International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-4, Issue-7)

Research Article

July 2015

Enhancing Mobile Phone Data Privacy using The Cloud

Gagandeep Kaur *
M.E. Student
I.G.C.E, Punjab, India

Er. Namisha Mahajan
Assistant Professor
I.G.C.E, Punjab, India

Mayank Arora
C.C.E.T., Sector-26
Chandigarh, India

Abstract—

As the technology is shifting from the desktop/Laptops towards smartphones, more and more organizations are trying to capture this platform to reap the benefit in any way possible. Everyday new applications are being introduced and the older ones are shifting to mobile devices, making it an area of great interest for data thefts and hackers. The proposed architecture tries to solve some privacy and data integrity issues by making sure the data is encrypted using a strong encryption scheme and also that the encryption doesn't makes the smartphone overburdened. The computation power is taken from the Cloud service providers by offloading the Encryption process partially. Doing this our goal of secure data is achieved without putting an overhead on the smartphone.

Keywords— Offloading, Mobile Cloud Computing, Privacy of Data.

I. INTRODUCTION

Cloud computing is a technology that provides convenient, on demand services and resources to its users. The users just have to pay for the services they use. With the use of cloud services centralization of information is being done into cloud servers such as emails, personal private videos etc[1-5].

ADVANTAGES OF CLOUD COMPUTING

a) Low software cost: with cloud computing the cost of purchasing software is reduced as some cloud services provide free services and others provide software in the pay per use model.
B) Use of low configuration computers: computer with lower configuration can be used.The cloud applications can run on a simple browser as the actual computation is being done on the Cloud side.
c) More storage capacity: cloud provides almost unlimited storage capacity. It can be accessed anywhere and backup can be easily done.
d) Reliable: cloud computing is reliable method of storing data as it prevents destruction of data when ever computer crashes.

DISADVANTAGES OF CLOUD COMPUTING

a) Security related threats: unauthorised access to data can lead to threat to the important and confidential information. This can also be called as lack of trust.
b) Fast internet connection: fast and constant internet is required for cloud computing.

SERVICE MODEL OF CLOUD COMPUTING

Infrastructure as a Service
Infrastructure as a service provides companies with computing resources including servers, networking, storage, and data centre space on a pay-per-use basis.
Platform as a Service
Platform as a service provides a Cloud-based environment with everything required to support the complete life cycle of building and delivering web-based (Cloud) applications—without the cost and complexity of buying and managing the underlying hardware, software, provisioning and hosting.
Software as a Service
Cloud-based applications or software as a service (SaaS) run on distant computers "in the Cloud" that are owned and operated by others and that connect to users' computers via the Internet and, usually, a web browser[5-8].

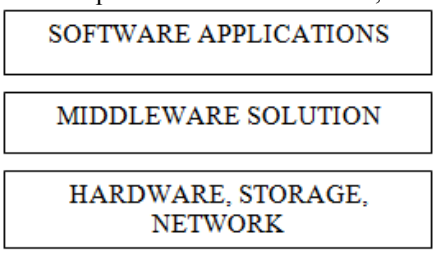

Fig no-1: Services of cloud computing

MOBILE CLOUD COMPUTING

Mobile cloud computing (MCC) at its simplest, refers to an infrastructure where both the data storage and data processing happen outside of the mobile device. Mobile cloud applications move the computing power and data storage away from the mobile devices and into powerful and centralized computing platforms located in clouds, which are then accessed over the wireless connection based on a thin native client[15-17].

CHARACTERSTICS OF MOBILE CLOUD COMPUTING

On-demand self service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms like mobile phones, laptops, PDAs etc.
Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. The customer does not have control or knowledge over the exact location of the provided resources. Examples of resources include storage, processing, memory, network bandwidth and virtual machines.
Rapid elasticity: Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in.
Measured Service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g. storage, processing, bandwidth and active user accounts)[26].

