ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2014

Security in Offloading Computations in Mobile Systems Using Cloud Computing

S.Masiperiyannan[1],C.M.Mehathaf Begum[2],I.Mohammed Farook Ali[3],G.Mayuri Priya[4],S.Sudhakar[5]

UG Student, Dept. of CSE, K S R College of Engineering, Tiruchengode, Tamilnadu, India[1,2,3,4]

Assistant professor, Dept. of CSE, K S R College of Engineering, Tiruchengode, Tamilnadu, India[5]

ABSTRACT- The progression in the technology has made very essential devices of such as aerial phones of late 80's and Pentium 4 processor into today's stock. None of them is comparable to the power of smart phones of this generation whose recent market has been reached its unbelievable height. We browse the Internet, send emails, organize our lives, watch videos, upload data on social networks, use online banking, find our way by using GPS and online maps, and communicate in revolutionary ways through smart phones. Many new apps are emerging at an incredible manner. We felt enthusiastic while using smart phones by installing and handling new apps, but less happy with the battery lifetime. Energy efficiency is the fundamental consideration for the mobile system. Cloud computing has the potential to save mobile client energy. But the savings from offloading the computations need to exceed the energy cost of the additional communication. If the apps are more computational intensive they can be offloaded or else they can be run in the mobile system itself. Offloading can be done from mobile system to grid-powered servers where computations are performed. Offloading depends on various parameters such as energy consumption and bandwidth. Offloading, however, causes privacy concerns because sensitive data may be sent to servers. The privacy can be protected by using two techniques such as Encryption of data and Steganography in computation offloading.

KEYWORDS: Bandwidth, Battery lifetime, Cloud Computing, Computations, Encryption, Offloading, Smart Phones, Steganography

I. INTRODUCTION

Nowadays mobile system has become the computing platform for many a users. It is also concerned that battery lifetime is the most desired feature of such system. A 2005 study of users in 15 countries found longer battery life to be more important than all other features, including cameras or storage. A survey at 2008 by Change Wave Research revealed short battery life to be the most disliked characteristic of Apple's iPhone 3GS, while a 2009 Nokia poll showed that battery life was the top concern of music phone users. Many applications are too computation intensive to perform on a mobile system. If a mobile user wants to use such applications, the computation must be performed in the cloud. Other applications such as image retrieval, voice recognition, gaming, and navigation can run on a mobile system. However, they consume significant amounts of energy.

II. LITERATURE SURVEY

Yang, K., Ou, .S and Chen, .H.H (2008) 'On Effective Offloading Services for Resource-Constrained Mobile Devices Running Heavier Mobile Internet Applications' describes that Rapid advances in wireless mobile network technologies and mobile handsets (MHs) facilitate ubiquitous infrastructure that can support a range of mobile services and applications in addition to conventional mobile Internet access. One recent trend is to effectively run desktop PC-oriented heavier applications on MHs. However, due to their miniature, portable size, MHs are resource-constrained and therefore, running these applications directly on an MH is not satisfactory given a user's expectations. To cope with this problem, this article proposes a novel offloading service that can seamlessly offload some of the tasks of a mobile application from an MH to nearby, resource-rich PCs (called surrogates).The system architecture and key components of the proposed offloading service are presented, prototyped, and evaluated. The results of experiments and simulations have demonstrated the effectiveness and efficiency of this offloading service for mobile applications.[13]

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2014

Fridrich et al. (2001) 'Detecting LSB Steganography in Color and Gray-scale Images' describe a reliable and accurate method for detecting least significant bit (LSB) non-sequential embedding in digital images. The secret message length is derived by inspecting the lossless capacity in the LSB and shifted LSB plane. An upper bound of 0.005 bits per pixel was experimentally determined for safe LSB embedding.[3]

