background data in relation to the theme of the study from the respondents of the survey and is presented below.

5.2.1 Benefits of cloud computing for business operations: Primarily, the respondents were asked whether cloud computing was beneficial for business operations. About 38% of the respondents strongly agreed that cloud computing methods were beneficial for the business operations of a company, whereas only 4% strictly disagreed with the notion of a beneficial impact. This can be attributed to the fact that most respondents were aware of the benefits of cloud computing in business operations and were using it, while those that strictly disagreed were quite unaware of it and might be using it for other purposes, such as entertainment.

In this regard, the authors of [37, 38] state that large and small companies have started adopting cloud computing technologies and this trend will continue in the following years. Furthermore, companies of all shapes and sizes will begin to adapt to cloud computing as this new technology is evolving like never before. Industry experts believe that this trend will only continue to grow and develop even further in the coming years (Fig. 4).

5.2.2 Advantages of cloud computing: Furthermore, respondents were asked about the advantages of the cloud computing services provided by their company. In this regard, ~44% of the respondents strongly agreed that cost-savings on hardware and outsourcing of non-core competencies were the major advantages provided under cloud computing. Other advantages include access to data anytime and anywhere, no up-front investments, and cost saving on software. Overall, it can be said that cloud computing reduces the cost of business operations and the outsourcing of non-core competencies. Moreover, data can be accessed from anywhere according to the needs of the user.

Apostu *et al.* [39] discussed that cloud computing is the most cost efficient technique in IT management. Additionally, compared to the traditional desktop, cloud computing is available at a much cheaper rate. Furthermore, one-time payment and other scalable options reduce the cost of using cloud computing (Fig. 5).

5.2.3 Challenges faced in adopting cloud computing: The respondents were also asked about the challenges they faced in adopting cloud computing services. Only about 13% of the

