Security and Privacy in Cloud Computing

Subjects: Computer Science, Information Systems
Contributor: Yunusa Abdulsalam

Advances in the usage of information and communication technologies (ICT) has given rise to the popularity and success of cloud computing. Cloud computing offers advantages and opportunities for business users to migrate and leverage the scalability of the pay-as-you-go price model. However, outsourcing information and business applications to the cloud or a third party raises security and privacy concerns, which have become critical in adopting cloud implementation and services. Researchers and affected organisations have proposed different security approaches in the literature to tackle the present security flaws. The literature also provides an extensive review of security and privacy issues in cloud computing. Unfortunately, the works provided in the literature lack the flexibility in mitigating multiple threats without conflicting with cloud security objectives. The literature has further focused on only highlighting security and privacy issues without providing adequate technical approaches to mitigate such security and privacy threats. Conversely, studies that offer technical solutions to security threats have failed to explain how such security threats exist.

Keywords: cloud computing ; security ; privacy ; privacy preserving

1. Introduction

The Internet service industry, including areas such as cloud computing, is an evolving paradigm for large scale infrastructure [1]. Cloud computing possesses the power to reduce costs by resource sharing and storage virtualisation, collectively merged with a provisioning mechanism that relies on a pay-as-you-go business architecture [2]. Cloud computing technologies such as Amazon's Elastic Computing Cloud (EC2), Simple Storage Service (S3) and Google App Engine have been the most popular in the software industry. Despite the impact and the efficient services these applications have offered, there are still security and privacy issues relating to how these cloud providers process users' data [3]. Issues arising because of insecure cloud computing platforms spread across different technological paradigms such as web-based outsourcing [4], mobile cloud computing [5] and service-oriented architectures (SOA). Secure cloud implementation demands an adaptive security mechanism to help users have a significant level of trust in the cloud. Without the ability of such techniques to guarantee a substantial level of security and privacy, there will continue to be a great fear of privacy loss and sensitive data leakage, which are significant obstacles and a deciding factors in the full adoption of cloud services [1].

Privacy is a fundamental human right that comprises the right to be left alone and demands the appropriate use and protection of personal information [6]. The implementation of cloud computing paradigms violates privacy in different ways, such as misappropriation of confidential information [7], uncontrollable use of cloud services, data propagation, potential unauthorised secondary usage, trans-border flow of data and dynamic provisioning. Other privacy concerns are data retention regulation, outsourced data deletion, and privacy awareness breaches [8]. In current practices, a consensus is typically achieved through a third-party service or by the general terms and conditions for personal data processing. The security and privacy issues become more complicated when granting user permission in an environment with minimal or no user interface due to unauthorised data usage permission and ineffective processing of personal information, which is often not considered during the designing phase. In terms of cloud security implementation, there are questions about data security policies for users in the cloud environment. Firstly, what are the commitments of Cloud Service Providers (CSPs) in establishing information security? Secondly, what data security policies have been published and made open to the public? The lack of clear justification has led to recent violations of privacy. In April 2019, Facebook Inc. was sued for a total of USD 5bn for Analytica privacy violations, making infrastructures for data security be under constant scrutiny to meet user privacy needs. Still, there has not been any clear direction for management support initiatives [9]. The authorisation process and access control mechanisms for data processing facilities have not been very efficient due to insider attacks generated from internal personnel. Most recently, organisations have been entrusting the security of users' confidential data to third-party access for security auditing, raising more security concerns on accountability of third-party. The best-case scenario is an honest but curious third party, which is still not suitable for real-life deployment [10]. Thirdly, what measures are defined to classify data access, and how can they be justified through third-party auditing? In granting

third-party access, organisations need to define a hierarchy for accessing data, and proper identity management for third-party access should be an essential task for every CSP [9]. Without appropriate identity management, an inside attack can occur by deploying malicious applications on edge nodes, exploiting vulnerabilities that affect the quality of service (QoS). Such hostile acts can significantly affect sensitive data temporarily saved on multiple edge routers.

As more organisations are moving to the cloud as an effective means of data storage, they need to share, process rapidly and disseminate a high volume of sensitive information to enhance effective decision-making [11]. However, a significant setback is the lack of security and privacy flexibility. Current security and privacy mechanism lacks the flexibility in responding to the changing external environment, which has led to an uncontrollable risk of data leakage. Organisations are concerned about stabilising cloud security infrastructures without depleting data leakage and information of users. Unfortunately, data storage services keep changing and, today, privacy can be individually defined—what might be private for an individual might be disclosed by some without concern. Therefore, there is a need to describe non-specific requirements when building privacy and security protocols for cloud computing. Strict privacy or security protocols will only be stagnant in the long run because technology and its resources are moving to the open world where everyone might decide what they choose to be private, especially in the cloud environment.

