Smartphone Security by Cloud Computing

Ria Das
Tata Consultancy Services, Kolkata, India

Indrajit Das
Department of Computer Science and Engineering
Meghnad Saha Institute of Technology

Abstract- Smartphone usage has been continuously growing in recent times. Smartphones offer Personal Computer (PC) functionality to the end user, hence they are vulnerable to the same sorts of security threats as desktop computers. Cloud computing is a new computing paradigm and a breakthrough technology of recent times. Its growing popularity can be attributed to its ability to transform computing to a utility, scalability, and cost effectiveness. More and more services are predicted to be offered in the cloud in the near future. Due to the resource constraints of smartphones, security services in the form of a cloud very scalable form in the cloud while off-loading the smartphone.

This paper proposes a generic architecture for providing security services in the cloud for smartphones. To enable the design of this architecture, it is essential to analyze and identify possible security solutions that could be provided as a cloud service to the smartphone. Security requirements of smartphones have been analyzed considering the various infection channels for smartphones, attacks and threats encountered in a smartphone environment, smartphone usage scenarios and the smartphones limitations. Next, the security functions that must be implemented in the smartphone to overcome these threats are identified. Furthermore, a review of the existing architectures for mobile computing are presented and their security issues are examined.

A detailed study of the analyzed results has been used to build the architecture for offering security services to smartphones in the cloud, targeted use case scenario being the usage in a corporate environment. The functions to be handled by each of the components of the architecture have been specified. Furthermore, the proposed architecture has been examined to prove its feasibility by analyzing it in terms of its security aspects, scalability and flexibility.

Keywords – Smartphone , Cloud Computing, Clone Cloud Architecture, Paranoid Android

I. INTRODUCTION

Over the last decade, the popularity of handheld devices such as Personal Digital Assistants (PDAs) and smartphones have increased tremendously. Gartner forecasts that the number of smartphones will exceed the number of Personal Computers (PCs) by 2013 [1]. Rich personal data and/or corporate data are increasingly stored in smartphones. In most cases there is little concern being given to the security of this information. Cisco's annual Internet security threat report predicts that criminals are already targeting smartphones, rather than traditional Microsoft Windows PCs [2]. The resource constraints of these devices seem to be a major limiting factor preventing them from supporting more powerful security. Offloading computationally intensive security services to the cloud could be extremely beneficial for users of these smartphones.
The simplicity and scalability that cloud computing offers has attracted the attention of both users and organizations. The United States Federal IT Market forecasts cloud computing as one of the technology segments that will witness double digit growth between 2011 and 2015 [3]. The application of cloud computing in mobile phones has caught the attention of researchers worldwide as there is a good match between these resources constrained handheld devices and the resource abundant cloud.

A. Problem Description

The mobile computing paradigm has seen tremendous advancements in recent times. Smartphones have emerged as a type of mobile device providing “all-in- one” convenience by integrating traditional mobile phone functionality and the functionality of handheld computers. Various models of smartphones have been released catering to the various demands of mobile users. Today smartphones offer PC-like functionality to end users allowing them to check their e-mail, maintain calendars, browse the internet, watch videos, play music, etc. In addition to these

functions, they are also used for privacy sensitive tasks such as on-line-banking - these tasks make them an attractive platform for attackers. Enormous numbers of applications are being developed for each of the mobile operating systems (OSs) and each application has its own security requirements and vulnerabilities. Heterogeneity in hardware, software, and communication protocols to connect to the Internet for all of the different smartphones add complexity when attempting to definite security functions for smartphones. This heterogeneity also increases the difficulty in designing, implementing, and testing applications for these smartphones.

Storing personal data on the smartphone has become a common practice. Awareness of the risks associated with smartphone usage is relatively low when compared to the awareness of risks for desktop computers. Sensitive data such as email and bank passwords are frequently stored by users in an unsafe manner on their smartphones. These poor security practices attract attackers to concentrate on smartphone platforms in order to exploit the vulnerabilities of the smartphone OSs and application software, as well as user generated vulnerabilities. Therefore, there is a growing need to address the security risks associated with smartphones.

Although there seems to be significant developments in terms of available computing power, local storage, and other capabilities of smartphones in comparison to so called "feature phones", desktop computing devices have evolved to a much greater extent – especially with respect to security. Part of the reason for this may be that desktop computers have been programmable by users for many decades, while only in recent years has it been possible for more than a very small and carefully controlled group of developers to create software for a mobile phone.

Offloading computation from resource constrained devices has been an area of focus for researchers. This aim of this paper is to improve the perceived performance of mobile devices by utilizing the broadband wireless connectivity of these devices. Security functions such as anti-virus scanning are resource intensive and additionally this computation and associated memory activity will deplete the battery power of the smartphone. Cloud computing seems to be a good fit by shifting the computation from the mobile devices to the cloud, hence exploiting the computational power of the cloud and the fact that the cloud computers are provided with mains power. This suggests that if there are computationally intensive security services that can be migrated to the cloud, then Security as a Service for smartphones is one way in which improved security could be offered as a service in the cloud for the users of smartphones.

