International Journal of Computer (IJC)
ISSN 2307-4523 (Print & Online)

http://ijcjournal.org/

Cloud Computing Privacy Concerns in Social Networks

Naif Ali Almudawi*

Department of Computer Science and Information System ,Najran University, Najran, Saudi Arabia
Email: naalmudawi@nu.edu.sa

Abstract

The establishment of social networks and the cloud computing technology has led to the enrollment of a large number of online users into the networks. These users to a larger extent are capitalizing on the benefits and available opportunities that lacked before to a larger extent. Cloud computing has therefore enhanced the freedom of interaction on social media that has made most users to freely share personal information via social media as well as storage of information into the cloud computing systems. Accumulation of diverse information raises problems related to data security that has prompted the need for maintaining personal data private and improvement of the trust towards the service provider. This study investigates the privacy concerns that arises from the use of cloud technology in social networks and provides a recommendation on the measures that needs to be enforced to secure personal information stored over the cloud.

Keywords: Cloud Computing; Social Networks; Privacy; Challenges.

1. Introduction

Cloud computing is the ability of a user to gain access to the computing resources over a network [24]. The shared resources include servers, storage, network, and services among others. Cloud computing provides many advantages the major one being the cost reduction [3]. Most organizations make use of cloud computing services provided by a third party at the time when these particular resources are needed and the scale down and scale up as required without channeling many resources into the infrastructural investment [10].

Also, data and other important applications can easily be accessible through the internet at any time Social networks comprise of different entities that are interconnected through different relations [2].

---

* Corresponding author.

The entities are usually referred to as the users. Various relationships that exist between the users are attributed to by different names used across various social networks. Names such as followers and friends are commonly used. The relationship has enabled many users to share messages and other media resources amongst themselves. The common online social networking sites that are in existence include Twitter, Facebook, and LinkedIn.

Currently, social networking and cloud computing are being used together in a number of ways [6]. The two options that exist are that the social media networks can either be incorporated into a social network or it can have scalable applications in the social networks. In social cloud systems, the cloud-based application offers authentication and user management services by the aid of social networks. Most organizations through social media use cloud computing to carry out most of their functions [2]. These companies, however, are faced with a number of challenges and the pressures to provide protection to information assets that belong to customers as well as other sensitive information.

Security, availability, and privacy are the topmost concerns in any cloud environment [1]. From the security standpoint, the cloud is perceived to be a double-edged sword. Social media users are vulnerable to different but related risks. Criticisms have been made about the privacy and security related to unauthorized access and utilization of information found on the cloud for ill motives and other malicious purposes. While the effectiveness of cloud computing in the social network is highly commendable, there is still a weakness in terms of its performance since the policies and practices that are associated with privacy and security remains weak. In this particular research, we seek to gain insight into the privacy concerns associated with cloud computing in social networks, assessment of the best practices to curb data leaks and other security concerns [17]. This paper has investigate the privacy concerns those arises from use of cloud computing in social networks and propose the possible solutions to the challenges

2. Literature Review

2.1 How social media uses cloud

The present generation has embraced the use of social networks in many roles both personal and commercial [23]. In order to manage such a high traffic, cloud technology has been adapted. Social networks have helped to a larger extent in enhancing the internet usability. Large multimedia content is stored in the cloud storage systems [14]. A lot of space is usually occupied by photographs and videos which are part of the most popular content found on social networks. Cloud computing providers like Amazon and Salesforce have diversified in the services offered that are inclusive of enterprise resource planning and customer relationship management [12]. Customers can, therefore, utilize these services without necessarily purchasing them since they are located in the cloud services.

Besides data storage, social sites utilize clouds in other tasks such as big data analytics. Facebook, for instance, has a more improved analytics that are used mainly the business users. Social networks use clouds to reduce the costs related to data backup and also data recovery when a disaster occurs [5]. Data stored at a particular location is riskier than one found in the cloud. This is due to the hardships encountered during recovery.

Through cloud computing, social network users can now access shared resources from anywhere on the globe. This is beneficial to most social networks as they maintain personal information of its clients and therefore should not lose any part of the information, however, trivial it is. Every user of the social network, therefore, utilizes cloud computing technology [11].

