Journal of Mines, Metals and Fuels, 71(1): 464-472; 2023. DOI: 10.18311/jmmf/2023/33760

Print ISSN : 0022-2755

Journal of Mines, Metals and Fuels

Contents available at: www.informaticsjournals.com/index.php/jmmf

Cloud Computing in a Realm of Ever-Increasing Diverse Consumer Expectations Towards Security Challenges that Impact Consumer's Loyalty: A Data Driven Approach

Rajendra P[1*] and Mohanasundaram T[2]

Research Scholar[1], Associate professor[2], Department of Management Studies, Ramaiah Institute of Technology, Bengaluru, Karnataka, India 560054. E-mail: rajendra.scorpius@gmail.com[1*], tmohansun@gmail.com[2]*

Abstract

Cloud computing had become the new paradigm of the future, as it is the most widely used of all the technologies which are available, allowing consumers to readily maneuver their innovative digital demands. In this study, it is revealed that consumers' expectations are more inclined towards data security and challenges associated with it but, data storage location was not found too much of importance in consumers mind. Furthermore, terms of service agreement between consumer and cloud service provider with declaration of rights was found to be having an anchoring effect on consumer loyalty. This security level perception in consumers mind was a raised due threat created by cyber hackers, data leaks, data misuse and extortion that frequently happened now and then, these events had spurred negative security and threat perception in minds of consumers. The sample size used in the study for consumer survey is 147. The sample unit consist of consumers and employees working on cloud platforms, regular users of cloud services. Consumers are however expecting a robust security measures with more security practices and also expect more clarity in service agreements terms and conditions, as it clear from our study that 32.3% consumers tend to read those lengthy instruction manuals and also those long cloud service providers service agreements, due to which they end up with correct choices. Results confirms that addressing diverse consumer's expectation towards security challenges positively influences consumer's loyalty.

Keywords: *Cloud computing, security expectation, consumer loyalty, data, CSP, data location1.*

1.0 Introduction

Data is power and an impactful force in today's fast paced environment. The whole internet community relies on precise online data storage, data organisation, and data retrieval services. Cloud computing has grown in popularity as a technique of storing data due to the widespread availability of fast data transfer speeds offered by internet service providers. Data may include files, photos, documents, sometimes sensitive contents, music, videos and other types of media as well. Thanks to cloud computing that enables access of data from any location with good internet speed as a requirement. The two major objectives of the study are (i) to identify diverse variables that affect consumer loyalty in sphere of cloud computing and (ii) to map out varied consumer expectations towards data storage, service agreement with rights of use declaration and cloud service security challenges that affect consumer loyalty.

History of cloud computing has very interesting beginnings with altogether a metamorphosis kind of

[*]Author for correspondence

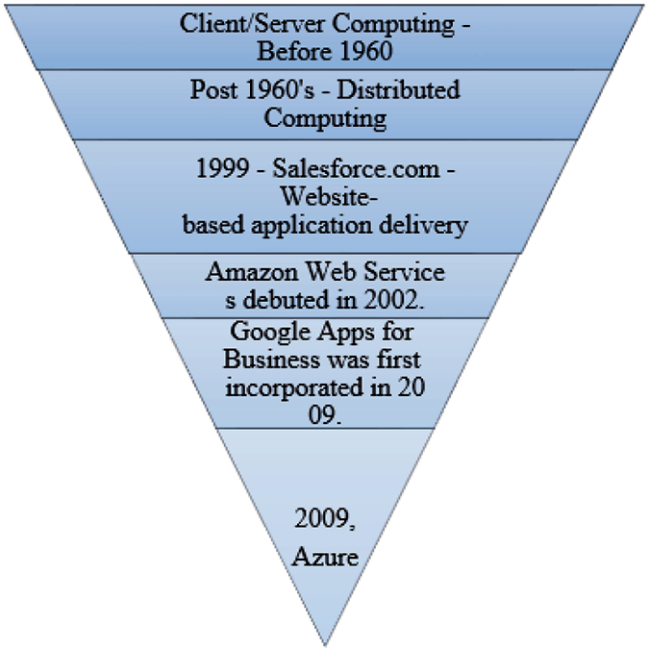

Figure 1: History of cloud computing

development. Prior cloud computing, there existed client/server computing, which was basically a primary backup, storage system in which all application programs, data, and controls were kept on the server side.

The next stage was the deployment of distributed computing, which involved connecting all computer systems and exchanging resources on demand.

After quite a lengthy period of gap, salesforce.com started selling software to users in 1999 via a simple website. The programmes were made available to companies over the World Wide Web, bringing the concept of computing as a value closer to reality.

Amazon Web Services (AWS) was founded in 2002 and lends storage, processing, and even human intelligence. However, until the Elastic Compute Cloud arrived in 2006, there was no really commercial service that was available to anyone.