NEED FOR MOBILE COMPUTING

Mobile devices face many resource challenges (battery life, storage, bandwidth etc.) Cloud computing offers advantages to users by allowing them to use infrastructure, platforms and software by cloud providers at low cost and elastically in an on-demand fashion.Mobile cloud computing provides mobile users with data storage and processing services in clouds, obviating the need to have a powerful device configuration (e.g. CPU speed, memory capacity etc), as all resource-intensive computing can be performed in the cloud[27].

II. PROPOSED WORK

An easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it. Ideology Our focus will be on making the data in the smart phone secure enough so that in case of a theft the data is not misused. This could be done by encrypting the data using some proven encryption scheme. This will ensure the safety of data but will impose an overhead on the smartphone to encrypt the data. It is proposed that if the encryption be done using the power of cloud then the process could be fast as well as it could ensure security. For the offloading purposes we will use an existing offloading scheme. The working of the proposed architecture could be better understood with the help of the following diagram. The data in the mobile phone is first encrypted at the phone side using DES.

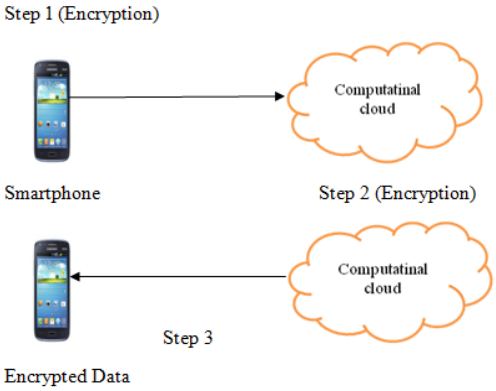

Figure 1.2: A Framework for securing smartphone data using the power of cloud.

So the encryption in this will be a two stage process firstly the data will be encrypted on the phone itself and then the data will be encrypted on the computational cloud and the final encrypted data will be stored in the Smartphone. Now if the phone gets lost the data will be of no use for anyone except the authentic user of the phone who possesses the Key to decrypt the data.

Methodology

TripleDES will be used as the encryption technique as we cannot rely completely on the cloud for encryption unless it is a private cloud. The first step of DES will be done at the phone side so that when the data reaches the computational cloud it is encrypted once. On the cloud side the data will be encrypted twice again to complete the process and the finally encrypted data will be sent back to the phone and stored in the phone. Using this technique will ensure that if in case the phone gets lost then also the data would not be compromised. Figure 1.3 shows a more detailed view of the

activities performed by both the actual Smartphone and the Virtual Smartphone, provided at the Cloud server. Also the communication between the two has been shown in the following control flow. On the Smartphone's side, the Security app is initially run and the user inputs like an Image or text that needs to be encrypted is accepted by the smartphone. The data is once encrypted using DES. In this framework we will be using Triple DES but the other two rounds of encryption will be done at the cloud side.

Now on the Cloud server's side, where the Virtual smartphone resides, the semi encrypted data i.e. data encrypted once using DES are fed. The next step performed by the virtual phone is to complete the remaining two rounds of DES. The finally encrypted data is then returned to the smartphone where it finally gets stored for future reference.

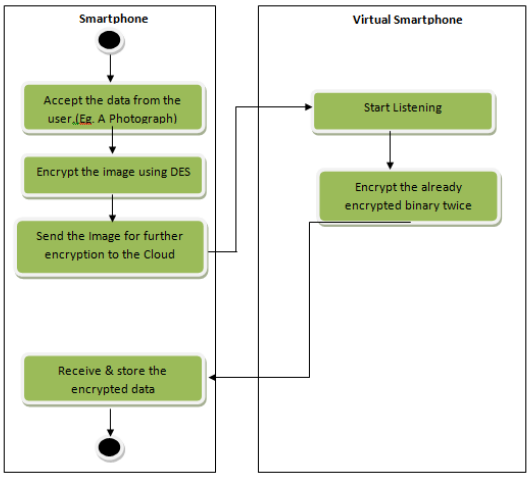

Figure 1.3 Control Flow diagram showing operations between a Smartphone and a Virtual device

