Know What You're Doing: Understanding the Security (Mis)conceptions of Cloud Technology Workforce in Bangladesh

Mashiyat Mahjabin Eshita, Ishmam Bin Rofi, S M Taiabul Haque, Jannatun Noor
Department of Computer Science and Engineering, BRAC University

1 Introduction

In the era of globalization, cloud computing plays a crucial role, often regarded as the digital nervous system, facilitating secure communication, storage, searching, retrieval, archiving, and processing [2, 9, 11–14]. The global cloud computing market, valued at $570 billion in 2022, rose to $678 billion in 2023 and is projected to reach $3 trillion by 2030, with a compound annual growth rate (CAGR) of 20% from 2023 to 2030 [1]. Despite its widespread use, many developers still hold misconceptions about the cloud. While existing studies [18–20] have explored these misconceptions with various motivations, they have predominantly focused on the user perspective. The perceptions of those who work with the cloud regularly, at both deployer and developer levels, remain largely unaddressed.

Prior studies have been conducted with usages of cloud in e-governance, the misconceptions about infrastructure, and user perspective on cloud misconceptions in the Global North [2, 4, 20], however, the perspectives of the people involved in the cloud sector of the Global South, especially in Bangladesh, have not been explored in the current literature. In a developing country like Bangladesh, local providers like InterCloud, Aamra, Mir Cloud, Tirzok Cloud, BracNet, PacECloud, Square Informatix, Plexus, and EyHost make up only 7% of the market, while international vendors dominate 53% [1]. Moreover, as the perceptions can be varied, understanding the knowledge of the cloud technology workforce[1] is important to identify the privacy and security mechanisms of the understudied population of the Global South.

To address this research gap, we surveyed Bangladeshi cloud technology workforce from leading IT companies about their opinions, to understand their perceptions on cloud security and privacy. We found that most of our participants possess certain misconceptions with a varied range of convictions. Surprisingly, senior developers, DevOps engineers, and lead engineers who have been working in this field for a long time also believe in the same perceptions related to cloud computing and security. Moreover, we found that many of our participants remained neutral in their opinions, indicating a lack of proper knowledge of cloud security where definitive answers exist.

2 Methodology

In our study on security misconceptions related to cloud computing, we conducted an online survey involving 24 members of the cloud technology workforce in Bangladesh, selected via snowball sampling. The sample comprised cloud developers (n=2), DevOps engineers (n=6), software engineers engaged in cloud infrastructure design, development, and deployment (n=8), and cloud technology learners (n=8). These participants, affiliated with renowned companies in Bangladesh, possess substantial experience in cloud computing. Data was collected through a Google Form, with responses recorded on a 5-point Likert scale, and distributed via email and WhatsApp. Despite using snowball sampling, we ensured a diverse participant pool from various companies across Bangladesh. The penultimate question in our survey was a modified version of the first question to facilitate conflict analysis, thus enhancing data credibility. The survey received approval from the Institutional Review Board (IRB) of the authors' institution.

Questionnaire Design and Positionality. The survey questions were formulated using insights from the literature on the prevalent misconceptions, which we gathered from popular tech blogs [8, 10, 15, 16], as well as the substantial expertise of the authors. One of the authors possesses over a decade of hands-on engagement within the cloud technology sector, having guided teams in the design, development, implementation, and security of essential cloud infrastructures. Additionally, another author is a security expert and two other authors are actively learning and completed courses on cloud technology and security.

[1] Including cloud engineers, DevOps engineers, software developers specializing in cloud-linked applications, cloud-related interns/learners

Serial	Question	Response			Correct Answer
		Yes	No	Neutral	
1	What do you think about that, "The cloud is inherently Secure" ?	8 (33.3%)	8 (33.3%)	8 (33.3%)	Neutral
2	Do you think that " Cloud Security is Too Difficult to Maintain" ?	8 (33.3%)	9 (37.5%)	7 (29.2%)	No
3	Do you think that "More security tools implies better security" ?	11 (45.8%)	7 (29.2%)	6 (25%)	No
4	Do you think that "Clients are alone responsible for security? "	0 (0%)	20 (83.3%)	4 (16.7%)	No
5	Do you think that "Cloud visibility is complex due to the dynamic nature of cloud" ?	9 (37.5%)	5 (20.8%)	10 (41.2%)	Yes
6	Do you think that "Using a cloud security tool ensures total cloud security? "	3 (12.5%)	13 (54.2%)	8 (33.3%)	No
7	Do you think that "Attacker needs to launch a complex attack to breach cloud security?"	12 (50%)	5 (20.8%)	7 (29.2%)	No
8	Do you think that "Most often cloud is by default secure?"	7 (29.2%)	9 (37.5%)	8 (33.3%)	Neutral
9	Do you think that "Data stored in public cloud provides less security and anyone can access them? "	7 (29.2%)	11 (45.8%)	6 (25%)	No