Around 2009, Google Services started delivering commercial cloud computing solutions. Naturally, all of the big corporations are active in the rise of cloud computing, some earlier than others. Microsoft introduced Windows Azure in 2009, and others like Oracle and HP have subsequently joined the party. This indicates the widespread adoption of cloud computing.

Cloud computing has become main organ of every enterprise in today's digitally dominated sphere. One cannot fathom a day without cloud services from individual level till large IT and Non-IT establishments, as even an individual encounter's some form of his data which is already stored and interconnected with cloud servers with or without their knowledge. like for in case of simple google account and it's many productive cloud based Artificial Intelligent tools like google drive, google sheet, google photos and google forms etc. offers quick, reliable and freemium services with good security encryption. While cloud computing offers numerous benefits, such as enhanced data accessibility, efficient team communication, and speedier content management, it also has certain issues in terms of establishing consumer confidence in terms of safety and security.

Any company that seeks to defend its software and data from malicious hackers must invest in cloud computing security measures. Since the vast majority of businesses are now utilising cloud technology in some form or another, cloud security is paramount. Even during the Covid-19 pandemic, cloud computing proved to be a holistic contributor by saving lives. Furthermore, cloud computing services are utilised to store, audit, analyse, forecast, and explore a massive amount of patient data. This streamlines the onerous task of data processing while also benefiting mankind during these vital pandemic times[c].

It is evident that even during the global pandemic, cloud computing kept on its stupendous contribution towards healthcare patient data monitoring, which saved the lives of many. This is also a positive reinforcement which may create a strong trust towards the cloud computing concept itself from the consumers' end. The public cloud service is forecasted to grow by 20.4% in 2022[2]. It is important from the cloud service providers' perspective to deliver high safety and security services while storing the customer data in a cloud platform as it enhances customer loyalty. Thus in this paper, we intend to find out the consumers' expectations on cloud service providers in meeting the security challenges which in turn affects the consumers' loyalty towards the cloud service providers.

2.0 Literature Review

Security in cloud is most vital aspect as customers are more aware and their expectation toward data security keeps on growing, by and large this is because frequent cyber-attacks on cloud servers by a group of organised hackers in recent times. Security experts have discovered a widespread counterintelligence campaign carried out by a crime syndicate known as "APT10" (a.k.a. MenuPass, POTASSIUM, Stone Panda, Red Apollo, and CVNX). The attacks were concentrated at information and communication technology Solutions providers, which the organisation used as intermediaries to get intellectual property and confidential information from its targets. According to[3] a Wall Street Journal study, the cloud hopper cyber-attack was more broader than previously understood. It covers at least a dozen cloud providers, in conjunction with the 14 undisclosed

Table 1: Security requirements for individual users (Zissis & Lekkas, 2012)

Hierarchy	Service level	Consumers	Security requirements	Threats
Level of application	Software as a service (SaaS)	Beneficiary refers to a person or organisation that subscribes to a cloud provider's service and is responsible for its use.	• Anonymity and confidentiality in a multitenant setting • Exposed data protection (remnants) • Control over access • Shield over communication • Fortification of software's • All time quick service availability	• Unauthorized access • Data alteration at rest and in transit • espionage and destruction of data • Invasion of privacy and deception
Simulated Level	Platform as a service (PaaS) and Infrastructure as a service (IaaS)	A person or group who distributes software on a cloud infrastructure is referred to as a designer– developer-moderator.	• Protection for virtual clouds and authentication protocols for communications • Dominion over access and complete end to end encryption of application's hosted	• Application and software manipulation • Protection from data hijackers • Advance programing flaw detection • evaluation of traffic flow • Protection from DDoS attack by multiple machines - Distributed Denial of Service.
Physical Level	On-premise	The term "owner" refers to the person or organisation that owns the infrastructure on which clouds are installed, on their own physical premises.	• The usage of cloud computing must be legal and not harmful. • Hardware safe keeping and dependability • Network fortification	• Over-flooding of connections • DDoS protection from multiple computer hackers - Distributed Denial of Service

firms targeted in the indictment to gain access to the server, the hackers sent phishing emails to administrators with high-level access on occasion. Authorities claim that they also hacked into the networks of contractors. Control over physical security is lost with the cloud model due to the sharing of computer resources with other businesses. There is no information or control over where the resources run. The business may have broken the law (risk of data seizure by a (foreign) government)[4].

As per[5] Table 1 it clearly maps out the security related diverse consumers expectations towards different service model and this can help cloud service provider with proper customer requirement profiling which can bridge the gap between consumer security level expectation and cloud service provider's security protocol offering, which ultimately leads to more accurate security related positive perception in subconscious of consumers that may lead to loyal consumers, as security is epitome requirement of any service delivered be it information Technology (IT) or Non IT.