2.2 Privacy concerns

Since all social media platforms rely fully on cloud computing, privacy remains a critical aspect. The major issues related to the privacy of cloud computing in these applications are the loss of control of the data and the dependence on the provider of the cloud computing [14]. These particular issues can develop into different legal and the security concerns that are related to identity management, infrastructure, risk management, legislative and regulatory compliance, integrity control, access control and other risks that are dependent on the cloud computing provider. Most users of social media are concerned much by the privacy of their information which can be easily compromised through data loss [14].

2.3 Privacy issues in social networks

Social networks provide an environment that is very much vulnerable to stealing and use of information from social media that is most sensitive [7]. During the early stages of Facebook development, for instance, access to social media information was easy due to lack of awareness by the users regarding privacy setting. Underdeveloped private policies and reliability to the common third party applications also contributed much to ease of access. Violations of privacy are of different magnitudes that vary right from image hacking, to profile hacking then later to the dangerous malware attacks.

There are three major privacy issues that are deemed weakness on social networks. These include cyber bullying, profile hacking, and identity theft[20]. Identity theft involves stealing or leaking of relevant data such as photos phrases or the use of one's information to come up with a new digital identity. With the use of phishing scams, individuals gain access to information via actions such as modification of addresses, getting the financial services or creation of new accounts using the victims' credentials. Some create fake documents and use it for their malicious gains [4].

Social network services are focused on establishing online communities of individuals who share common interests and activities. This type of computer-mediated type of communication has brought a big change in the rules of communication and social interaction. Due to a large number of people utilizing these features, new privacy concerns have been raised as a large amount of personal information is being loaded into the database of the online organizations. This particular approach has brought together a pool of rich information that is prone to misuse [15]. The present regulations and privacy mechanisms that were introduced to counter such threats seems not enough to measure to assure security and privacy of sensitive information. There are different sources of uncertainties that have resulted in many problems cropping up due to the increase in the usage of social media and hence privacy concerns. These include

2.3.1. Online marketing

Online marketing is one of the recent applications of social networking in the marketing of various businesses [25]. This has grown so fast due to the abundance of many applications that are meant to tailor the virtual customer. These apps can be first misjudged as a platform through which one's spare time is saved but facts prove that they are platforms through which different people gain access to personal data that is then resold to marketing and research companies [25]. People's information is also used to facilitate future services and products by the competing companies.

2.3.2. Lack of enforcement policies

Most social media users carry out the online registration using their personal information with the aim of submitting their actual identity. This information once submitted online, cloud computing device providers stores them into their database which means that it now gets out of the individuals control and other policies of user business [16]. Consequently, privacy concerns arise since the individuals lack direct of the provided information and hence prone to illegal access, and theft among other issues related to data integrity.

2.3.3. Friending unknown persons

Most business who seeks to extend their market networks via social media tends to friend individuals whom they do not even know their identity. This activity provides a loophole for friending fraudsters and hackers among other dangerous peoples. As a result, information is given to unknown sources that might result to illegal access. Hackers and fraudsters utilize the weaknesses that existing to the cloud computing application of the social networks to spread malware, and also scam consumers into providing personal data [6].

3. Issues due to data loss

Most social network users are informed about the dangers associated with letting the control of personal information out of their hands and letting it stored by the cloud computing provider [8]. In this particular case, there is a very high probability that this information can be easily compromised by the provider of cloud computing service itself. This data is also vulnerable to getting compromised by other people and competitive enterprises that utilize the cloud computing services. In addition to this, data stored in cloud lacks transparency and there not clear n how, why, where, and when personal information is processed [8].One of the data protection requirements is that customers should know the operations performed on their data a measure that is never implemented by cloud computing providers. Cyber bullying involves the use of an individual's private information to give threats to them, stalk them, harass them, and performing other dangerous acts online [8]. Cyber bullying is common among teenagers and it is deemed dangerous since their impacts are greater including psychological impacts [20]. This crime at some point can result to the bullied teen committing suicide. Profile hacking is also rampant on social networks caused by hackers steals someone's password and use it to gain entry into one's account.