2. Cloud Computing Security

Cloud computing's diverse range of applications has drawn academic attention to security when it comes to data storing, management and processing [12]. Cloud computing brings open issues regarding the security and privacy of outsourced data. Due to its dynamic abstraction and scalability, applications and data outsourced to the cloud have unlimited security boundaries and infrastructure. Another primary security concern surrounding the adoption of cloud computing is its multi-tenancy nature and sharing of virtualised resources [10]. Cloud providers such as Google, Microsoft, and Amazon have recently accelerated their cloud computing infrastructure and services to support a more considerable amount of users [13]. Nevertheless, the issue of privacy and security will continue to grow because cloud databases usually contain important sensitive information [14]. The confidence level in adopting the cloud is dropping due to the threats analysed in **Table 1** and highlighted as follows [15].

Table 1. Cloud computing security vulnerabilities using STRIDE.

Vulnerability Component	Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
Immoral use and abuse of cloud computing		X	X	X	X	
Malicious insider attackers	X	X	X	X	X	X
Vulnerable programming interfaces		X		X		X
Data leakage and loss		X	X	X	X	
Distributed technology vulnerabilities	X	X				X
Services and account hijacking	X	X	X	X	X	X
Anonymous profile threat		X	X	X	X	

The symbol X denotes the existence of a STRIDE component.

3. Privacy Preservation through Access Patterns and Design

Privacy Process Patterns are specifically designed to model privacy issues effectively. They can be defined as patterns applied to privacy associated processes by specifying how privacy issues can be realised through identifiable procedures, connecting flows and the activities that link them. As supplementary, they assist software developers to understand how better to implement several privacy properties in a more precise manner. Privacy Process Patterns (PPP) are considered a more robust way to bridge the gap between user confidentiality and cloud service providers. Privacy Pattern Properties are defined as follows [16]

- *Anonymity* can be defined as a quality that does not permit the user to be identified in any form, either directly or indirectly. A problem that can arise when a user is anonymous is the issue of *Accountability* and a large anonymity set. The benefits include location tracking freedom, user's freedom of expression, and low user involvement. This property can be implemented using Tor [17], Onion routing [18] and DC-nets [19]

- *Pseudonymity* can be defined as the utilisation of an alias instead of personally identifiable information. A problem that can arise is the issue of *Integrity* [20]. The benefits include supporting user access to services without disclosing real identities. Users still maintain integrity protocol. This property can be implemented using administrative tools such as biometrics, identity management and smart cards.

- *Unlinkability* can be defined as using a service or resource with the inability of third-party linkage between the user and the service. Issue: *Integrity and Accountability*. Benefits: privacy-preserving by not allowing malicious monitoring of user experience. Implementation: Onion routing, Tor and DC-nets.

- *Undetectability* inability of third-party tracking amongst a set of possible users. Issues: undetectability strength is highly dependent on the size of the undetectability set. Benefits: preserve users' privacy without allowing detectability of service by malicious intruders. Secondly, attackers cannot adequately detect the existence of an exact Item of Interest (IOI), e.g., the use of steganography and watermarking. Implementation: smartcards and permission management, encryption methods such as mail and transaction encryption.

- *Unobservability* inability to perceive the existence of a user amongst a set of potential users. Issue: dependent on the integrity level and anonymity set. Benefits: anonymity and undetectability enforcement per resources. Secondly, ensuring user experience without the connection and observability of a third-party. Implementation: smartcards and permission management. Anonymizer services such as Tor, Hordes and GAP.

The literature has identified the need to introduce a Privacy by Design (PbD) to support the need for sensitive and confidential information stored, shared and distributed at the digital level [21][22][23]. From the literature, works are still in progress to define privacy design patterns in cloud computing. Developing a privacy pattern language will further assist developers in building the gap between the design and implementation phase. However, despite the works presented in the literature, there is still a gap between privacy design and implementation. Authors in [23] implemented and provided Privacy Process Patterns by Design that can be used to bridge gaps highlighted in the literature. The authors demonstrated the practicality of the application through JavaScript Object Notation (JSON) in conjunction with the Privacy Safeguard (PriS) methodology and applied them to a real case study. Further implementation of privacy access patterns was implemented by [21][22][24]. The challenges of Privacy by Design were highlighted by Diamantopoulou et al. as a factor of design and implementation of policies established by software engineers, as they lack a standard definition of privacy requirements and policies. Secondly, the lack of proper policy requirement knowledge for correct implementation. Therefore, there is a need to propose a set of Privacy Process Patterns that enhances the detailed understanding of cloud computing and a distinct coalition between cloud computing infrastructure and privacy requirements. The proper implementation helps support a privacy-aware technique in bridging the gap between user confidentiality and cloud service providers.