Because of the complexity and dynamism of cloud services, the cloud environment requires considerably far beyond typical security solutions, that would not translate well to virtual servers[6]. Security will become a competitive differentiator in the cloud computing sector[7]. In order[8] to secure each Virtual Machine (VM) against attacks, a Cloud Computing system must include certain Intrusion Detection Systems (IDSs) and another issue with cloud computing is that the large volume of logs makes it difficult for network administrators to evaluate those effectively. The vast majority of cloud computing consumers have no clue where their data is stored[9]. Cloud storage[10] providers may provide a choice of solutions to satisfy the demands of most consumers while also encouraging rapid growth to augment consumer value. Watermarking and steganography were used to demonstrate that our combined data leakage detection system outperforms other existing data leakage detection algorithms[11]. Based on a comprehensive review of trust mechanisms, alternative approaches were recognised depending on several factors such as public image, Alternative ways were identified based on multiple elements such as public image, proof, certification, encryption, shared security keys, SLA verification, policies, and myriad of additional subjective and domain-specific

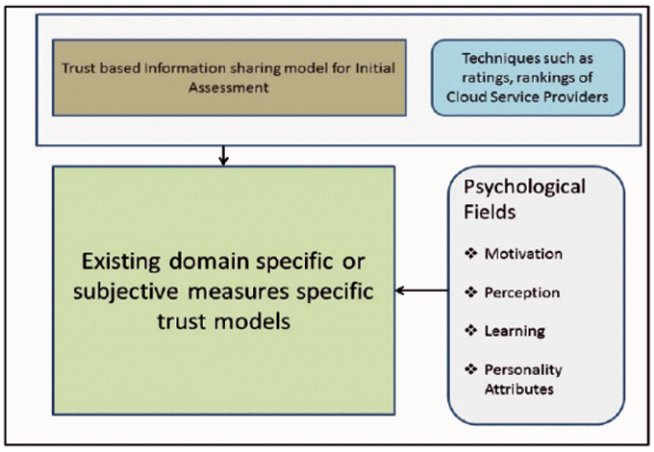

Figure 2: A trust model that reinforces faith on CSP(Aljumah & Ahanger, 2018)

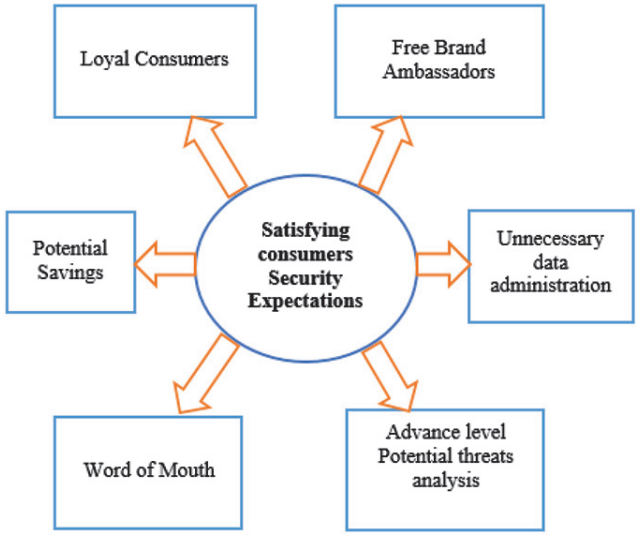

Figure 3: The benefits of cloud computing in terms of meeting consumers security requirements

features based on a complete analysis of trust mechanisms[12]. Trust on a CSP comes through consumers only when there is strong senses of psychological confidence towards good security measure provided.

The fog[13] computing paradigm has established new trends and heights in current networking and has surmounted the primary technological obstacles of cloud computing. This however does not replace cloud computing technology, but rather adds viable additional features to the present cloud computing paradigm. Not only does fog computing provide storing, network management, and virtual servers, but also functions as an Iot ecosystem (internet of things).

Through Figure 3 we can understand that just by meeting all consumers security expectation it may benefit CSP's in various aspects like consumer may become loyal, word of mouth marketing (positive feedback), reduces pointless data management and reduces cost associated with it, also potential cost savings coupled with forecasting of future security that may erupt, as when any consumer expectation is surveyed and their requirement matched one gets hold on loop holes in the process that can be patched-up to avoid future threats.

2.1 The Principal Components of Cloud Computing

Cloud computing has four distinct feature and one service model and one more deployment model as its architect, which is depicted in pictorial form in Fig.4.

In order to preserve our digital assets, the unpatched vulnerabilities connected with IaaS-based cloud computing must be examined[14]. Subscribers will indeed be unwilling to embrace PaaS systems to execute any important application unless they are regarded safe and reliable settings[15]. In SaaS more security mechanism is deployed at multi-level, as this entrusts consumers in enhancing their security perception, this is described graphically in Fig.5, Tenants' virtual machines are secured by a sophisticated intrusion detection system and an even more complex layer of remote attack detection, both of which are handled by the tenant security requirement manager[16].