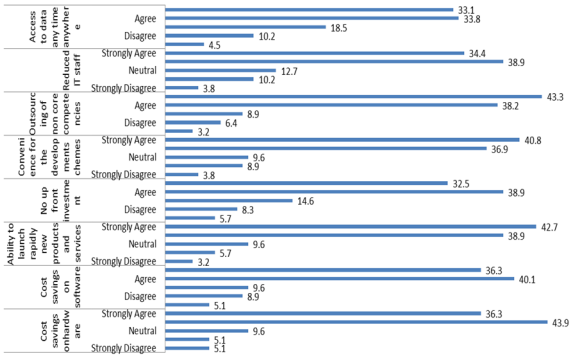

Fig. 5 *Advantages of cloud computing*

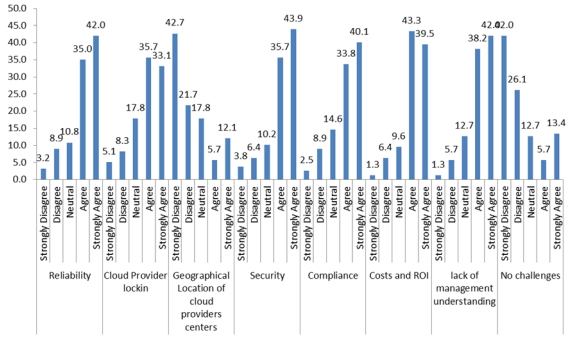

Fig. 6 *Challenges faced in adopting cloud computing*

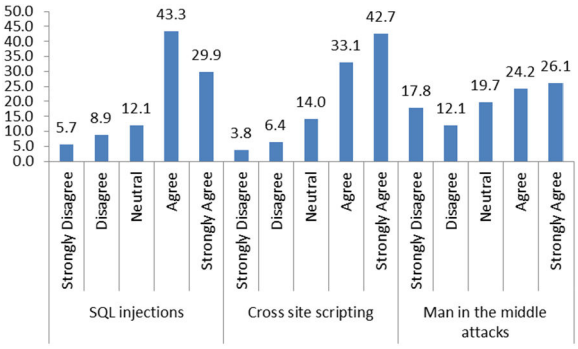

Fig. 7 *Basic security threats faced while using cloud computing*

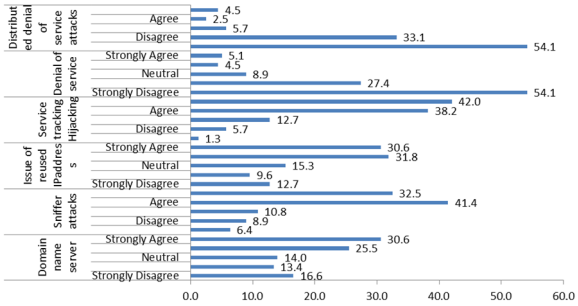

Fig. 8 *Challenges faced with respect to network security in cloud computing*

respondents strongly agreed that there were no challenges in adopting cloud computing services for business operations. Approximately 42% of the respondents strongly agreed with the fact that reliability and lack of management understanding is a major challenge. This means that the employees feared using cloud computing services because of the lack of in-depth knowledge among the management that, in turn, affects their usage. Furthermore, ~44% of the respondents thought that there were major security concerns while using cloud computing techniques. Overall, it can be said that the present cloud computing services are not very reliable and the inefficiency of proper management can act as a disadvantage, which can devalue such services.

In this regard, the study conducted by the authors of [28, 40] states that cloud computing works through heterogeneous resources and due to improper management some companies are not able to achieve success. The management of cloud computing should flow as a planned mechanism for the provision of resources in the cloud environment (Fig. 6).

6 Inferential analysis

This section analyses the main aim of the study, i.e. to assess the security threats and defence mechanisms of cloud computing. Frequency analysis is used to derive insight into this issue, followed by a discussion on defence mechanisms adopted to secure cloud computing from such threats.

6.1 Threats faced while using cloud computing

In the investigation of the threats faced while using cloud computing, this research accounts for the following few broad security threats: basic security concerned related to data breaches, network security, CAPTCHA breaking, Google hacking, and other threats (Fig. 7).

6.1.1 Basic security concerns related to data breaches: In regard to the security threats faced by the respondents using cloud computing services, about 43% of the respondents agreed that SQL injections and cross-site scripting were the major threats faced. Furthermore, there were mixed responses as to the threat of the man in the middle (MITM) attacks to cloud computing systems. These attacks breach the walls securing the content and lead to the loss of precious data.

The studies conducted by the authors of [41–43] reveal that among all types of malware injections, SQL injection is the most common. Hackers often target SQL databases or services and try to inject malicious code. Furthermore, the study conducted by Turab *et al*. [44] states that MITM attacks are one of the most popular means of hacking, as the hacker gains access to network traffic using routing and transport protocols, thereby leading to the theft of confidential information.

6.1.2 Network security: With respect to network security concerns, 42% of the respondents agreed that sniffer attacks were the most faced challenge to cloud computing services. This attack captures data through network traffic via a sniffer application. However, 54% of the respondents strongly disagreed that DoS and distributed DoS were not among the major security challenges faced. Furthermore, 31% of the respondents strongly agreed that domain name server (DNS) was a crucial concern regarding network security, as the name of the server returns the wrong internet protocol (IP) address to users that, in turn, divert the traffic thereby capturing the user's details. Therefore, it can be indicated that there is a major threat in terms of using webs flooded with traffic, especially in the form of applications. In this regard, the study conducted by Senthilkumar and Viswanatham [45] details that DNS attacks have increased the organisational risk in the cloud computing environment significantly in terms of harming user's personal details (Fig. 8).

6.1.3 CAPTCHA breaking and Google hacking: CAPTCHA breaking through image-based hacking is one of the other emerging challenges faced by cloud-based computing. About 38% of the respondents strongly agreed and 44% of the respondents agreed that CAPTCHA breaking is a threat faced when using cloud computing services. Furthermore, in the context of Google hacking, 41% also agreed that this hacking was frequently encountered by the respondents and negatively affected smooth business operations. The study conducted by Paul Rajan and Shanmugapriyaa [46] states that now spammers are easily able to break the CAPTCHA given by sites like Gmail and Hotmail. Spammers usually utilise the audio system to read CAPTCHA for their internet clients (Fig. 9).