Wolski, R. et al (2008) 'Using Bandwidth Data to Make Computation Offloading Decisions' present a framework for making computation offloading decisions in computational grid settings in which schedulers determine when to move parts of a computation to more capable resources to improve performance. Such schedulers must predict when an offloaded computation will outperform one that is local by forecasting the local cost (execution time for computing locally) and remote cost (execution time for computing remotely and transmission time for the input/output of the computation to/from the remote system). Typically, this decision amounts to predicting the bandwidth between the local and remote systems to estimate these costs. Our framework unifies such decision models by formulating the problem as a statistical decision problem that can either be treated "classically" or using a Bayesian approach. Using an implementation of this framework, we evaluate the efficacy of a number of different decision strategies (several of which have been employed by previous systems). Our results indicate that a Bayesian approach employing automatic change-point detection when estimating the prior distribution is the best-performing approach. [12]

Chandramouli et al. (2004) 'Image Steganography and Steganalysis: Concepts and Practice' reported that over some general concepts and ideas that apply to steganography and steganalysis. Specifically we establish a framework and define notion of security for a steganographic system. We show how conventional definitions do not really adequately cover image steganography and an provide alternate definition. We also review some of the more recent image steganography and steganalysis techniques[6]

Miettinen, A. and Nurminen, J. (2010) 'Energy efficiency of mobile clients in cloud computing' describes that energy efficiency is a fundamental consideration for mobile devices. Cloud computing has the potential to save mobile client energy but the savings from offloading the computation need to exceed the energy cost of the additional communication. In this paper they provide an analysis of the critical factors affecting the energy consumption of mobile clients in cloud computing. Further, they present their measurements about the central characteristics of contemporary mobile handheld devices that define the basic balance between local and remote computing. They also describe a concrete example, which demonstrates energy savings. They show that the trade-offs are highly sensitive to the exact characteristics of the workload, data communication patterns and technologies used, and discuss the implications for the design and engineering of energy efficient mobile cloud computing solutions.[6]

Wang, C. and Li, Z (2004) 'Parametric Analysis for Adaptive Computation Offloading' says that many programs can be invoked under different execution options, input parameters and data files. Such different execution contexts may lead to strikingly different execution instances. The optimal code generation may be sensitive to the execution instances. In this paper, we show how to use parametric program analysis to deal with this issue for the optimization problem of computation offloading. Computation offloading has been shown to be an effective way to improve performance and energy saving on mobile devices. Optimal program partitioning for computation offloading depends on the tradeoff between the computation workload and the communication cost. The computation workload and communication requirement may change with different execution instances. Optimal decisions on program partitioning must be made at run time when sufficient information about workload and communication requirement becomes available. Our cost analysis obtains program computation workload and communication cost expressed as functions of run-time parameters, and our parametric partitioning algorithm finds the optimal program partitioning corresponding to different ranges of run-time parameters. At run time, the transformed program self-schedules its tasks on either the mobile device or the server, based on the optimal program partitioning that corresponds to the current values of run-time parameters. Experimental results on an HP IPAQ handheld device show that different run-time parameters can lead to quite different program partitioning decisions.[11]

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2014

III. OFFLOADING COMPUTATIONS TO SAVE ENERGY

If the computations are too computational intensive the mobile system does not perform the computations; instead, computation is performed somewhere else, thereby extending the mobile system's battery lifetime. The cloud computing is distinguished from the existing model of adoption of virtualization in which instead of service providers managing programs running on servers, virtualization allows cloud vendors to run arbitrary applications from different customers on virtual machines. Cloud vendors thus provide computing cycles, and users can use these cycles to reduce the amounts of computation on mobile systems and save energy. Thus, cloud computing can save energy for mobile users through *computation offloading*. Virtualization, a fundamental feature in cloud computing, lets applications from different customers run on different virtual machines, thereby providing separation and protection. When computations are high and bandwidth is also high, offloading can be done. As shown in the Fig.1 Offloading can beneficial only when large amount of computations C are needed with relatively small amount of Communications D.

