Achieving Energy Efficiency and Security in Mobile Cloud Computing

Sourya Joyee De, Sourav Saha and Asim K. Pal
Management Information Systems Group, Indian Institute of Management Calcutta, Joka, D. H. Road, Kolkata, India

Keywords: Mobile Cloud Computing, Security, Privacy.

Abstract: Computation offloading to the Cloud for energy efficiency in portable devices is an emerging area of research triggered by the widespread use and acceptance of smart phones. A number of architectures have already been proposed in this context. However, security issues in the cloud still remain a concern that can play an important role in deciding whether offloading really helps to achieve energy efficiency in mobile phones. Our framework is based on a layered data approach together with user selected security policies. This motivated us to develop a mathematical model to depict the energy consumption when performing a security-enhanced computation in the cloud. The model demonstrates the potential energy saving in the event of user or organization specified policy for secure computing and data storage in the Cloud.

1 INTRODUCTION

Today mobile phones have a wide range of functionalities and are fast becoming the primary computing devices for many people (Kumar and Lu, 2010). However battery life still remains a constraint and demands improvement. Even for high-end phones like the iPhone, the consumer's top priority is battery life (Paczkowski, 2009). Long battery life implies that a user can remain connected to the world for longer time.

Of late, mobile phones are being used as an interface for cloud computing (Luo, 2009). Earlier, the use of Mobile Cloud had several challenges like setup time and cost. However with newer technologies like virtualization, cloud instances can be invoked for even a short time (Barham et al., 2003). Thus recent research focuses on how heavier applications can be offloaded to the cloud to save battery life. The decision that which tasks should be offloaded depends on the amount of computation (task complexity) and data to be transmitted (bandwidth and power consumption), etc.

Even with ever-increasing concerns about information security and the trustworthiness of cloud service providers (CSPs), the sensitiveness of information to undesirable exposure has not yet been considered an integral part of the energy saving problem. Use of security techniques can adversely affect energy efficiency. Data is an integral part of mobile devices and users are sensitive about its privacy and security. However, not all information has identical requirements. For example, a user will be happy to share pictures of his last holiday trip. He will be a little cautious when sharing information like contact details stored in his phone. The same user will be extremely wary if information like credit card numbers or bank account numbers is compromised. Existing works mainly focus on the benefit achieved in terms of energy saved for a computation done in the cloud vis-à-vis a mobile phone. This trade-off does not take into account the decision on which data should reside in the cloud and the policy that governs the usage of such data. There are certain applications that are highly computation intensive and are better processed in the cloud. However if these applications use sensitive data, then the existing models for mobile cloud either fail to address the issue or applies a generic policy for all the data. Such generic policy may not be suitable for everyone. For example, if a policy requires data erasure every time a computation is performed then the user may incur heavy charges for bandwidth consumption during frequent data uploads to the cloud. Similarly, if policies are not rigid, the provider might end up pooling all information in the cloud, thereby risking security in case of an attack. This paper therefore considers aspects like amount of data that needs uploading

De S., Saha S. and K. Pal A..
Achieving Energy Efficiency and Security in Mobile Cloud Computing.
DOI: 10.5220/0004374204690474
In *Proceedings of the 3rd International Conference on Cloud Computing and Services Science* (CLOSER-2013), pages 469-474
ISBN: 978-989-8565-52-5

during a computation along with energy consumptions for providing necessary security to the data. Unlike existing works, the model looks at various facets like security, costs and efficiency to arrive at the final decision.

Very few works on energy efficient mobile cloud computing consider security of offloaded code and data as a concern. The MAUI architecture of Cuervo et al (2010) works in the client-server mode where decisions are taken during runtime on which methods should be remotely executed. The CloneCloud architecture (Chun et al., 2011) partitions applications into portions executing in the mobile phone and threads that migrate and execute in the cloud benefitting from cloud resources. The basic assumption is that it may be beneficial to upload data and code to the cloud as long as execution in the cloud is faster, more reliable and more secure. In this paper, we assume that execution and storage in cloud is not necessarily more secure unless proper security techniques are deployed. Most importantly, we point out that we can achieve both security and energy efficiency in most cases simply by categorizing data based on their sensitivity and user security policies along with user perception about the security offered by the cloud. ThinkAir architecture (Kosta et al., 2011) develops on MAUI and CloneCloud by exploiting parallelizability of method execution using multiple VM images. It also addresses on-demand resource allocation in the cloud for smart phone users. Zhang et al (2009) take into account security of elastic applications but they do not consider the effects of the security techniques on the energy efficiency achieved by the migrating weblets. Kumar and Lu (2010) provide a comprehensive mathematical model of energy savings in a mobile phone showing that computations that require high amount of data transfer while the number of instructions is relatively low should not be offloaded as they do not provide much energy savings or may lead to more energy consumption. They also conclude that if additional energy required to protect privacy and security is large then offloading to the cloud may not save energy. We propose an improved version of their model based on our framework and show that even after due considerations of security and privacy issues, offloading tasks to the cloud can save energy.