4. Privacy and cloud computing

Cloud computing providers have made efforts to enforce control measures meant to disclose personal data

though it still remains to be a major challenge. Data security from the academic point of view is assessed basing on the confidentiality, integrity, and availability. In cloud computing, a lot of focus is shifted towards data privacy. All types of cloud computing including private, public and hybrid are faced with lots of privacy related issues due to the fact that data and information are spread on various machines and devices [22]. Some organizations such as Volkswagen group moved away from the use of cloud computing due to the privacy concerns.

The major reason for social media users to use cloud computing for data and information storage is to provide convenience since they are in a position to access this content at any time and from any device. Users can also share the content with various people. This particular transmission gives the users the power to use, duplicate, and destroy shared data that is deemed to be multi-tenancy and service abused [21]. Social networks users are therefore required to control the way their information is handled in cloud computing.

Every cloud environment has various risks associated with it. the common security and privacy concerns include:

2.5.1. Multi-tenancy

To establish a secure multi-tenant environment, issues such as application deployment, data protection, data access, and access policies should be taken into consideration [9].

2.5.2. Outsourcing

With cloud computing, social network users lose control over their own data. Privacy, therefore, becomes a big concern in this particular scenario. It is, therefore, important for the cloud providers to develop an appropriate mechanism that prevents the use of customer information in other ways other than the intended purposes [12].

2.5.3. Virtualization

All information found on cloud servers is usually accessed virtually. To enhance security and privacy, a proper mechanism should need to be put in place to ensure there are strong isolation and a mediated communication and sharing between the virtual devices [19]. An access control system that is flexible can be used to enforce the access policies which dictate how virtual machines share data over the cloud host.

2.5.4. Heterogeneity

Cloud environments are characterized by heterogeneity. Different providers of cloud services have different approaches to security and privacy provisions which result in integration challenges [21].

5. Possible solutions to data privacy challenges

Social networking is fully dependent on cloud computing hence privacy of personal data becomes a critical issue of concern [22]. Measures should be enforced to assure users of their privacy. Also, the users should try

and assure security to their personal information to avoid getting subjected to issues like theft, fraud, and illegal access among others [13]. One of the most suitable ways of protecting personal data is performing data encryption [21]. Users should encrypt their data before storing it in the cloud server. The data owner can then specify members of a particular group who have the permission to access the information. Data access control should be assured through the heterogeneous data-centric security.

The cloud computing service providers should come up with a data security model that comprises of data encryption, authentication, data integrity, user protection, and data recovery to enhance the security of data found in the crowd [22]. Data protection should be provided as a service so that security and privacy of data are enhanced. During the data transmission process, confidential and most sensitive data should be protected by configuring the SSL for each and every server instance.

Within the multi-tenant environment, security should be given very high priority. In this particular setting, privacy should be assured in each layer found in the cloud application architecture. The service provider should fully deal with the physical security to encourage the use of the cloud in social networks [24]. However, application-level and network security remain the user's responsibility.

Legal compliance and risk management should be well stipulated within the contract that exists between the customer and the cloud computing provider to assure transparency regarding storage and processing of data over the cloud [18]. This will strengthen the trust between the two and hence assure the social media users security of their most sensitive and confidential information. It is also of much importance that customers consider backing up essential data locally to ensure data availability.

6. Conclusion and future work

Despite the good benefits, cloud computing technology provides to the users of social networks, a lot of challenges concerning data security are encountered. The total number of social network users is rising day by day hence there is an increase in the collaboration between social networking companies and cloud computing. As a result of this, new issues related to the privacy and trust is being identified. Most social media users are aware of the privacy issues related to their personal information and as a result, measures are being developed frequently to protect this information. Both the users of social networking and the cloud computing providers have a major role in ensuring the privacy and security of personal data. In this research, the privacy concerns and the possible solutions to security issues are provided to prevent the risks associated with cloud computing. In future developments, concrete standards can be developed to provide security of the cloud. To ensure access of data over the cloud is secure, there is need to develop advanced encryption techniques to be applied in both storage and retrieval of data from the cloud.