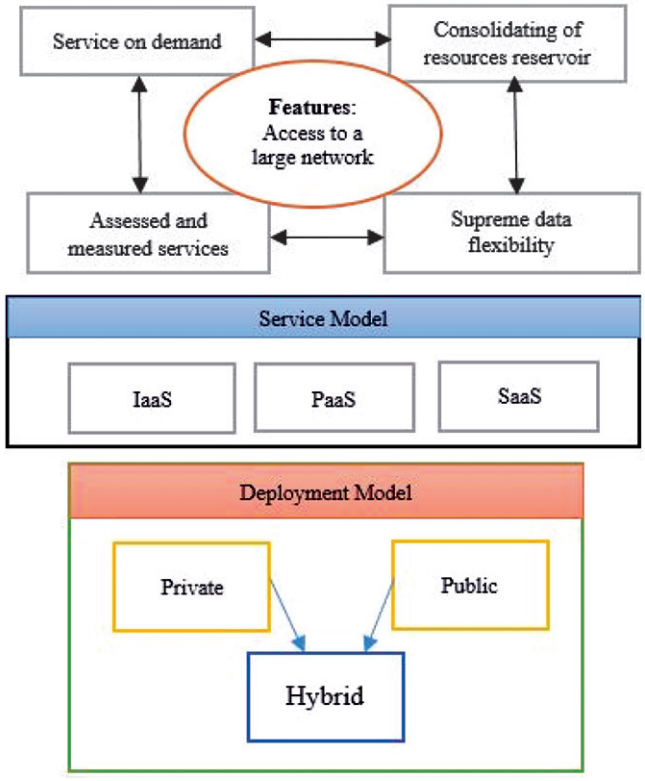

Figure 4: Features and Modes of cloud computing

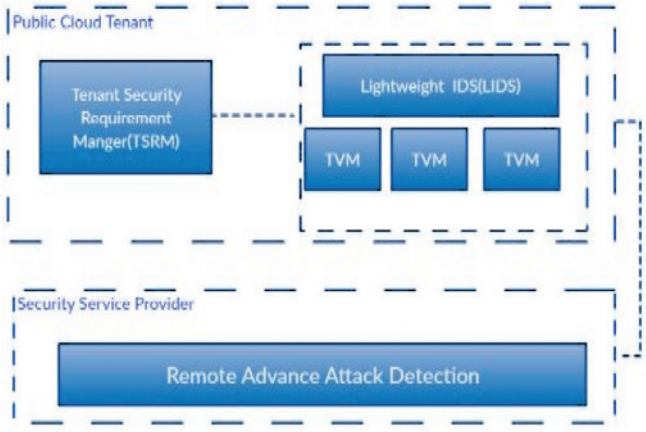

Figure 5: SaaS Saftey structural design (Hawedi et al., 2018)

2.2 Main facets of security threats

2.2.1 Harassment, victimisation and belligerent cloud exploitation:

Cyber attackers and unauthorised users get unrestricted access to cloud services, enables attackers to commit a range of cyberattacks such as password takeover, password bootlegging, and so on in exchange for a ransom payment. To circumvent such assaults, one can utilise hash functions, which are mathematical functions that are used in this approach to transform an input text to an alphanumeric string. This approach ensures that no two strings produce the same alphanumeric string, below is the equation for the same[17].

$$F(x) = \times \bmod 10 \quad \ldots (1)$$

2.2.2 Cloud related API security threats

APIs are used to communicate between the consumer and the CSPs (Application Program Interface). The cloud provider assures the consumer that security is built into the service model they utilise, as this is the core aspect because anything may happen if, API's security is compromised, which has detrimental directly on consumers cloud account or servers[18] this is a serious issue as any data pilferage happens with customer data causes adverse impact on consumer loyalty. Through Fig.7 we can see how different layers of attacks are possible for cloud API. Using this CSPs need to be watchful in mitigating those attacks beforehand.

2.2.3 Indistinguishable platform related Threats

Multiple customers can share the same programme, which may be operating on the same operating system, identical equipment, and the same location or even different ones doesn't matter to hackers, repository and consequently both the aggressor and the consumers are pooling the same hosts[19,21]. As a result, some consumers are apprehensive about migrating their systems from on premise to cloud. On-