2 ENERGY EFFICIENT SECURITY FRAMEWORK

Our energy efficient security framework consists of the following building blocks: Data Layers, User Security Policy, Adversarial Model and Data Upload and Computation. We describe these below. Henceforth, we use the words user and organization interchangeably.

1) **Data Layers:** We classify user data into three categories namely sensitive (eg., credit card numbers), private (eg., appointments, calendar etc) and public (eg., scores in a game) which are in decreasing order of value to the user. This categorization helps in identifying and performing computation-intensive and energy consuming security algorithms (like encryption, decryption etc) in mobile phones only for those data and computations that bear a significant risk. It also decides where the data can be stored and in effect helps in limiting bandwidth usage for data transfers during computations on the data. Copies of each type of data are maintained in the mobile phone memory so that in case the phone is offline, it can still perform computations.
2) **User Security Policy:** User policies regarding data storage and computations are presented in Table 1. Policies may result due to regulatory restrictions, compliance requirements or resource availability.
3) **Adversarial Model:** We consider three levels of trust assigned to the cloud: honest, semi-honest and malicious (Goldreich, 2004). A virtual machine (VM) is honest if it computes correctly all functions and does not keep copies of data used in computations etc whereas semi-honest VMs may keep records of the unencrypted data on which the computation took place and hence perform additional, unauthorized computations on them. A malicious VM can compute incorrect function values and keep records of unencrypted data to perform additional, unauthorized computations on them, abort a protocol or collude with other malicious parties. A storage provider is honest if it does not reveal user data. Semi-honest storage providers try to glean as much information as possible from stored user data. A malicious storage provider can collude with other malicious providers and outside attackers to extract information from stored data. All data and computations in user mobile phone are secure.
4) **Data Upload and Computation:** DP 1 allows no data to be stored in the cloud. Under DP 2, sensitive data is uploaded to the cloud only when computations are to be performed on them. Other data can be uploaded beforehand. DP 3 allows

prior uploading of all data. Public data is uploaded to the cloud and stored there unencrypted. Under policy combinations (2,1), (2,2), (3,1) and (3,2) private data is encrypted before it is transferred to the cloud. However, to reduce the burden of encryption operations on the user we use Zhou & Huang's (2011) privacy preserving cipher policy attribute based encryption (PP-CP-ABE) and attribute based data storage (ABDS) scheme where users need to only partially encrypt the data before sending it to the encryption service provider (ESP) which completes the task of encryption. The data can be updated and the cloud can use the data for computations depending on the attribute related keys that it receives from the user.

Table 1: User Security Policies from user Perception.

Data Policy (DP)	Interpretation
DP 1: No data leaves the user permanently.	Cloud is malicious for storage.
DP 2: Data partly managed by third party service providers depending on sensitivity of data.	Semi-honest cloud for private data; malicious for sensitive data.
DP 3: Data managed fully by third party service providers irrespective of sensitivity.	Semi-honest cloud for private and sensitive data storage.
Computation Policy (CP)	**Interpretation**
CP 1: Computations are trusted.	Honest cloud for all computations.
CP 2: Computations are semi-trusted.	Honest cloud for computations on public/ private data; semi-honest/ malicious for sensitive data.
CP 3: Computations are untrusted.	Honest cloud for computations on public data; semi-honest/ malicious in case of private and sensitive data.

For (1,1) and (1,2) private data can be uploaded using any secure public-key encryption scheme. For (1,1) and (2,1), even sensitive data can be encrypted using any secure public-key encryption scheme while for (3,1) we can use the PP-CP-ABE and ABDS schemes. For on-the-fly data upload (for private data in (1,3) and sensitive data in (1,3) and (2,3)) the user uploads shares of the relevant portion of the data to different VMs in the same cloud. If at least one VM is honest, then the cloud is unable to recover the data. When prior data upload is allowed (for private data in (2,3) and (3,3) and sensitive data in (3,3)), it is stored encrypted using the PP-CP-ABE and ABDS schemes but access rights are distributed in shares to multiple VMs.