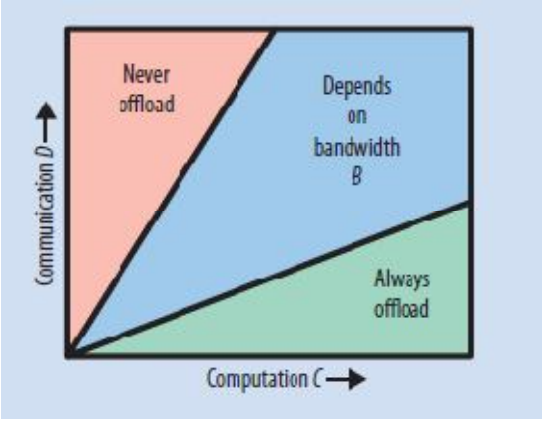

Fig.1 when computations are high and bandwidth is also high, offloading can be done.

IV. ENERGY ANALYSIS DURING OFFLOADING

Suppose the computation requires C instructions. Let S and M be the speeds, in instructions per second, of the cloud server and the mobile system, respectively. The same task thus takes C/S seconds on the server and C/M seconds on the mobile system. If the server and mobile system exchange D bytes of data and B is the network bandwidth, it takes D/B seconds to transmit and receive data. The mobile system consumes, in watts, Pc for computing, Pi while being idle, and P_{tr} for sending and receiving data. (Transmission power is generally higher than reception power, but for the purpose of this analysis, they are identical.)If the mobile system performs the computation, the energy consumption is $Pc \times (C/M)$. If the server performs the computation, the energy consumption is $[Pi \times (C/S)] + [P_{tr} \times (D/B)]$. The amount of energy saved is

$$P_c \times \frac{C}{M} - P_i \times \frac{C}{S} - P_{tr} \times \frac{D}{B}. \quad (1)$$

Suppose the server is F times faster that is, $S = F \times M$. We can rewrite the formula as

$$\frac{C}{M} \times \left(P_c - \frac{P_i}{F}\right) - P_{tr} \times \frac{D}{B}. \quad (2)$$

Energy is saved when this formula produces a positive number. The formula is positive if D/B is sufficiently small compared with C/M and F is sufficiently large.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2014

P_c	Computation power	U	Speed of mobile system
P_t	Network power	S	Speed of server
P_i	Idle power	B	Bandwidth of network

Table.1 Parameters of Offloading

The analysis indicates that the energy saved by computation offloading depends on the wireless bandwidth *B*, the amount of computation to be performed *C*, and the amount of data to be transmitted *D*. Existing studies thus focus on determining whether to offload computation by predicting the relationships among these three factors. However, there is a fundamental assumption under-lying this analysis with the client-server model: Because the server does not already contain the data, all the data must be sent to the service provider. The client must offload the program and data to the server. For example, typically a newly discovered server for computation offloading does not already contain a mobile user's personal image collection. However, cloud computing changes that assumption: The cloud stores data and performs computation on it. For example, services like Google's Picasa and Amazon S3 can store data, and Amazon EC2 can be used to perform computation on the data stored using S3.This results in a significant change in the value of *D* for most applications. There is no longer a need to send the data over the wireless network; it suffices to send a pointer to the data. Also, the value of *F* is elastic: Large numbers of processors can be obtained on the cloud. This increases the energy savings in Equation 2: A very small *D* and very large *F* imply that energy can always be saved.

V. PRIVACY AND SECURITY

In cloud computing, offloading of data to the cloud has implications for privacy and security. Because the data is stored and managed in the cloud, security and privacy settings depend on the IT management the cloud provides. A bug or security loophole in the cloud might result in a breach of privacy. For example, in March 2009, a bug in Google caused documents to be shared without the owners' knowledge,9 while a July 2009 breach in Twitter allowed a hacker to obtain confidential documents. Cloud service providers typically work with many third-party vendors, and there is no guarantee as to how these vendors safeguard data. For example, a phishing attack in 2007 duped a staff member for salesforce.com into revealing a password;13 the attacker then used the password to access confidential data. Obviously, Some type of data cannot be stored in the cloud considering the privacy and security issues. One possible solution is to encrypt the data before offloading. But encryption alone cannot solve the problem. A technique called Steganography is also used in the proposed system to hide the data from the cloud vendor.