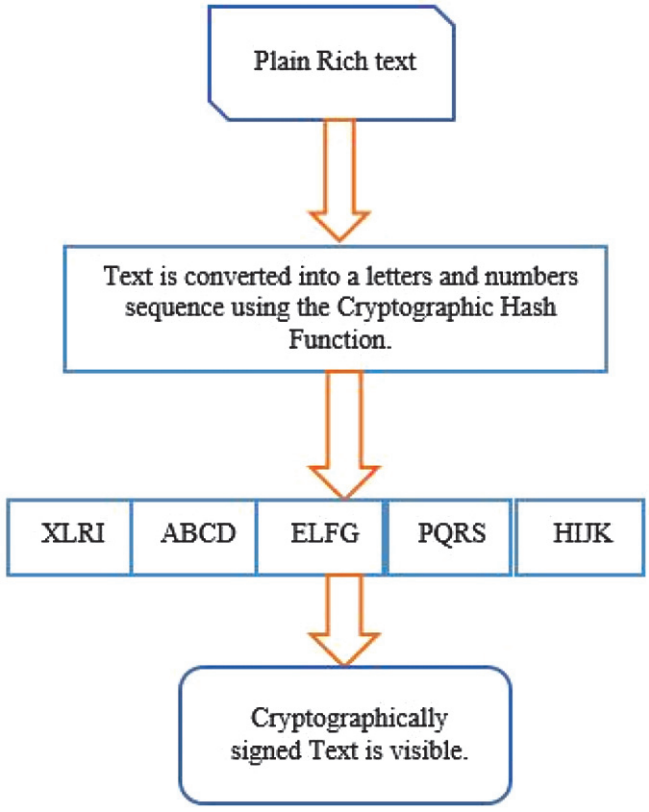

Figure 6: A cipher (cryptographic) mechanism in action to defeat cyber predators(Albugmi et al., 2016)

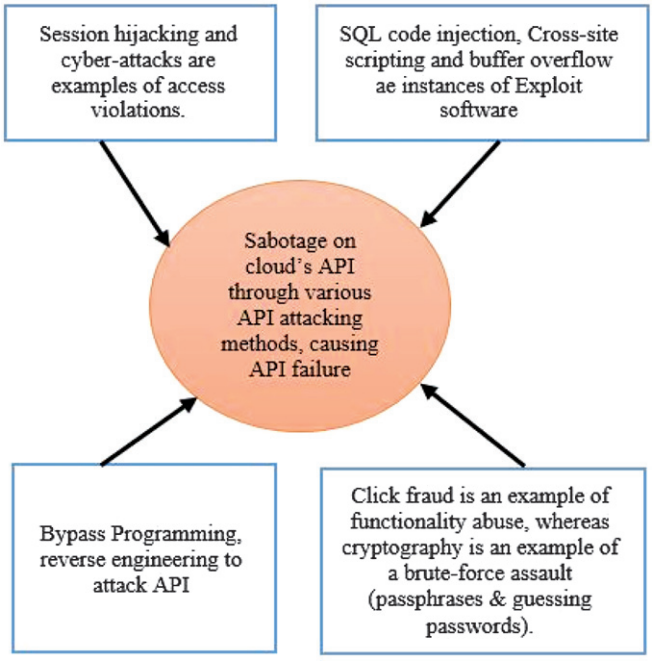

Figure 7: A cipher (cryptographic) mechanism in action to defeat cyber predators

premise is not inherently safer, but both have advantages and disadvantages, which ultimately raises customers' apprehension to employing increasingly new technology owing to their vulnerabilities.

2.2.4 Third party security related threat

Even though cloud computing services are provided remotely via the internet, unauthorised third-party access to cloud data might culminate in illegal behaviour[20-21]. There should be robust multilayer data encryption for 3rd party to not enter without permission.

2.2.5 Data burglary and blackmail

Data-related impacts, such as data loss or unauthorised access, have ramifications not just on system security but also on the protection of the individual affected personal data[22]. This is the most heinous of all assaults in which customers' or clients' data is hijacked and the client is blackmailed with dire consequences if the cyber-attackers' or hackers' unlawful demand is not met. As a result of this impact, many people have a strong aversion to internet-based services, as the cloud operates on the internet. This will have a negative influence on customer loyalty.

3.0 Research Methodology

A descriptive research study has been conducted to understand and analyse the impact of security challenges on consumer loyalty. We used inferential statistical analysis for making generalisations. The study uses judgement sampling technique. The respondents of the study are the employees of diverse industry who are directly or indirectly using advanced cloud computing in their respective work area on an everyday basis. The two major objectives of the study are (i) to identify diverse variables that affect consumer loyalty in sphere of cloud computing and (ii) to map out varied consumer expectations towards data storage and cloud service security challenges. A well-structured questionnaire has been designed and used for survey. The data has been collected from 147 respondents and the same has been included for the analysis after completing data cleaning processes. The data has been analysed using different inferential statistical analysis (both Parametric and non-parametric tests), one sample t-test test, ANOVA, and Multiple regression for making generalisations on the study. The results of the analysis are interpreted to arrive a meaningful conclusion about consumers divers expectations towards cloud computing and security challenges that impact consumer loyalty. In this study we have framed 3 hypotheses for proving our objective in terms of how ever-increasing diverse consumer expectations towards security challenges that impact consumer's loyalty, by drawing opinions from respondents.

Hypotheses 1: H_0. There is no significant impact upon consumer loyalty by disclosing security procedures and location of data on consumers.