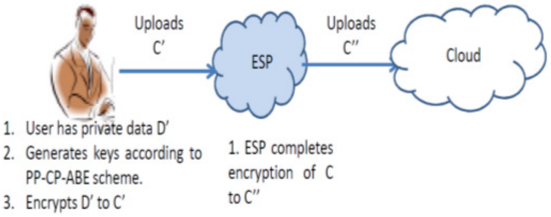
Uploads
C'
ESP
Uploads
C''
Cloud
1. User has private data D'
2. Generates keys according to PP-CP-ABE scheme.
3. Encrypts D' to C'
1. ESP completes encryption of C to C''

Figure 1: User with Policy Combination (2,2) Uploads Private Data.

In this scenario, computation of any function can be performed by using the concept of Kamara & Raykova (2011) where VMs participate in a multi-party computation of the given function on shared input and produce shares of the output.

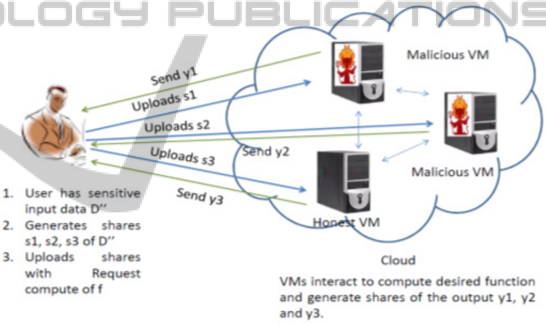
Send y1
Uploads s1
Uploads s2
Uploads s3
Send y2
Send y3
Malicious VM
Malicious VM
Honest VM
1. User has sensitive input data D''
2. Generates shares s1, s2, s3 of D''
3. Uploads shares with Request compute of f
Cloud
VMs interact to compute desired function and generate shares of the output y1, y2 and y3.

Figure 2: User with Policy Combination (2,2) Uploads Sensitive Data During Computation.

3 EXECUTION

The cloud replicates an image, maintained in at least three VMs, of the user mobile. In general, all computations take place in a single VM but computations on sensitive data use the images available in all the VMs. Mobile phone applications are exactly replicated in the cloud image (referred to as Im APP).

The user interface (UI) (refer to Figure 3) interacts with the user to support his requirements of data storage, update and running any application and the Cloud Interface (CI) interacts with the cloud for data upload, update or for running any application.

The Data Manager (DM) is responsible for classifying data as suggested by the user, storing and retrieving data and generating relevant information for identifying the data later. The Crypto Service (CS) performs all encryption/ decryption related tasks such as key generation, output reconstruction etc. The CS in CI also performs the initial encryption operation before delegating the rest of the task to the ESP for private data and generates shares of sensitive data before distributing them to its counterpart in different VMs. On receiving the encrypted data or a share and in some cases a function representation the CS counter-part sends them to the DM in Operations Module (OM).

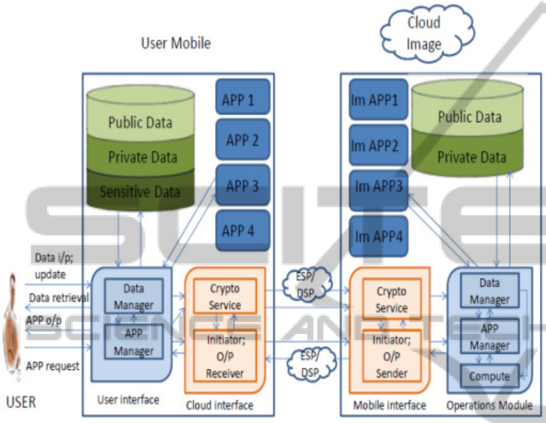

Figure 3: Implementing the conceptual framework through interactions between user mobile and cloud images in VMs.

On receiving user request for an application, the APP Manager (AM) finds out the type of computations and the data necessary for running it by referring to the particular application. Depending on the user policy, the AM either just sends the APP request to the Initiator sub-module in CI or sends the necessary representation of the functions to be computed for the application to the CS sub-module for encryption. The AM checks with the DM for the data and function and if function representation has not been received, it contacts the Im APP to know functions to be computed. The Initiator triggers a request for an application in its counter-part in MI. The Initiator counterpart also transmits the request application to the AM in OM. The Compute sub-module receives the shares or the data and the function and performs the computations.