VI. ENCRYPTION OF DATA

The data can be encrypted in the mobile system itself before offloading. Here Random Key Generation Algorithm is used. The mobile user can encrypt the data before offloading to the cloud using the random key generated. The cloud vendor before performing computations in it requests for the key to the mobile users, then the cloud vendor after receiving the key decrypts the data and performs computations in it.

VII. STEGANOGRAPHY

Steganography is to hide data before sending them to servers so that unauthorized access of data can be prevented. Steganography hides data so that the server is unaware of the existence of information. Image processing is computation-intensive and a good candidate for offloading. Fig.2 shows two examples of steganography. A *cover image* is used to disguise the *data image* so that the data image is hard to recognize. The combined image is called a *stego image.* A key challenge is to allow offloaded computation to be performed on steganographic data because the computation must remain meaningful on stego images. Suppose we want to compare the images in Figure 2 (b) and (c), Figure 2 (d) and (e) are sent to the server instead. Figure 2 (f) shows the pixel-wise difference between (d) and (e). Since the cover image is never sent to server, the server cannot detect hidden data

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2014

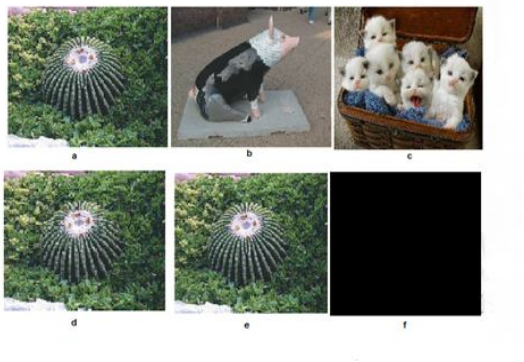

Fig.2 Two examples of steganography. (a) is the cover image. (b), (c) are hidden in (a) and their corresponding stego images are (d) and (e). (f) is the difference of (d) and (e)

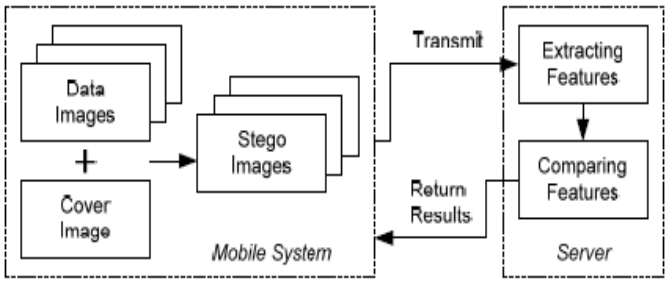

Fig.3 Offloading image computation protected by Steganography

As shown in Fig.3, before sending the data to the server, the images are processed using steganography. The stego images are sent to the server for further processing. The adopted protection techniques must ensure the computation performed at the server remains meaningful. Mean-while, the hidden data must be difficult for the server to detect.

VIII. ENERGY CONSUMPTION MODEL

With Steganographic protection, original data *D* are first protected by protection scheme *P*. The protected data D' are sent to the server and processed by the program C' to generate the result R'. This result *R'* is returned to the mobile system and finally the result *R''* is produced using the inverse protection P_i. To process the protected data, some modification to the program may be required. Hence, the program *C0*is possibly different from *C*. The final result *R''* must be acceptable compared with *R*. Ideally, *R00* is the same as *R*. However, due to various reasons, they may be different; as a result, the quality of the program may be degraded when data are protected.

