

Cis 417 week 7 discussion 1 and 2 term paper examples

[Business](#), [Company](#)



Mobile devices play a key role in mail investigations. This is true because most people synchronize all their data to the mobile devices and it is the most often used platform in accessing mails. A key risk in the application of handheld devices is the susceptibility to theft, breakdown or just normal loss. Since users will always walk around with their mobile devices, they are more prone to loss as opposed to desktop computers that are always in the offices. Loss of these devices means loss of crucial data. Wireless networks also lack some aspects of stability under given circumstances. For instance, when there are cases of power breakdowns, wireless networks are rendered unstable, and some configurations may need to be done to restore their stability (Kumar, Manjunath & Kuri, 2008).

Apple's iCloud has been key cloud service provider in the recent past. Its main function is to provide for transportation and storage of data and information for its users. Its main advantage is its ability to provide high standard security for the information it stores against unauthorized access. It is also a cheap means of storing data and also safe. For instance, data stored in Dropbox is always safe and cheap to keep. However, Apple holds all the decryption keys to this data and can access, modify, manipulate and even distribute it to legal authorities when called upon. This is in a bid to make email investigations possible.

Forced client merging is a major challenge facing users of the cloud and storage of web mail. Cloud computing technology lacks the isolation mechanisms that could allow users in a cloud, though sharing virtual resources, to operate independently. This has much to deal with memory allocations and individual reputation. It is notable that storage spaces in a

cloud are merged, making it relatively difficult for a specific person to store data on a private platform within the cloud. This could attract enormous attacks that could affect a number of users. These attacks, however, have been considered hard to be effected as compared to the individual company operating systems that have been in place in the past.

iCloud is an aspect of cloud computing made available by Apple to users interested. It facilitates storage and access of various services in the cloud, among them calendars, emails, contacts and other services. This application is designed to allow log in with other email accounts that are not necessarily @iCloud. com. It also provides for a portal for all web mail hence making investigations possible. Since it is a cloud service prone to many threats, users of iCloud should embrace encryption so much as a measure to ensuring the security of their information.

References

Apple holds the master decryption key when it comes to iCloud security, privacy | Ars Technica. (n. d.). Ars Technica. Retrieved May 23, 2013, from <http://arstechnica.com/apple/2012/04/apple-holds-the-master-key-when-it-comes-to-icloud-security-privacy/>

Durkee, D. (2010), ' Why Cloud Computing Will Never Be Free',
Communication of the
ACM, Vol. 53, No. 5, pp. 62-69.

Kumar, A., Manjunath, D., & Kuri, J. (2008). Wireless networking. Amsterdam:
Morgan Kaufmann/Elsevier.