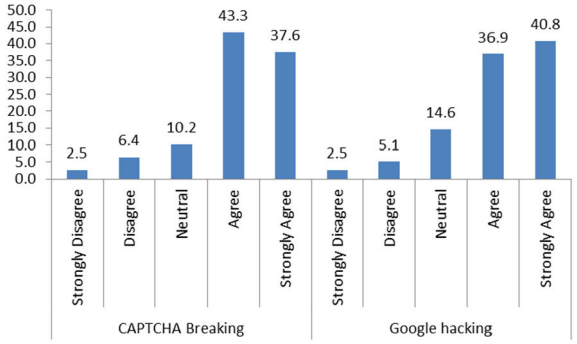

Fig. 9 *Challenges faced with respect to CAPTCHA breaking and Google hacking in cloud computing*

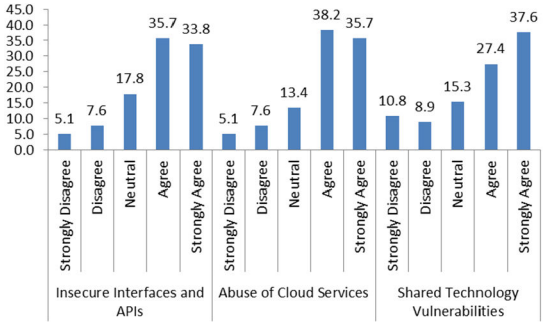

Fig. 10 *Other threats faced in cloud computing services*

6.1.4 Other threats: Apart from all the threats discussed above, the respondents were also asked about other threats faced in cloud computing services. About 34% of the respondents strongly agreed that insecure interfaces and APIs affect the smooth delivery of a cloud computing service. Furthermore, about 37 and 36% of the respondents, respectively, strongly agreed that the challenge of shared technology vulnerabilities and the abuse of cloud services are common challenges faced by the respondents. The studies conducted by the authors of [47–49] state that shared technology vulnerabilities make systems more prone to virus attacks, as well as to the loss of precious content (Fig. 10).

7 Defence mechanisms

Dissimilar to data breaches, DoS attacks etc., data loss [1] frequently occurs due to natural or man-prompted catastrophes as an outcome of the corporeal demolition of the servers or by a human mistake. Nevertheless, data loss can also be an effect of a beleaguered occurrence. Apart from the reason, the consequences are all identical: the enterprise may lose all of the records they have been accumulating for years. Some major reasons for such an anomaly are due to insecure APIs [50], insider anomaly, improper security monitoring, and auditing, and lack of a disaster recovery plan [51].

Furthermore, the threats linked to information removal occur for the reason that the end user has condensed reflectivity into where their information is tangibly kept in the cloud and a diminished capability to authenticate the confident omission of their data. The effect is worse when using infrastructure as a service [52] due to an operator's capability to provide resources or implement reprehensible actions that necessitate forensics [53] for malware/malicious action discovery.

Following the threats observed by the respondents in cloud computing services, next, this work addressed what defence mechanisms can be undertaken to secure the content. The researcher examined the responses for this section via an open-ended question from the respondents. Primarily, in terms of the data loss and data breaches, the respondents were of the view that there should be a two-way authentication process to protect the data. In addition, a few respondents suggested that the relevant service providers should incorporate robust passwords in order to restrict the access of attackers to the user's confidential information. Next, in terms of the threat of malicious insiders, many respondents stated that intrusion detection systems should be framed in a cloud network set up to monitor network traffic and nodes to detecting malicious activities. In addition, there were few respondents who highlighted using a file allocation table (FAT) to secure content from such malicious insider attackers. To this end, Gupta *et al*. [54] state that this solution creates a number of VMs by storing them at a particular location. The applications of the client can run through the FAT table and these instances are managed by the hypervisor.

To cope with a DNS attack, most of the respondents suggested using a domain system security extension [55]. This system would help to keep the access of the user confined to a web page so that no other individual can simultaneously invade it. Furthermore, in terms of the threat from sniffer attacks, a majority of the respondents stated that the companies should launch an encryption scheme such as the packet sniffer programme that codifies the information of users.

In this regard, the studies conducted by the authors of [29, 37, 43, 44] use a packet sniffer programme to put the network card of a computer into a promiscuous mode, which enables the computer to listen to the traffic. The packets are filtered on an IP header based on a certain set of criteria and ports in these packets. These networks can work for both wired and wireless networks.

8 Conclusion

Cloud computing is a valuable resource for the business operations of a company as this advanced technique offers access to data anytime and anywhere. Furthermore, as compared to traditional desktops, this technique saves costs on hardware and software. Therefore, this study is useful for both small and large companies in recognising the importance of cloud computing services in their business operations. Additionally, this study aids such companies to identify various challenges, threats, and the application of defence mechanisms in association with cloud computing services. Overall it can be found that there is a major threat in terms of data breaches via lack of management understanding of the use of cloud computing services, keeping in mind its defence mechanisms. Furthermore, there can be an abuse of cloud computing services that, in turn, affect not only the businesses' confidential data but also the personal identity and information of the user.