4 ENERGY ANALYSIS

We propose the following generic energy consumption model (meaning of symbols appear in Table 2) where energy saved

$$
\begin{aligned}
&= \frac{\alpha_s C_1 + \alpha_{priv} C_2 + \alpha_{pub} C_3}{M} \times \left(P_C - \frac{P_i}{F}\right) \\
&- P_{tr} \times \frac{(\alpha_s + \alpha_{priv} + \alpha_{pub})}{B} - P_c \\
&\times \frac{\alpha_s C_S + \alpha_{priv} C_{priv} + \alpha_{pub}\, C_{pub}}{M} \\
&= \frac{\alpha_s C_1 + \alpha_{priv} C_2 + \alpha_{pub} C_3}{M} \times \left(P_C - \frac{P_i}{F}\right) \\
&- P_{tr} \times \frac{(\alpha_s + \alpha_{priv} + \alpha_{pub})}{B} - P_c \\
&\times \frac{(\alpha_s \beta_s C_1 + \alpha_{priv} \beta_{priv} C_2 + \alpha_{pub} \beta_{pub} C_3)}{M}
\end{aligned}
\qquad (1)
$$

Table 2: Symbols and values for energy analysis.

Symbol	Meaning	Values for example
$C_1/C_2/C_3$	number of instructions for sensitive/private/ public data per unit of data	$C_1 = C_2 = C_3 = 10$ per bit
M	speed (in instructions /second) of the mobile system	400
S	speed (in instructions/second) of the cloud server	$F = \frac{S}{M}$ $= 160$
B	network bandwidth	56 $Mbits$ $/sec$
$P_C/P_i/P_{tr}$	power consumed by mobile phone for computing/when transmitting data/when idle	$P_C = 0.9$ $P_i = 0.3$ $P_{tr} = 1.3$ (in watts)
C_S /C_{priv}/ C_{pub}	number of instructions for a security algorithm protecting sensitive/ private/ public data per unit data	
$\alpha_s/\alpha_{priv}/$ α_{pub}	amount of sensitive/ private/ public data required by the computation	α_s $= \alpha_{priv}$ $= \alpha_{pub}$ $= 5\ MB$
C	total number of instructions in a computation to be performed = $\alpha_s C_1 +$ $\alpha_{priv} C_2 + \alpha_{pub} C_3$	400 instruction s
$\beta_s/\beta_{priv}/$ β_{pub}	$\frac{C_S}{C_1} \left(\frac{C_{priv}}{C_2}, \frac{C_{pub}}{C_3}\right)$	β_{priv} $= \beta_s$ $= \beta_{pub}$ $= 1$

In the above model (see Table 3 for details) we ignore the bandwidth cost of initially uploading data (if any) to the cloud (as data upload needs to be done only once in a while), the requirement of policy combinations are given in Table 3 and Table 4.

computations for encryption before uploading such data etc. Also, we ignore fine-grain separation of privacy/security costs for different types of encryption schemes and other techniques used in different scenarios and the variations in the computations required by security algorithms used for different computation policies under a particular data policy. For e.g., under DP 2, β_s may vary for CP 1, CP 2 and CP 3. However the equations can be easily modified to take these into account.

Table 3: Energy analysis for different policy combinations.