Hypotheses 2: H_0: There is no significant difference among different age groups with respect to factors of terms and conditions defined by cloud service provider in service agreement which impact consumer loyalty.

Hypotheses 3: H_0: There is no significant relationship between the cloud computing server security aspects and total customer loyalty.

4.0 Analysis and Discussion

The study is initiated to empirically find out the effect of security challenges faced by both consumers and CSPs that affect consumers' loyalty.

4.1 Hypotheses 1

Null Hypotheses (H_0): There is no significant impact upon consumer loyalty by disclosing security procedures and location of data on consumers.

A one-tailed test is a statistical test in which the critical region of a dispersion is one-sided, meaning it is either bigger than or less than a given value. If the sample being tested falls into this critical region, the alternative hypothesis will be accepted instead of the null hypothesis.

Since P value is less than 0.01, the null hypotheses is rejected at 1% significance level with regard to statements on impact upon consumer loyalty by disclosing security procedures and location of data on consumers. Hence the opinion regard to statements on impact upon consumer loyalty by disclosing security procedures are not equal to average level. Based on mean score, Opinion regard to impact of consumer loyalty upon disclosing security procedures are above average level. This clearly demonstrate there should be proper mechanism in reporting location where the consumers data is store as it may greatly impact the loyalty displayed by consumer in longer run.

4.2 Hypotheses 2

Null Hypotheses (H_0): There is no significant difference among different age groups with respect to factors of terms and conditions defined by cloud service provider in service agreement which impact consumer loyalty.

One way ANOVA is so named because it is a strategy for determining if the means of two samples differ considerably (using the F distribution).

Since P value is less than 0.01, null hypotheses is rejected at 1% significance level Factors of CSP Terms and conditions. There is significant difference among different age groups with respect to factors of terms and conditions defined by

Table 2. T-test for specified value (Average=3) on security protocols and importance of disclosing location

Security protocols and importance of reveling location	Mean	Std. devation	T value	P value
CSP searching consumers data without their consent	3.57	1.31	5.273	0.000**
Duty of CSP to revel data storage location	3.99	0.92	12.978	0.000**
CSP compulsorily declare security protocol followed	4.19	0.99	14.601	0.000**
Depending on significance of data stored security level may be decided	3.92	1.07	10.410	0.000**
Respondent's belief – Makes no difference in security even after declaring security measures in action.	3.54	1.14	4.060	0.000**

Note: 1. ** indicates significance at 1% level
2. * signifies significance at 5% level

Table 3: ANOVA for significant difference among age group with respect to factors of terms and conditions defined by cloud service provider

Factors of CSP Terms and condition	Age Group in years						T-value	P-value
	20-25	25-30	30-35	35-40	40-45	Above 45		
It is right of consumer to know what happens with his data after transferring	3.50^{b} (0.51)	4.44^{c} (0.75)	4.80^{c} (0.41)	4.33^{c} (0.84)	3.50^{b} (1.15)	2^{a} (0.00)	18.859	0.000**
I do not believe in CSP's Terms and conditions	$3.25^{a,b}$ (0.85)	$4.15^{b,c}$ (0.85)	$3.20^{a,b}$ (1.50)	2.44^{a} (1.44)	2.50^{a} (1.54)	5^{c} (0.00)	10.231	0.000**
No need to declare CSP terms and condition, as I own the data	$3.50^{a,b}$ (0.51)	$4.15^{b,c}$ (0.86)	3.00^{a} (1.44)	$3.40^{a,b}$ (1.50)	4.50^{c} (0.51)	$4.00^{b,c}$ (0.00)	5.854	0.000**

Note: 1. The value within bracket refers to Standard Deviation
2.** symbolises a statistical significance of 1%
3.* represents significance value at 5%
4. Different alphabet among Age Group in years denotes significance at 5% level using Duncan Multiple Range test (DMRT)

cloud service provider which impact consumer loyalty. Based on Duncan Multiple Range Test (DMRT), the age group of 20-25 and 40-45 is significantly differing with age group of above 45 and 25-30 also with 30-35 at 1% significance level right of consumer to know what happens with his data after transferring with respect to all 3 Factors of CSP Terms and condition. This clearly signifies that there is different age group have different level of expectation and perception towards terms and conditions defined by cloud service provider in service agreement which impact consumer loyalty. Thus, using this CSPs have to tailor age wise different service terms and condition as per that age group wise diverse expectation toward service agreement declaration, as it has a substantial anchoring effect on long term consumer loyalty.

4.3 Hypotheses 3

Null Hypotheses (H_0): There is no significant relationship between the cloud computing server security aspects and total customer loyalty.

Multiple regression analysis is a powerful statistical technique that allows us to estimate the relationship between the dependent and independent variables. Further, it enables us to predict the dependent variable from two or independent variables.