III. RELATED RESEARCH

In the year 2013 M. Arora et al.[27] proposed a framework for making the applications of these smart phones intelligent enough, to offload their compute intensive parts from the smart phone to the virtual image of the Smartphone on the cloud thus using the unlimited resources of the cloud. By using this framework the application developers will be able to enhance the capabilities of the smart phones and will be empowered to make the applications even richer. Another author Xu wang et al.[23] proposed cloud computing and took Google's cloud computing techniques as an example, summed up key techniques, such as data storage technology (Google File System), data management technology (Big Table), as well as programming model and task scheduling model (Map Reduce), used in cloud computing, and then some example of cloud computing vendors were illustrated and compared. A new approach was proposed by G. Zhao et al.[1] in the year 2013 which aims to construct a system for trusted data sharing through untrusted cloud providers to address the above mentioned issue. The constructed system can imperatively impose the access control policies of data owners, preventing the cloud storage providers from unauthorized access and making illegal authorization to access the data.

In the year 2014 M Arora, Neha Saini [5] proposed that the area to be focused that is security of mobile data, offloading to cloud for storage and processing. There are many encryption techniques used by researchers such as RSA, DES and AES for security purpose. These techniques have some loopholes. So a framework which will use ECC technique with progressive encryption to provide better security to the mobile data on cloud without creating much overhead on the Smartphone.

IV. CONCLUSIONS

The research discussed in the above paper will help the enterprise to shift their applications and data to Mobile cloud Computing as a relation of trust and security is being formed between the Cloud Service provider and the mobile user. More over the risk of data loss/leakage from the mobile device is also reduced as the data is being encrypted before storing. Data encryption schemes nowadays are quiet complex and result in extra overhead on the smartphone's scarse resources. The smartphones rely on a small battery to provide power to them and such encryption/ decryption processes lead to a heavy overhead on the phone's limited power source, thus draining the phone's battery. The scheme proposed in this paper is offloading the encryption/decryption process to an external computational Cloud. Thus providing Privacy/security to the phone's data without putting an extra overhead on the Phone's battery.

REFERENCES

[1] G. Zhao, C. Rong, Jin Li, F. Zhang and Yong Tang,"Trusted data sharing over untrusted cloud storage providers", in *2nd IEEE International Conference on Cloud Computing Technology and Science*, Page(s): 98 – 103, 2010.

[2] Md. AI-Hasan, K. Deb and M. O. Rahman, "User-Authentication approach for data security between smartphone and cloud", in *8th International Forum on Strategic Technology (IFOST),* Vol.2, Page(s): 2 – 6, 2013.

[3] M. Arora, M. Kalra and Dr. S. Singh, "Autonomous computation offloading framework for android using cloud" in 2nd *International Conference on Information Management in the Knowledge Economy,* 2013.

[4] S. Maria Celestin Vigila, K. Muneeswaran, "Elliptic curve based key generation for symmetric encryption" in *International Conference on Signal Processing, Communication, Computing and Networking Technologies* , Page(s): 824 – 829, 2011.

[5] M. M. Sandoval, C. F. Uribe, "A hardware architecture for elliptic curve cryptography and lossless data compression", in 8th *International Conference on Electronics, Communications and Computers,* Page(s): 113 – 118, 2005.

[6] D. Mukherjee, H. Wang, A. Said, S. Liu, "Format independent encryption of generalized scalable bit-streams enabling arbitrary secure adaptations" in *IEEE International Conference on Acoustics, Speech and Signal Processing* , Vol. 2, Page(s): 1033 - 1036, 2005.

[7] S. Govindarajan, P. Gasti, K. S. Balagani, "Secure privacy-preserving protocols for outsourcing continuous authentication of smartphone users with touch data" in *IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS),* Page(s): 1 – 8, 2013 .

[8] P. Ragunathan, K. Sambath, V. Karthik, "Accessing a network using a secure android application" in *International Conference on Advanced Networking and Applications,* Vol. 4, Page(s):1503-1508, 2012.

[9] A. Tripathi and P. Yadav, "Enhancing security of cloud computing using elliptic curve cryptography" in *International Journal on Computer Applications*,Vol.57, Page(s): 1-8, 2012.

[10] G. Portokalidis, P. Homburg, K. Anagnostakis and H. Bos, "Paranoid Android: Versatile Protection for Smartphones," in *Proceedings of the 26th Annual Computer Security Applications Conference*, Page(s): 347-356, 2010.