The growth of telecommunication and computer networks has brought some serious security concerns into the light. As the services of cloud computing are based on sharing and networking, security is one major problem in this system. Technically, cloud computing systems are prone to multiple attacks and hacking attempts that can majorly harm cloud computing service providers. Hackers are adopting innovative approaches to damage highly secured systems through malicious attacks.

Hackers will always develop new characteristics and features to make things work on their side. The operations and engineering systems are continuously working to secure these systems. However, hackers have acted intelligently enough to capture entire industrial and financial systems through attacks. Hackers apply innovative methods by characterising themselves as 'crackers, whackers, and samurais' in the way they intend to cause damage to the victim's information. The cloud computing system is flooded with multiple attacks, majorly including the DoS attacks, side channel attacks, CMIAs, and authentication attacks. Malware injection attacks severely harm the cloud system as hackers gain full control over the victims' data, in turn, exploiting the service to the cloud attack surface. Side channel attacks have also developed as the main threat to cloud computing systems as this attack is based on cryptographic algorithms. Furthermore, the DoS and authentication attacks have emerged due to high workloads in the cloud computing environment. In the context of these attacks, cloud computing services have observed a high frequency of attacks in the current year. The complexity of protecting security across domains is emerging as a challenge for cloud enterprises.

Apart from using various defence mechanisms to deal with such threats, organisations are also developing new training programmes for their employees. The employees are being trained to deal with

the innovative methods adopted by the hackers, but still, the organisations have not achieved efficiency in developing effective security mechanisms. The organisations need to focus on the effective management and monitoring of cloud services.

9 Acknowledgments

The authors would like to acknowledge the support of the Deanship of Scientific Research at Prince Sattam Bin Abdulaziz University under the research project no. 2017/01/7091.

10 References

[1] Jouini, M., Rabai, L.B.A.: 'A security framework for secure cloud computing environments', *Int. J. Cloud Appl. Comput. (IJCAC)*, 2019 **6**, (3), pp. 32–44 doi:10.4018/IJCAC.2016070103, https://www.igi-global.com/gateway/article/159836

[2] Sharma, A., Keshwani, B., Dadheech, P.: 'Authentication issues and techniques in cloud computing security: a review'. Available at SSRN 3362164, 2019

[3] Saha, M., Panda, S.K., Panigrahi, S.: 'Distributed computing security: issues and challenges. cyber security in parallel and distributed computing: concepts, techniques, applications and case studies, 2019, pp. 129–138

[4] Wani, A.R., Rana, Q.P., Pandey, N.: 'Analysis and countermeasures for security and privacy issues in cloud computing', in '*System performance and management analytics*' (Springer, Singapore, 2019), pp. 47–54

[5] Dey, H., Islam, R., Arif, H.: 'An integrated model to make cloud authentication and multi-tenancy more secure'. 2019 Int. Conf. on Robotics, Electrical and Signal Processing Techniques (ICREST), Dhaka, Bangladesh, 2019, pp. 502–506 https://ieeexplore.ieee.org/abstract/document/8644077/versions

[6] Alhenaki, L., Alwatban, A., Alamri, B., *et al.*: 'A survey on the security of cloud computing'. 2019 2nd Int. Conf. on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 2019, pp. 1–7

[7] Pitchai, R., Babu, S., Supraja, P., *et al.*: 'Prediction of availability and integrity of cloud data using soft computing technique', *Soft Comput.*, 2019, **23**, (18), pp. 8555–8562

[8] Lee, K.: 'Security threats in cloud computing environments 1'. 2012

[9] Krishna, G., S, J.T.: 'Defensive security mechanisms for cloud computing security risks – a review', *Int. J. Sci. Res.*, 2014, **3**, (2), pp. 73–75

[10] Ahmat, K.A.: 'Emerging cloud computing security threats'. arXiv, no. 1, 2015

[11] Suryateja, P.S.: 'Threats and vulnerabilities of cloud computing: a review', *Int. J. Comput. Sci. Eng.*, 2018, **6**, (3), pp. 297–302

[12] Senyo, P.K., Addae, E., Boateng, R.: 'Cloud computing research: a review of research themes, frameworks, methods and future research directions', *Int. J. Inf. Manage.*, 2018, **38**, (1), pp. 128–139

[13] Khana, N., Al-Yasiri, A.: 'Identifying cloud security threats to strengthen cloud computing adoption framework', *Proc. Comput. Sci.*, 2018, **94**, pp. 485–490

[14] Parekh, D.H., Sridaran, R.: '*Mitigating cloud security threats using public-key infrastructure*', in Bokhari, M., Agrawal, N., Saini, D. (Eds.): '*Advances in intelligent systems and computing*', vol. 729 (Springer, 2018)

[15] Iyengar, N.S.Ch.N., Ganapathy, G.: 'An effective layered load balance defensive mechanism against DDoS attacks in cloud computing environment', *Int. J. Secur. Appl.*, 2015, **9**, (7), pp. 17–36.