Scenario	Data type needed for Computation	Data Requirements	Security/ Privacy related computation requirements	Energy Savings	Energy consumptions in example (units)
Scenario 1: Policy combinations (1,1), (1,2) and (1,3)	Sensitive	$\alpha_{priv} = 0;$ $\alpha_{pub} = 0;$ $\alpha_s > 0$	$\beta_{priv} = 0;$ $\beta_{pub} = 0;$ $\beta_s > 0$	$\frac{\alpha_s C_1}{M} \times \left(P_C - \frac{P_i}{F}\right) - P_{tr} \times \frac{\alpha_s}{B} - P_c \times \frac{\alpha_s \beta_s C_1}{M}$	1.830446
	Private	$\alpha_{priv} > 0;$ $\alpha_{pub} = 0;$ $\alpha_s = 0$	$\beta_{priv} > 0;$ $\beta_{pub} = 0;$ $\beta_s = 0$	$\frac{\alpha_{priv} C_2}{M} \times \left(P_C - \frac{P_i}{F}\right) - P_{tr} \times \frac{\alpha_{priv}}{B} - P_c \times \frac{\alpha_{priv} \beta_{priv} C_2}{M}$	1.830446
	Public	$\alpha_{priv} = 0;$ $\alpha_{pub} > 0;$ $\alpha_s = 0$	$\beta_{priv} = 0;$ $\beta_{pub} = 0;$ $\beta_s = 0$	$\frac{\alpha_{pub} C_3}{M} \times \left(P_C - \frac{P_i}{F}\right) - P_{tr} \times \frac{\alpha_{pub}}{B}$	0.9304464
	Mixed (mixture of public, private, sensitive)	$\alpha_{priv} > 0;$ $\alpha_{pub} > 0;$ $\alpha_s > 0$	$\beta_{priv} > 0;$ $\beta_{pub} = 0;$ $\beta_s > 0$	$\frac{\alpha_s C_1 + \alpha_{priv} C_2 + \alpha_{pub} C_3}{M} \times \left(P_C - \frac{P_i}{F}\right) - P_{tr} \times \frac{(\alpha_s + \alpha_{priv} + \alpha_{pub})}{B} - P_c \times \frac{(\alpha_s \beta_s C_1 + \alpha_{priv} \beta_{priv} C_2)}{M}$	1.530446
Scenario 2: Policy combinations (2,1), (2,2) and (2,3)	Sensitive	$\alpha_{priv} = 0;$ $\alpha_{pub} = 0;$ $\alpha_s > 0$	$\beta_{priv} = 0;$ $\beta_{pub} = 0;$ $\beta_s > 0$	$\frac{\alpha_s C_1}{M} \times \left(P_C - \frac{P_i}{F}\right) - P_{tr} \times \frac{\alpha_s}{B} - P_c \times \frac{\alpha_s \beta_s C_1}{M}$	1.830446
	Private	$\alpha_{priv} > 0;$ $\alpha_{pub} = 0;$ $\alpha_s = 0$	$\beta_{priv} = 0;$ $\beta_{pub} = 0;$ $\beta_s = 0$	$\frac{\alpha_{priv} C_2}{M} \times \left(P_C - \frac{P_i}{F}\right)$	0.001875
	Public	$\alpha_{priv} = 0;$ $\alpha_{pub} > 0;$ $\alpha_s = 0$	$\beta_{priv} = 0;$ $\beta_{pub} = 0;$ $\beta_s = 0$	$\frac{\alpha_{pub} C_3}{M} \times \left(P_C - \frac{P_i}{F}\right)$	0.001875
	Mixed	$\alpha_{priv} > 0;$ $\alpha_{pub} > 0;$ $\alpha_s > 0$	$\beta_{priv} = 0;$ $\beta_{pub} = 0;$ $\beta_s > 0$	$\frac{\alpha_s C_1 + \alpha_{priv} C_2 + \alpha_{pub} C_3}{M} \times \left(P_C - \frac{P_i}{F}\right) - P_{tr} \times \frac{\alpha_s}{B} - P_c \times \frac{\alpha_s \beta_s C_1}{M}$	0.611399
Scenario 3: Policy Combinations (3,1), (3,2) and (3,3)	Sensitive	$\alpha_{priv} = 0;$ $\alpha_{pub} = 0;$ $\alpha_s > 0$	$\beta_{priv} = 0;$ $\beta_{pub} = 0;$ $\beta_s = 0$	$\frac{\alpha_s C_1}{M} \times \left(P_C - \frac{P_i}{F}\right)$	0.001875
	Private	$\alpha_{priv} > 0;$ $\alpha_{pub} = 0;$ $\alpha_s = 0$	$\beta_{priv} = 0;$ $\beta_{pub} = 0;$ $\beta_s = 0$	$\frac{\alpha_{priv} C_2}{M} \times \left(P_C - \frac{P_i}{F}\right)$	0.001875
	Public	$\alpha_{priv} = 0;$ $\alpha_{pub} > 0;$ $\alpha_s = 0$	$\beta_{priv} = 0;$ $\beta_{pub} = 0;$ $\beta_s = 0$	$\frac{\alpha_{pub} C_3}{M} \times \left(P_C - \frac{P_i}{F}\right)$	0.001875
	Mixed	$\alpha_{priv} > 0;$ $\alpha_{pub} > 0;$ $\alpha_s > 0$	$\beta_{priv} = 0;$ $\beta_{pub} = 0;$ $\beta_s = 0$	$\frac{\alpha_s C_1 + \alpha_{priv} C_2 + \alpha_{pub} C_3}{M} \times \left(P_C - \frac{P_i}{F}\right)$	0.001875