[11] E. Cuervo, A. Balasubramanian, D.K. Cho, A. Wolman, S. Saroiu, R. Chandra and P. Bahl, "MAUI: Making smartphones last longer with code offload," in *Proceedings of the 8th international conference on Mobile systems applications and services*, Page(s): 49-62, 2010.

[12] L. Subramanian, Gerald Q. Maguire Jr. and P. Stephanow "An architecture to provide cloud based security service for smartphones",[Online].Available:http://www.divaportal.org/smash/get/diva2:509785/FULLTEXT01.pdf.

[13] P. Teufl, A. Fitzek, D. Hein, A. Marsalek, A. Oprisnik and T. Zefferer " Android encryption system", in *Proceedings of the 8th internationalconference*,2014.[Online].Available:http://www.asit.at/pdfs/Technologiebeobachtung/Android_Encryption_Systems_Paper_1569918947.pdf.

[14] K. Bhardwaj and S. Chaudhary "Implementation of elliptic curve cryptography in 'C'", in *International Journal on Emerging Technologies*, Vol. 2, Page(s): 38- 51, 2012.

[15] A. Dabholkar and K. C. Yow "Efficient implementation of elliptic curve cryptography (ECC) for personal digital assistants (PDAs)" in *Journal on Wireless Personal Communication*, Vol. 29, Page(s): 233 – 246, 2004.

[16] A. Saarinen, M. Siekkinen, Y. Xiao, J. K. Nurminen, M. Kemppainen and P. Hui, "SmartDiet: Offloading popular apps to save energy," in *Data Communications Conference on Association for Computing Machinery's Special Interest Group* , Page(s): 297-298, 2012.

[17] W. SONG and X. SU, "Review of mobile cloud computing," in *IEEE 3'rd international conference on Communication Software and Networks*, Page(s): 1-4, 2011.

[18] J. Peng, X. Zhang, Z. Lei, B. Zhang, W. Zhang and Q. Li, "Comparison of several cloud computing platforms" in *Proceedings of IEEE international conference on Information Science and Engineering*, Page(s): 23-27, 2009.

[19] National Institute of Science and Technology, "The NIST,".Available:http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. Last accessed on July 2014.

[20] R. Buyya, J. Broberg and A. Goscinski. Introduction to Cloud Computing in Cloud Computing: Principles and Paradigms, Wiley Press [Online], Page(s):1-44, 2011.

[21] Android Open Source Project. Philosophy and Goals. Available: http://source.android.com/about/philosophy.html. Last accessed on July 2014.

[22] M. A. Vouk, "Cloud Computing - Issues, Research and Implementations", in *Journal of Computing and Information Technology* - CIT 16, Vol. 4, Page(s): 235-246, 2008.

[23] Y. Hu, Wong, G. Iszlai, M. Litoiu "Resource provisioning for cloud computing", in *Proceedings of the Center for Advanced Studies on Collaborative Research*, Page(s): 101-111, 2009.

[24] Y. Tang, P. P. C. Lee, J. C. S. Lui, and R. Perlman, "FADE: Secure overlay cloud storage with file assured deletion", in *Proceedings of Secure Communication*, 2010.

[25] T. S. Kar, M. A. P. Mahmud, "A newer secure communication, file encryption and user identification based cloud security architecture" in *International Journal of Computer Applications*, Vol. 52, 2012.

[26] N. Fernando , Seng W. Loke , W. Rahayu, " Mobile cloud computing : A Survey" in *International Journal of Future Generation Computer Systems*, Page(s): 84-106, May 2012.

[27] K. Divya, N. Sadhasivam, "Secure data sharing in cloud environment using multi authority attribute based encryption" in *International Journal of Innovative Research on Computer and Communication Engineering* , Vol.2, Page(s): 24-29, March 2014.

[28] M. Arora, M. Kalra and Dr. S. Singh, "Autonomous computation offloading framework for android using cloud" in 2nd International Conference on Information Management in the Knowledge Economy, 2013.