[16] Bhadauria, R., Sanyal, S.: 'Survey on security issues in cloud computing and associated mitigation techniques'. arXiv, 2012

[17] Baciu, I.E.: 'Advantages and disadvantages of cloud computing services, from the employee's point of view'. 2015, no. 13, pp. 95–101

[18] Potey, M.M., Dhote, C.A., Sharma, D.H.: 'Cloud computing – understanding risk, threats, vulnerability and controls a survey', *Int. J. Comput. Appl.*, 2013, **67**, (3), pp. 9–14

[19] Baker, P.M.A.: 'An overview of cloud computing and its capabilities!', *Sch. Syst. Eng.*, 2012, **18**, pp. 47–53

[20] Bisong, A., Syed, M.R.: 'An overview of the security concerns in enterprise cloud computing', CoRR, 2011, vol. 3, April 2012, pp. 30–45

[21] Claycomb, W.R.: 'Tutorial: cloud computing security', 2012

[22] C.A. Technologies: 'Protecting your APIs against attack and hijack with CA layer 7', February 2014

[23] Ahmed, H.: 'Cloud computing security threats and countermeasures', *Int. J. Sci. Eng. Res.*, 2014, **5**, (7), pp. 206–215

[24] Potey, M.M., Sharma, D.H.: 'Cloud computing-understanding risk, threats, vulnerability and controls: a survey', 2013

[25] Gunjan, K., Tiwari, R.K., Sahoo, G.: 'Towards securing APIs in cloud computing', *Int. J. Comput. Eng. Appl.*, **II**, (II), pp. 27–34

[26] Gu, Q., Liu, P.: 'Denial of service attacks' *Technical Report* (2012), vol. **3**, pp. 454–468 http://s2.ist.psu.edu/paper/DDoS-Chap-Gu-June-07.pdf

[27] Geer, D.: 'Malicious bots threaten network security', *Computer*, 2005, **38**, (1), pp. 18–20

[28] Ali, S.-H.-A., Ozawa, S., Nakazato, J., *et al.*: 'An online malicious spam email detection system using resource allocating network with locality sensitive hashing keywords malicious spam email detection system, incremental learning, resource allocating network, locality sensitive hashing', *J. Intell. Learn. Syst. Appl.*, 2013, **7**, (7), pp. 42–57

[29] Oluwabukola, O., Oludele, A., Ogbonna, A.C.: 'Issues in informing science and information technology a packet sniffer (PSniffer) application for network security in java'. 2013, vol. 10, pp. 389–400

[30] Zhang, Z., Cheng, Y., Nepal, S., *et al.*: 'KASR: a reliable and practical approach to attack surface reduction of commodity OS kernels'. Int. Symp. on Research in Attacks, Intrusions, and Defenses, Springer, Cham, 2018, pp. 691–710

[31] Abbasi, H., Ezzati-Jivan, N., Bellaiche, M., *et al.*: 'Machine learning-based EDoS attack detection technique using execution trace analysis', *J. Hardware Syst. Sec.*, 2019, **3**, (2), pp. 164–176

[32] Rakotondravony, N., Taubmann, B., Mandarawi, W., *et al.*: 'Classifying malware attacks in IaaS cloud environments', *J. Cloud Comput.*, 2017, **6**, (1), p. 26

[33] Ranjan, I., Agnihotri, R.B.: 'Ambiguity in cloud security with malware-injection attack'. 2019 3rd Int. Conf. on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, June 2019, pp. 306–310

[34] Hong, J.B., Nhlabatsi, A., Kim, D.S., *et al.*: 'Systematic identification of threats in the cloud: a survey', *Comput. Netw.*, 2019, **150**, pp. 46–69

[35] Mahalkari, A., Tailor, A., Shukla, A.: 'Cloud computing security, defense in depth detailed survey', *Int. J. Comput. Sci. Inf. Technol.*, 2016, **7**, (3), pp. 1145–1151