Total customer loyalty

$$= \alpha + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 + \beta_5 X_5 + \beta_6 X_6 + e_t \quad ...(2)$$

Where,

X_1 = It is not necessary for a cloud service provider to allow clients to choose a separate specific location for data backup for security and safety reasons.

X_2 = Specific location back-up of data for safety and security purpose may depend on cloud service providers to allow client for making location choice.

X_3 = Possibility of CSPs unauthorized access towards stored client data

X_4 = Duty of CSPs to disclose location of a data storage

X_5 = Obligation of CSPs to declare the security measures

X_6 = Security measures depends on significance of client data

The result shows that the overall regression model is statistically significant. The R2 value 0.484 indicates that the model is reasonably well-fit. The model captures 48.4 per cent variation in the total customer loyalty that are explained by

Table 4: Multiple Regression model testing significance of CSPs security aspect linked consumer loyalty

H_0: There is no significant relationship between the Cloud computing server security aspects and total customer loyalty					
	ANOVA				
Model	Sum of squares.	df	Mean square	F	Sig. level
Regression	813.89	7	116.27	18.624	.000*
Residual	867.79	139	6.24		
Total	1681.68	146			
R^2	0.484			Adj. R^2	0.458
	Regression coefficients				
Variables	Unstandardized coefficients		Standardized Coefficients	t-value	Sig. level
	Beta	S.E.			
C	8.029	1.653		4.857	0.000**
X_1	1.360	.222	.519	6.136	0.000**
X_2	-1.035	.231	-.367	-4.477	0.000**
X_3	-.840	.207	-.325	-4.050	0.000**
X_4	-.121	.292	-.033	-.414	0.679
X_5	.633	.276	.184	2.298	0.023**
X_6	.324	.258	.102	1.257	0.211

Dependent variable: Total Customer Loyalty; ** Significant at 5 per cent level.

the chosen variables. Among the seven independent variables included in the study, only two variables viz., Duty of CSPs to disclose location of a data storage and security measures depends on significance of client data are not statistically significant. Thus, the security aspect variables are proved to be significantly influencing the total customer loyalty. The positive and statistically significant coefficient of X1 implies that the cloud service provider's decision not to enable customers to pick the site for backup for safety and security reasons has an impact on overall customer loyalty. The negative and significant coefficient of X2 indicates that cloud service providers' decision to enable consumers to choose their own location is solely at their discretion, which has a negative impact on customer loyalty. As a result, consumers are faced with a dilemma when it comes to selecting a CSP. The negative and significant co-efficient of X3 indicates that unauthorised access to stored client data by CSPs has an adverse impact on consumer loyalty. This in fact clearly portrays that brand switching will surface when unauthorized access to their stored data. The obligation of CSPs to declare the security measures (X5) have significant positive effect on total customer loyalty. The CSPs' disclosure of security measures will increase the customer's trust and loyalty to the CSP.

5.0 Conclusions

Cloud computing is the result of the convergence of numerous major technology disruptors that have grown and seasoned through time. Cloud computing has the ability to save businesses money, but it also poses noteworthy security risks associated to it by default which is unescapable, as any technology will have some or the other loopholes in its architecture, that which is being illegally exploited by cyber attackers with malicious intention. Enterprises using cloud computing technology to reduce costs and boost profitability should carefully consider the security risk of cloud computing, since it is a factor which is directly tangled to user data security and long term client's loyalty. In this study we conclude that consumer's expectation toward security challenges of CSPs have a direct impact on consumer's loyalty, as many level of data related security threats are to be addressed by CSPs which might increase consumer retention and magnify amount of loyal consumers. However, data storage location received a neutral reaction from customers, indicating that data storage location had neutral influence on consumer loyalty. Furthermore, customers were more likely to want to know what degree of security methods were used to protect their stored or hosted data. 32% of consumers strongly agreed that investing

in the cloud was a great move for and 67% felt that strong encryption standards have a direct influence on consumer loyalty. Customer loyalty is overshadowed by reliability and security of CSPs. Cloud service providers' proactive and customer-centric practises will go a long way toward preventing consumers from switching brands.