We take the example of performing content-based image retrieval (CBIR) on a collection of images captured by a mobile phone. Here we consider that the total amount of data is 15 MB. We set the energy consumption ($0.9\,units$) when computed entirely in mobile phones as benchmark 1 and that ($2.578571\,units$) using Kumar and Lu's model as benchmark 2 (for numerical assumptions see Table 2). With respect to benchmark 1, our framework leads to decreased energy consumption for computations using only public (percentage improvement 99.79%) or only private (99.79%) or mixed (32.07%) for Scenario 2 and for all types of data (single or mixed) in Scenario 3 (99.79% both). With respect to benchmark 2, there has been decrease in energy consumption in all scenarios. The least energy consumption occurs in scenario 3 where no data is ever uploaded/downloaded during computation and the mobile phone need not perform any security related computation for computations in the cloud. The energy consumption for scenario 1 is relatively more (as compared to that for scenario 3) because all types of data must be uploaded/ downloaded and proper security computations relevant to the data have to be performed by the mobile phone whenever the computation uses such data.

The meanings of symbols used are presented in Table 2 and details of the model under different

5 FUTURE SCOPE

People and processes are an integral part of every organization. Without the cooperation from people, processes can hardly be a success. In the era of BYOD (bring your own device), there is a thin line between enterprise provided infrastructure and personal devices. This immediately leads to some very interesting extension of our work for the enterprise scenario. 1) Automatic identification and classification of organization specified sensitive data as outlined in policy 2) Identifying additional sensitive data and auto-protection overriding any user-imposed possible information leakage channels;

To better address energy efficiency vs. security issue we wish to look at cost and energy efficiency of offloading 1) when computing with real-time data; 2) assured deletion of data and preventing threats on control data (account-related data, battery consumption data etc). The framework has been proposed for mobile devices for energy efficiency. Security considerations and setup will be equally applicable for any computing device for end-users that needs protection from data leakage.

REFERENCES

Zhang, X., Schiffman, J.,Gibbs, S., Kunjithapam, A., Jeong, S.,2009. Securing Elastic Applications on Mobile Devices for Cloud Computing. In *CCSW'09, Proceedings of the 2009 ACM Workshop on Cloud Computing Security, pp. 127-134.*ACM.

Kosta, S., Aucinas, A.,Hui, P., Mortier, R., Zhang, X.,2011. Unleashing the Power of Mobile Cloud Computing using ThinkAir. In *arXiv:1105.3232*. arXiv.org.

Chun, B., Ihm, S., Maniatis, P.,Naik, M., Patti, A.,2011. CloneCloud: Elastic Execution between Mobile Device and Cloud. In *EuroSys'11, Proceedings of the 6th conference on Computer systems, pp. 301-314*. ACM.

Zhou, Z., Huang, D., 2011. Efficient and Secure Data Storage Operations for Mobile Cloud Computing.In *IACR Cryptology ePrint Archive 2011: 185(2011)*. IACR.

Kumar, K., Lu, Y., 2010. Cloud Computing for Mobile Users: Can Offloading Computation Save Energy? In *Computer Vol. 43, No. 4, pp. 51-56*. IEEE Computer Society.

Cuervo, E., Balasubramanian, A., Cho, D., Wolman, A.,Saroiu, S.,Chandra, R., Bahl, P.,2010. MAUI: Making Smartphones Last Longer with Code Offload. In *MobiSys'10, Proceedings of the 8th International Conference on Mobile Systems, Applications and Services, pp. 49-62*. ACM.

Kamara, S., Raykova, M., 2011. Secure Outsourced Computation in Multi-tenant Cloud. In *WCSC'11, Proceedings of the Workshop on Cryptography and Security in Clouds*. IBM.

Paczkowski, J., 2009.iPhone Owners Would Like to Replace Battery. In *AllThingsD.com, August 21, 2009*. Dow Jones.

Luo, X., 2009. From Augmented Reality to Augmented Computing: A Look at Cloud Mobile Convergence. In *ISUVR'09, Proceedings of the 2009 International Symposium on Ubiquitous Virtual Reality, pp. 29-32*. IEEE Computer Society.

Barham, P., Dragovic, B., Fraser, K., Hand, S., Harris, T., Ho, A., Neugebauer, R., Pratt, I., Warfield, A.,2003. Xen and the Art of Virtualization. In *SOSP'03, Proceedings of the 19th ACM Symposium on Operating systems principles, pp. 164-177*. ACM.

Goldreich, O., 2004. Foundations of Cryptography Volume II Basic Applications. Cambridge University Press.