The authors of [23] successfully designed a set of privacy process patterns that can be used to bridge the gap between privacy design and implementation and their instantiation in several platforms without expertise or skill limitations. The authors argued that privacy should be controllable through access patterns and designs in that it allows secrecy preferences by a user. This helps users of the system be flexible when divulging Personal Identifiable Information [25]. Papanikolaou et al. [26] carried out extensive surveys on how to automate legal and regulatory processes to regulate and extract privacy rules. The idea is to apply a link policy and compliant techniques to provide salient means for maintaining and achieving user privacy in the cloud.

4. Conclusions

Considerations were made based on cloud computing security and privacy issues that demand self-adaptiveness. The multiple security threats posed by the security issues are depicted in **Table 2**. **Table 2** shows a need for control mechanisms that provide hybrid mitigation when designing security implementation for cloud infrastructure. For instance, attack mitigation and control mechanisms such as ML algorithms for detection and prevention are faster and more accurate due to the high probability of detecting attacks compared to similar approaches using homomorphic encryption schemes. ML systems can recover from an integrity loss on time, gaining sufficient awareness without substantial availability loss. Therefore, knowing the damage of an attack campaign and how feasible it can become requires a high awareness level.

Table 2. Cloud computing security and privacy component using STRIDE.

Security Component	Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
Accountability		X		X		X
Identity Management	X		X	X	X	
Data Integrity		X	X	X		X
Intrusion and Detection	X	X		X	X	X
Data Privacy		X	X	X		X
Access Control	X	X	X		X	X
Access Patterns and Designs		X	X	X		

The symbol X denotes the existence of a STRIDE component.

From the literature and trends of emerging technologies, the challenge in any system from the internet's critical infrastructures such as cloud computing is systems' ability to self-protect regarding security and privacy. Secure adaptive techniques are ubiquitous and can be adopted at any stage of an underlining technology, from hardware and software to the core computing infrastructure. Secure adaptiveness implies that the system can self-protect during multiple attacks or a malicious user exploring multiple vulnerabilities. Cloud computing will still be prone to security and privacy concerns without the practical adoption of adaptive mechanisms for efficient client and user experience. The observation from the study shows that most works in the literature have no consensus in the design and implementation of effective cloud security schemes, which means that security and privacy implementation in the literature does not balance integrity, accountability, and privacy. Furthermore, cloud models for privacy-preserving are not user-centric, creating no flexibility and control management over security or privacy protocols that maintain users' sensitive data.

References

1. Tari, Z. Security and Privacy in Cloud Computing. IEEE Cloud Comput. 2014, 1, 54–57.
2. Bentajer, A.; Hedabou, M.; Abouelmehdi, K.; Elfezazi, S. CS-IBE: A data confidentiality system in public cloud storage system. Procedia Comput. Sci. 2018, 141, 559–564.
3. Fernandez-Gago, C.; Pearson, S.; D'errico, M.; Alnemr, R.; Pulls, T.; de Oliveira, A.S. A4Cloud Workshop: Accountability in the Cloud. In Proceedings of the IFIP International Summer School on Privacy and Identity Management, Edinburgh, UK, 16–21 August 2015; pp. 61–78.
4. Azougaghe, A.; Oualhaj, O.A.; Hedabou, M.; Belkasmi, M.; Kobbane, A. Many-to-one matching game towards secure virtual machines migration in cloud computing. In Proceedings of the 2016 International Conference on Advanced Communication Systems and Information Security (ACOSIS), Marrakesh, Morocco, 17–19 October 2016; pp. 1–7.
5. Mollah, M.B.; Azad, M.A.K.; Vasilakos, A. Security and privacy challenges in mobile cloud computing: Survey and way ahead. J. Netw. Comput. Appl. 2017, 84, 38–54.
6. Warren, S.D.; Brandeis, L.D. The Right to Privacy Harward Law Review. In Ethical Issues in the Use of Computers; Wadsworth Publishing Co.: Belmont, CA, USA, 1890; Volume 4, pp. 193–220.
7. Deng, M. Privacy Preserving Content Protection (Privacy Behoud Content Protection); Faculty of Engineering—Katholieke Universiteit Leuven: Leuven, Belgium, 2010.
8. Priem, B.; Kosta, E.; Kuczerawy, A.; Dumortier, J.; Leenes, R. User-centric privacy-enhancing identity management. In Digital Privacy; Springer: New York, NY, USA, 2011; pp. 91–106.
9. Kumar, P.; Sehgal, V.K.; Chauhan, D.S.; Gupta, P.; Diwakar, M. Effective ways of secure, private and trusted cloud computing. arXiv 2011, arXiv:1111.3165.
10. Abdulsalam, Y.S.; Hedabou, M. Decentralized Data Integrity Scheme for Preserving Privacy in Cloud Computing. In Proceedings of the 2021 International Conference on Security, Pattern Analysis, and Cybernetics (SPAC), Chengdu, China, 18–20 June 2021; pp. 607–612.
11. Sun, X.; Liu, P.; Singhal, A. Toward Cyberresiliency in the Context of Cloud Computing . IEEE Secur. Priv. 2018, 16, 71–75.
12. Li, P.; Li, J.; Huang, Z.; Li, T.; Gao, C.Z.; Yiu, S.M.; Chen, K. Multi-key privacy-preserving deep learning in cloud computing. Future Gener. Comput. Syst. 2017, 74, 76–85.