References

[1] Abid,”Designing network services for the cloud: Delivering business-grade cloud services”, Indianapolis, Ind: Cisco. 2012.

[2] C. C. Aggarwal ” An introduction to social network data analytics”, InSocial network data analytics ,

pp. 1-15. 2011. Springer US.

[3] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, and M. Zaharia, " A view of cloud computing", Communications of the ACM, vol. 53(4), pp. 50-58.

[4] R.Buyya, J. Broberg, and A.M. Goscinski, (2010), "Cloud computing: Principles and paradigms",Vol. 87. John Wiley & Sons.

[5] M. Carroll, A. Van Der Merwe, and P. Kotze, "Secure cloud computing: Benefits, risks and controls", In 2011 Information Security for South Africa 2011, August, pp. 1-9. IEEE.

[6] K. Chard, S. Caton, O.F. Rana, and K. Bubendorfer," Social cloud: Cloud computing in social networks", IEEE CLOUD, vol. 10, pp. 99-106. 2010.

[7] R. Chbeir, and B. A. Bouna. (2013). Security and privacy preserving in social networks. Vienna: Springer.

[8] D. K. Citron, "Hate crimes in cyberspace", Harvard University Press; 2014 Sep 22.

[9] T. Dillon, C. Wu, and E. Chang, "Cloud computing: issues and challenges", In 2010 24th IEEE international conference on advanced information networking and applications. 2010, April, pp. 27-33. Ieee.

[10] H. T. Dinh. C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: architecture, applications, and approaches. Wireless communications and mobile computing", vol.13(18), 1587-1611.2013.

[11] G. Huerta-Canepa, and D. Lee., "A virtual cloud computing provider for mobile devices. In Proceedings of the 1st ACM Workshop on Mobile Cloud Computing & Services: Social Networks and Beyond", 2010, June. p. 6. ACM.

[12] M. H. Hugos, and D. Hulitzky. (2010). Business in the cloud: what every business needs to know about cloud computing. John Wiley & Sons. p. 139.

[13] J. Jang-Jaccard, and S. Nepal, "A survey of emerging threats in cybersecurity", Journal of Computer and System Sciences, vol. 80(5), pp. 973-993. 2014.

[14] K. Kumar, and Y. H. Lu, "Cloud computing for mobile users: Can offloading computation save energy? ", Computer, vol. 43(4), 51-56. 2010.

[15] G. Pallis, D. Zeinalipour-Yazti, and M.D. Dikaiakos, "Online social networks: status and trends", In New Directions in Web Data Management vol.1, pp. 213-234.2011. Springer Berlin Heidelberg.

[16] S. Pearson, "Taking account of privacy when designing cloud computing services", In Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing . 2009, May. pp. 44-52. IEEE Computer Society.

[17] S. Pearson and A. Benameur, "Privacy, security and trust issues arising from cloud computing", In Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on , 2010, November, pp. 693-702. IEEE.

[18] , J. W. Rittinghouse and J. F. Ransome. (2016). Cloud computing: implementation, management, and security. CRC press.

[19] W. J. Robison, "Free at what cost? cloud computing privacy under the stored communications act", Georgetown Law Journal.vol.98(4), 2010.

[20] J. Sen, " Security and privacy issues in cloud computing.Architectures and Protocols for Secure

Information Technology Infrastructures", 2013, pp.1-45.

[21] D.Song, E. Shi, I. Fischer, and U. Shankar, "Cloud data protection for the masses", 2012.

[22] M. Vaidya, "Handling Critical Issues of Big Data on Cloud. Managing Big Data in Cloud Computing Environments", pp100.2016.

[23] X. Zhao, N. Salehi, S. Naranjit, S. Alwaalan, S. Voida, and D. Cosley, "The many faces of facebook: experiencing social media as performance, exhibition, and personal archive", In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2013, April , pp. 1-10. ACM.

[24] D. Zissis, and D. Lekkas, "Addressing cloud computing security issues", Future Generation computer systems, vol. 28(3), 2012, pp.583-592.

[25] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of-the-art and research challenges", Journal of internet services and applications,vol.1(1), pp.7-18. 2010.