Table 1: Summary of survey data

3 Findings

Our study revealed that a notable portion of the cloud technology workforce holds specific perceptions, while many others lack understanding of these concepts and therefore remain impartial. The outcomes of our analysis are outlined in (Table 1)[2], where we have presented our survey findings alongside their corresponding percentages. From our results, we noted that 33.33% of participants rejected the notion that the cloud is inherently secure. Conversely, 33% of participants affirmed the notion, while an equal percentage remained neutral.

In regards to the misconception that maintaining cloud security is challenging, 33% of participants agreed, while 37.5% of the technology workforce disagreed with the notion, and 29.17% remained neutral. Regarding the common belief that more security tools equate to better security, the majority (45.83%) agreed. Only 29.17% of the technology workforce refuted this belief, while 25% remained neutral. This indicates that many in the cloud technology workforce hold this misconception, revealing a notable lack of understanding and knowledge gap regarding cloud security maintenance.

When questioning the technology workforce about their understanding of the shared responsibility model, we found a positive response. None agreed that clients alone are responsible for security; instead, 83.33% denied it, with only 16.67% remaining neutral. However, responses were less promising regarding the dynamic nature of cloud security. While 37.5% correctly acknowledged its complexity, 20.83% provided incorrect answers, and a significant 41.17% remained neutral, indicating a lack of understanding about cloud dynamics and security.

When questioned about the belief that cloud security tools guarantee complete security, the majority of the technology workforce (54.17%) rejected this notion. However, 12.5% believed it, and 33.33% remained neutral, indicating a misunderstanding of cloud security measures. We also inquired if participants thought attackers needed to execute complex attacks to breach cloud security. Approximately 50% of the technology workforce believed this, while only 20.83% disagreed, and 29.17% remained neutral. Finally, we asked our participants whether they believed that public clouds are less secure than private ones. Here, 29.16% of the technology workforce believed in the concept, while the majority (45.83%) rejected this concept, and 25% of the technology workforce remained neutral.

4 Discussion and Future Work

We acknowledge the limitation of our sample size. Additionally, response bias may be attributed to self-reported data. In the future, we plan to recruit more participants from the burgeoning cloud technology workforce in Bangladesh [1] to conduct a more comprehensive study. Despite these limitations, our findings offer valuable insights into the prevailing perceptions and beliefs regarding cloud security among cloud computing professionals in Bangladesh.

First, the findings indicate a lack of fundamental understanding among the individuals in the cloud sector, particularly regarding the intricacies of cloud security and associated tools, comprehension of cloud security mechanisms, and acknowledgment of the shared responsibility between users and developers in ensuring cloud security [6]. Moreover, our findings supplement the findings from prior research that reveal cybersecurity misconceptions among students [7, 18] and misconceptions regarding cloud office suites and cloud privacy and security in general [2, 3, 19, 20].

Next, our analysis connects with the prior studies [5, 19] that show the consequences of lack of clarity, including raising security challenges, ineffective implementations of models, and security concerns leading toward vulnerabilities and compromises where the primary security concern involves the physical infrastructure and the information owner sorting and processing data [17].

Our study indicates that cloud professionals in Bangladesh do not have a clear understanding of cloud security and privacy. This could potentially compromise the safety of the cloud environment for clients and make them vulnerable. Proper guidelines and comprehensive training are required to equip them with the necessary knowledge.

[2] In this table, "Yes" refers to responses of 4 or 5 on the Likert scale, "No" refers to responses of 1 or 2, and "Neutral" refers to a response of 3.