6.0 References

1. Singh, R. (2021): Cloud computing and Covid-19. 2021 3rd International Conference on Signal Processing and Communication, ICPSC 2021, 552–557. https://doi.org/10.1109/ICSPC51351.2021.9451792
2. Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly $500 Billion in 2022. (n.d.). Retrieved May 28, 2022, from https://www.gartner.com/en/newsroom/press-releases/2022-04-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-500-billion-in-2022 (accessed May 28, 2022).
3. Rob Barry and Dustin Volz. (n.d.). Ghosts in the Clouds: Inside China's Major Corporate Hack. Retrieved May 23, 2022, from https://robbarry.org/assets/pdfs/Ghosts in the Clouds.pdf
4. Popoviæ, K., & Hocenski, •. (2010): Cloud computing security issues and challenges.
5. Zissis, D., & Lekkas, D. (2012): Addressing cloud computing security issues. *Future Generation Computer Systems*, 28(3), 583–592. https://doi.org/10.1016/J.FUTURE.2010.12.006
6. Vemula, D. H. L., Khichi, T., Murugesan, G., Valderrama-Plasencia, L., Salazar-Gonzales, M., & Ventayen, R. J. M. (2022): Role of cloud computing and its impact on consumer behavior in financial sector. Materials Today: Proceedings, 51, 2190–2193. https://doi.org/10.1016/J.MATPR.2021.11.146
7. Chen, Y., Paxson, V., & Katz, R. H. (2010): What's New About Cloud Computing Security? http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html.
8. Lee, J. H., Park, M. W., Eom, J. H., and Chung, T. M. (2011, February): Multi-level intrusion detection system and log management in cloud computing. In 13th International Conference on Advanced Communication Technology (ICACT2011) (pp. 552-555). IEEE.
9. Khan, A. W., Khan, M. U., Khan, J. A., Ahmad, A., Khan, K., Zamir, M., Kim, W. and Ijaz, M. F. (2021): Analyzing and Evaluating Critical Challenges and Practices for Software Vendor Organizations to Secure Big Data on Cloud Computing: An AHP-Based Systematic Approach. *IEEE Access*, 9, 107309–107332.
10. Vatsa, M., Rastogi, S., Tiwari, A., & Jain, S. (2021): Impacts of Cloud Computing in Digital Marketing. Proceedings of the 5th International Conference on Electronics, Communication and Aerospace Technology, ICECA 2021, 1170–1174.
11. Jyothi, R. N. S., Sireesha, J., Mahitha, A., Ruchitha, B. and Deepthi, E. (2022): Protection and Saving of Delicate Data by using Cloud Computing. 2022 International Conference on Electronics and Renewable Systems (ICEARS), 1660–1667. https://doi.org/10.1109/ICEARS53579.2022.9752329.
12. Alshammari, M. M. (2020): Psychological Dimensions in Trust-Based Models in Cloud Computing. Proceedings - 2020 19th Distributed Computing and Applications for Business Engineering and Science, DCABES 2020, 87–91. https://doi.org/10.1109/DCABES50732.2020.00031
13. Aljumah, A., & Ahanger, T. A. (2018): Fog computing and security issues: A review. 2018 7th International Conference on Computers Communications and Control, ICCCC 2018 - Proceedings, 237–239. https://doi.org/10.1109/ICCCC.2018.8390464
14. Hay, B., Nance, K., & Bishop, M. (2011): Storm clouds rising: Security challenges for IaaS cloud computing. Proceedings of the Annual Hawaii International Conference on System Sciences. https://doi.org/10.1109/HICSS.2011.386
15. Rodero-Merino, L., Vaquero, L. M., Caron, E., Muresan, A., & Desprez, F. (2012): Building safe PaaS clouds: A survey on security in multitenant software platforms. *Computers & Security*, 31(1), 96–108. https://doi.org/10.1016/J.COSE.2011.10.006
16. Hawedi, M., Talhi, C., & Boucheneb, H. (2018): Security as a Service for Public Cloud Tenants(SaaS). Procedia Computer Science, 130, 1025–1030. https://doi.org/10.1016/J.PROCS.2018.04.143
17. Albugmi, A., Alassafi, M. O., Walters, R., & Wills, G. (2016): Data security in cloud computing. 5th International Conference on Future Generation Communication Technologies, FGCT 2016, 55–59. https://doi.org/10.1109/FGCT.2016.7605062
18. Tiwari, P. K., & Mishra, B. (2012): Cloud computing security issues, challenges and solution. *International journal of emerging technology and advanced engineering*, 2(8), 306-310.
19. Ahmed, A.A., & Hussan, M.I.T. (2018): Adnaan Arbaaz Ahmed, B.Tech Scholar, Department of Information Technology, Guru Nanak Institutions Technical Campus. Guru Nanak Institutions Technical Campus, 7(4). https://www.researchgate.net/publication/33968866.
20. Albugmi, A., Alassafi, M. O., Walters, R., & Wills, G. (2016): Data security in cloud computing. 5th International Conference on Future Generation Communication Technologies, FGCT 2016, 55–59. https://doi.org/10.1109/FGCT.2016.7605062
21. Doshi, R., & Kute, V. (2020): A Review Paper on Security Concerns in Cloud Computing and Proposed Security Models. International Conference on Emerging Trends in Information Technology and Engineering, Ic-ETITE 2020. https://doi.org/10.1109/IC-ETITE47903.2020.37
22. Barona, R., & Anita, E. A. M. (2017): A survey on data breach challenges in cloud computing security: Issues and threats. Proceedings of IEEE International Conference on Circuit, Power and Computing Technologies, ICCPCT 2017. https://doi.org/10.1109/ICCPCT.2017.8074287.