13. Zhou, M.; Zhang, R.; Xie, W.; Qian, W.; Zhou, A. Security and privacy in cloud computing: A survey. In Proceedings of the 2010 Sixth International Conference on Semantics, Knowledge and Grids, Beijing, China, 1–3 November 2010; pp. 105–112.
14. Pearson, S. Taking account of privacy when designing cloud computing services. In Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing, Vancouver, BC, Canada, 23 May 2009; pp. 44–52.
15. Ko, R.K.; Jagadpramana, P.; Mowbray, M.; Pearson, S.; Kirchberg, M.; Liang, Q.; Lee, B.S. TrustCloud: A framework for accountability and trust in cloud computing. In Proceedings of the 2011 IEEE World Congress on Services, Washington, DC, USA, 4–9 July 2011; pp. 584–588.
16. Pfitzmann, A.; Hansen, M. A Terminology for Talking about Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management 2010. Available online: http://dud.inf.tu-dresden.de/Anon_Terminology.shtml (accessed on 20 October 2021).
17. Dingledine, R.; Mathewson, N.; Syverson, P. Tor: The Second-Generation Onion Router; Technical Report; Naval Research Lab: Washington, DC, USA, 2004.
18. Goldschlag, D.; Reed, M.; Syverson, P. Onion Routing for Anonymous and Private Internet Connections; Communication of the ACM; ACM: New York, NY, USA, 1999.
19. Chaum, D. The dining cryptographers problem: Unconditional sender and recipient untraceability. J. Cryptol. 1988, 1, 65–75.
20. Bagai, R.; Lu, H.; Li, R.; Tang, B. An accurate system-wide anonymity metric for probabilistic attacks. In Proceedings of the International Symposium on Privacy Enhancing Technologies Symposium, Waterloo, ON, Canada, 27–29 July 2011; pp. 117–133.
21. Goodrich, M.T.; Mitzenmacher, M.; Ohrimenko, O.; Tamassia, R. Privacy-preserving group data access via stateless oblivious RAM simulation. In Proceedings of the Twenty-Third Annual ACM-SIAM Symposium on Discrete Algorithms, Kyoto, Japan, 17–19 January 2012; Society for Industrial and Applied Mathematics: Philadelphia, PA, USA, 2012; pp. 157–167.
22. Stefanov, E.; Van Dijk, M.; Shi, E.; Fletcher, C.; Ren, L.; Yu, X.; Devadas, S. Path ORAM: An extremely simple oblivious RAM protocol. In Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, Berlin, Germany, 4–8 November 2013; pp. 299–310.
23. Diamantopoulou, V.; Kalloniatis, C.; Gritzalis, S.; Mouratidis, H. Supporting privacy by design using privacy process patterns. In Proceedings of the IFIP International Conference on ICT Systems Security and Privacy Protection, Rome, Italy, 29–31 May 2017; pp. 491–505.
24. Haider, S.K.; van Dijk, M. Flat ORAM: A Simplified Write-Only Oblivious RAM Construction for Secure Processors. Cryptography 2019, 3, 10.
25. Ngai, E.; Ohlman, B.; Tsudik, G.; Uzun, E.; Wählisch, M.; Wood, C.A. Can we make a cake and eat it too? A discussion of ICN security and privacy. ACM SIGCOMM Comput. Commun. Rev. 2017, 47, 49–54.
26. Papanikolaou, N.; Pearson, S.; Mont, M.C. Towards natural-language understanding and automated enforcement of privacy rules and regulations in the cloud: Survey and bibliography. In Proceedings of the FTRA International Conference on Secure and Trust Computing, Data Management, and Application, Loutraki, Greece, 28–30 June 2011; pp. 166–173.