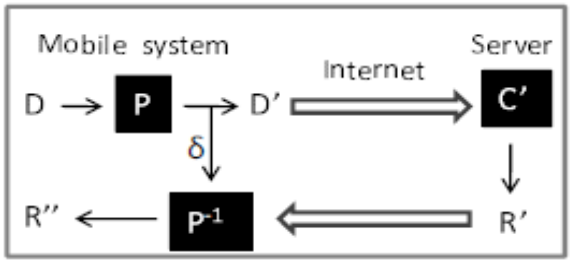

Fig.4 Offloading a program with protection. The data are protected by *P* and *D'* are sent to the server. *R'* is returned and produces the final result *R''*

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2014

In Fig.4, data *D* are protected by *P*; *D'* are offloaded and *C'* is performed at the Parameters for offloading *Pc* Computation power *U* Speed of mobile system *Pt* Network power *S* Speed of server *Pl* Idle power *B* Bandwidth of network server; *R0* is returned to the mobile system and processed by the inverse protection $P_i 1$. Hence the total energy consumption includes computation energy for performing *P* and P_i, idle energy when the server runs *C'*, and transmission energy for sending data *D0* and receiving *R'*.

$$P_c \times \frac{comp(P + P^{-1})}{U} + P_l \times \frac{comp(C')}{S} + P_t \times \frac{size(D' + R')}{B} \quad (3)$$

To save energy, we have to find *P* and P_i that do not require excessive amounts of computation, and the sizes of transmitted data *D'* and *R'* are small. Meanwhile, *R''* must be sufficiently close to *R*.

IX. CONCLUSION

In the cloud, computing and storage resources are virtualized. Analysis suggests that cloud computing can potentially save energy for mobile users. Not all applications are energy efficient when migrated to the cloud. Mobile cloud computing services would be significantly different from cloud services for desktops Offer energy savings. There are a variety of data security techniques available. Security, quality and the size are the key factors that analyzed in this research work. This research work is done in the area of Encryption and Steganography. The steganography process uses images to hide the data. Using Java the studied tool is developed. The system is tested with different combination of process in different order. The final solution of the study is encryption and data hiding is to improve the security and reduce the size of secret data process.It is concluded that the application works well and it is tested very well and are properly debugged. The site is simultaneously accessed from more than one system. Simultaneous login from more than one place is tested.

REFERENCES

[1]K. Kumar and Y. H. Lu, "Cloud computing for mobile users: Can offloading computation save energy?" IEEE Computer, vol. 43, no. 4, pp. 51–56, April 2010

[2]A. Miettinen and J. Nurminen, "Energy efficiency of mobile clients incloud computing," in Proc. of Hot Cloud, pp 27-56,2010

[3]Hong et al. Energy Efficient Content-Based Image Retrieval for Mobile Systems. In *ISCAS*, pages1673-1676, 2009

[3]T-Mobile Forums, "A Message from Our Chief Operations Officer, Jim Alling," 6 Oct. 2009; http://forums.t-mobile.com/t5/Previous-Sidekick-Models/A-Message-From-Our-Chief-Operations-Officer-Jim-Alling/m-p/200661.

[4]J. Paczkowski, "Iphone Owners Would Like to Replace Battery," *All Things Digital, 21 Aug. 2009;*

[5]Datta et al. Image Retrieval: Ideas, Infuences, and Trends of the New Age. In *ACM Computing Surveys*,pp{34-94} 2008.

[6]R. Wolski et al., "Using Bandwidth Data to Make Computation Offloading Decisions," *Proc. IEEE Int'l Symp. Parallel and Distributed Processing (IPDPS 08), 2008, pp.{ 1-8}*

[7]R. McMillan, "Salesforce.com Warns Customers of Phishing Scam," *PCWorld*, 6 Nov. 2007; http://www.pcworld.com/businesscenter/article/139353/salesforcecom_warns_customers_of_phishing_scam.html.

[8]C. Wang and Z. Li, "Parametric Analysis for Adaptive Computation Offloading," *ACM SIGPLAN Notices, vol. 39, no. 6, 2004, pp. {119-130}*

[9]Zhang et al. Steganography with Least Histogram Abnormality. In *Computer Network Security, pp {*395-406}, 2003.

[10]Fridrich et al. Detecting LSB Steganography in Colorand Gray-scale Images. In *IEEE Multimedia,* volume 8, pages 22{28, 2001.