[36] Parker, I., African, S.: 'Chapter 6. Research design and methodology' in '*Methodology*'(2002), pp. 175–185 Transcript of CIMA address delivered at Glasgow University, 15 March

[37] Andrei, T., Jain, R.: 'Cloud computing challenges and related security issues', Available at http://www.cse.wustl.edu/~jain/cse571-09/ftp/cloud.…, 2009, pp. 1–10

[38] Abbadi, I., Lyle, J.: 'Challenges for provenance in cloud computing'. USENIX Workshop On Theory and Practice of Provenance (TaPP'11), USENIX Association, 2011

[39] Apostu, A., Puican, F., Ularu, G., *et al.*: 'Study on advantages and disadvantages of cloud computing - the advantages of telemetry applications in the cloud', Int. Conf. 13th, Appl. Comput. Sci. Morioka City, Japan, 2013, pp. 118–123

[40] Puthal, D., Sahoo, B.P.S., Mishra, S., *et al.*: 'Cloud computing features, issues, and challenges: a big picture'. Proc. 1st Int. Conf. on Computational Intelligence Networks (CINE 2015), Bhubaneshwar,India, 2015, pp. 116–123

[41] Xue, C.T.S., Xin, F.T.W.: 'Benefits and challenges of the adoption of cloud computing in business', *Int. J. Cloud Comput. Serv. Archit.*, 2016, **6**, (6), pp. 01–15

[42] Khalil, I., Khreishah, A., Azeem, M.: 'Cloud computing security: a survey', *Computers*, 2014, **3**, (1), pp. 1–35

[43] Kumar, S.V.K., Padmapriya, S.: 'A survey on cloud computing security threats and vulnerabilities', *Int. J. Innov. Res. Electr. Electron. Instrum. Control Eng.*, 2014, **2**, (1), pp. 622–625

[44] Turab, N.M., Abu, A., Shadi, T.: 'Cloud computing challenges and solutions', *Int. J. Comput. Netw. Commun.*, 2013, **5**, (5), pp. 209–216

[45] Senthilkumar, S., Viswanatham, M.: 'ACAFD: secure and scalable access control with assured file deletion for outsourced data in cloud', *J. ICT Res. Appl.*, 2014, **8**, (1), pp. 18–30

[46] Paul Rajan, A.R., Shanmugapriyaa, S.: 'Evolution of cloud storage as cloud computing infrastructure service', *IOSR J. Comput. Eng.*, 2012, **1**, (1), pp. 38–45

[47] Oyegoke, F.A.: 'Security challenges of cloud computing for enterprise usage and adoption', *IOSR J. Comput. Eng.*, 2014, **15**, (5), pp. 57–61

[48] Office, T., Coordinator, N., Technology, I.: 'Key privacy and security considerations for healthcare application programming interfaces (APIs)', December 2017

[49] Of, O.: 'Information application programming interface (API) enterprise design pattern table of contents', August 2018

[50] Shyam, G.K., Doddi, S.: 'Achieving cloud security solutions through machine and non-machine learning techniques: a survey', *J. Eng. Sci. Technol. Rev.*, 2019, **12**, (3), pp. 51–63

[51] Mendonca, J., Andrade, E., Endo, P.T., *et al.*: 'Disaster recovery solutions for IT systems: a systematic mapping study', *J. Syst. Softw.*, 2019, **149**, pp. 511–530

[52] Madni, S.H.H., Latiff, M.S.A., Ali, J.: 'Hybrid gradient descent cuckoo search (HGDCS) algorithm for resource scheduling in IaaS cloud computing environment', *Cluster Comput.*, 2019, **22**, (1), pp. 301–334

[53] Atamli, A., Petracca, G., Crowcroft, J.: 'IO-Trust: an out-of-band trusted memory acquisition for intrusion detection and forensics investigations in cloud IOMMU based systems'. Proc. 14th Int. Conf. on Availability, Reliability and Security, New York, NY, USA, August 2019, **45**, pp. 1–6 DOI: https://doi.org/10.1145/3339252.3340511

[54] Gupta, G., Laxmi, P.R., Sharma, S.: 'A survey on cloud security issues and techniques', *Int. J. Comput. Sci. Appl.*, 2014, **4**, (1), pp. 125–132

[55] Andersson, K., Tekniska, H., Montag, D.: 'Development of DNS security, attacks and countermeasures', Semantic Scholar, 2007