References

[1] Road To Smart Bangladesh. https://roadtosmartbangladesh.org/show/6/cloud-computing-is-transforming-business-%technology-in-bangladesh?dev_test. Accessed 24-05-2024.

[2] Angela Adrian. How much privacy do clouds provide? an australian perspective. *Computer Law & Security Review*, 29(1):48–57, 2013.

[3] Akhil Behl and Kanika Behl. An analysis of cloud computing security issues. In *2012 world congress on information and communication technologies*, pages 109–114. IEEE, 2012.

[4] Kelly W Bennett and James Robertson. Security in the cloud: Understanding your responsibility. In *Cyber Sensing 2019*, volume 11011, page 1101106. SPIE, 2019.

[5] Robert Anderson Keith Duncan and Mark Whittington. Enhancing cloud security and privacy: the power and the weakness of the audit trail. *Cloud Computing 2016*, 2016.

[6] Chunye Gong, Jie Liu, Qiang Zhang, Haitao Chen, and Zhenghu Gong. The characteristics of cloud computing. In *2010 39th International Conference on Parallel Processing Workshops*, pages 275–279. IEEE, 2010.

[7] SM Taiabul Haque, Tauhidul Alam, Mamoon Al-Rasheed, and Matthew Wright. Password construction and management strategies of the online users of bangladesh: A demographic comparison with the users of the first-world countries. In *Workshop on Human and Technology*, 2013.

[8] Guðrún Vaka Helgadóttir. Demystifying the myths about cloud security: What you need to know - awarego, July 2023.

[9] Farabi Fardin Khan, Nafis Mohaimin Hossain, Md Nazrul Huda Shanto, Sad Bin Anwar, and Jannatun Noor. Mitigating ddos attacks using a resource sharing network. In *Proceedings of the 9th International Conference on Networking, Systems and Security*, pages 1–11, 2022.

[10] Taylor Munsell. 7 cloud security myths debunked (and what's the truth), February 2024.

[11] Jannatun Noor, Hasan Ibna Akbar, Ruhul Amin Sujon, and ABM Alim Al Islam. Secure processing-aware media storage (spms). In *2017 IEEE 36th International Performance Computing and Communications Conference (IPCCC)*, pages 1–8. IEEE, 2017.

[12] Jannatun Noor and ABM Alim Al Islam. ibuck: Reliable and secured image processing middleware for openstack swift. In *2017 International Conference on Networking, Systems and Security (NSysS)*, pages 144–149. IEEE, 2017.

[13] Jannatun Noor, Md Sadiqul Islam Sakif, Joyanta Jyoti Mondal, Mir Rownak Ali Uday, Rizwanul Haque Ratul, Sriram Chellappan, and ABM Alim Al Islam. Sherlock in oss: A novel approach of content-based searching in object storage system. *IEEE Access*, 2024.

[14] Jannatun Noor, Saiful Islam Salim, and ABM Alim Al Islam. Strategizing secured image storing and efficient image retrieval through a new cloud framework. *Journal of Network and Computer Applications*, 192:103167, 2021.

[15] Sharon R. Cloud security myths vs facts: Top 12 myths - pingsafe blog, November 2023.

[16] David Spark. 20 of the greatest myths of cloud security, May 2023.

[17] Vassilka Tchifilionova. Security and privacy implications of cloud computing–lost in the cloud. In *Open Research Problems in Network Security: IFIP WG 11.4 International Workshop, iNetSec 2010, Sofia, Bulgaria, March 5-6, 2010, Revised Selected Papers*, pages 149–158. Springer, 2011.

[18] Julia D Thompson, Geoffrey L Herman, Travis Scheponik, Linda Oliva, Alan Sherman, Ennis Golaszewski, Dhananjay Phatak, and Kostantinos Patsourakos. Student misconceptions about cybersecurity concepts: Analysis of think-aloud interviews. *Journal of Cybersecurity Education, Research and Practice*, 2018(1):5, 2018.

[19] M Utin. From misconceptions to failure: Security and privacy in us cloud computing. 2015.

[20] Dominik Wermke, Nicolas Huaman, Christian Stransky, Niklas Busch, Yasemin Acar, and Sascha Fahl. Cloudy with a chance of misconceptions: exploring users' perceptions and expectations of security and privacy in cloud office suites. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*, pages 359–377, 2020.