In a corporate organization set up, sensitive corporate data is stored by each employee of the company. With the use of smartphones, the tendency to use a smartphone for official purposes is also on the rise as it is quite handy. For example, carrying mobile phones to meetings instead of using laptops. Therefore, it becomes highly important to protect the information from being disclosed and misused by external entities. Furthermore, it becomes necessary to ensure that the employees abide by the policies of the company to ensure security.

B. Background

Smartphones

Smartphones are a category of mobile phones which are "smart" (i.e., more capable) when compared to traditional mobile phones. Smartphones are targeted to address the need for a pocket PC in addition to a phone. As a result they offer many features which are not usually associated with mobile phones, such as the ability to run downloaded software applications, web browsing capabilities, etc.

Cloud Computing

Cloud computing has emerged as a new computing paradigm providing hosted services by exploiting the concept of dynamically scalable and shared resources accessible over the internet. A cloud service is rented on demand, i.e. based on the customer's current requirements. Because the cloud provider can dynamically allocate virtual processors to their customers, cloud computing is highly scalable, hence the user can have as much or as little service as he or she wants at any given time. Depending on the type of the cloud service rented, the responsibility of the user in managing the service varies.

By utilizing subscription based payment for resources and services a customer can substantially reduce their operational and capital costs. Cloud computing caters to the customer's needs by offering a way to rapidly increase capacity when needed or to add new capabilities on the fly while minimizing investments in new infrastructure, training new personnel, licensing new software, etc.

II. SMARTPHONE SECURITY

A. Security Objectives

A well secured system should provide confidentiality, integrity, availability, and accountability. We will describe each of these security objectives in more detail below.

Confidentiality

Confidentiality refers to preserving the privacy or secrecy of information, i.e. preventing unauthorized disclosure. This requires that the information be kept in encrypted form and that only an authorized party can access this information in unencrypted form. In a smartphone, the confidentiality of information that is stored in the phone and that is transmitted from the phone should be ensured – this implies that (1) the information is kept in encrypted form or that the physical & logical device has to be protected and (2) that only encrypted information is transmitted (thus just before transmission is the *last* time that the information could be in an unencrypted form).

Integrity

Integrity refers to the protection of information from unauthorized, uncontrolled, or accidental alterations. Proper authentication, authorization, and access control mechanisms can help protect the integrity of data. Maintaining information integrity refers to the protection of data from attacks and disaster. In the case of a smartphone, this requires integrity checks of the operating system and application software, ensuring the integrity of the data that is stored and transmitted over the network, and protecting the smartphone data in case of theft (this last implies that there is a copy of the data stored in a location other than in the phone – hence this other copy could be accessed if the physical phone is stolen). The copy of the data that is stored separately from the phone is often referred to as a backup copy of the data. In this way, it is possible to recover an unaltered version of the smartphone data. This data can be stored either in one location or spread in a redundant fashion across multiple servers. (See for example the cryptographically redundant storage of encryption keys in [4].)

Availability

The system needs to provide service preferably without interruptions, but in any case there should be rapid recovery after a service interruption. The importance of this objective depends on how crucial the service is to the on-going needs of the person or organization that depends upon this service. In the case of network attached systems, the system should be resistant to Denial of Service (DoS) Attacks. DoS attacks could be made against the smartphone itself or against the service. DoS attacks should be avoided in order to ensure availability of service to the smartphone users.

Accountability

Accountability refers to the ability to account for the activities of an individual or an entity in the system. This can be implemented by utilizing logging and monitoring services within the system. These logs can be used to prevent individuals from denying their actions, thus achieving non-repudiation. Logs might also be important for understanding *retrospectively* what happened when a fault, error, fraud, or intrusion is discovered. Accountability could be very important for corporate smartphone usage, as a corporate smartphone user might be subjected to a variety of policies and regulations.

Additionally, these corporate users might even have restrictions on whom they can communicate with in order to enforce limitations on the spread of information or to prevent access to information that is not permitted.

B. Threats on Smart Phone

In earlier times the probability of mobile phone threats were comparatively low when compared to PCs, as the devices generally were **not** programmable by anyone other than the vendor and the phones themselves were generally behind firewalls and network address translation devices operated by the network operator. Today smartphones offer PC like functionalities, hence are at risk of being attacked by similar threats to those encountered by PCs. Malware can be installed on the phone via Short Message Service (SMS) messages, Multimedia Messaging Service (MMS) messages, email, documents, web pages, etc.

The portability, convenience of usage and the functionalities of smartphones help their users to perform day-to-day activities such as sending e-mails, social networking, on-line banking, etc. – thus users will enter (and may also store) sensitive information on their devices. For many users their smartphone is the device that they use to access nearly all services, hence such a smartphone is a high value target for attackers. Note that these attacks can take the form of passive attacks based upon accessing sensitive information (for example, bank account & PIN number) or they can be active attacks (for example, causing the phone to send premium SMS messages or place calls to premium numbers operated by the attacker).

A number of different kinds of threats that affect smartphones are Denial of Service attacks (DOS), Malware, Social Engineering attacks, Theft, etc.

C. Infection Channel

Smartphones can become infected through a wide range of infection routes. The following subsections detail each of the possible infection channels.

Bluetooth

It requires the smartphone's Bluetooth connection to be switched on, sufficient signal strength, and that the phone is in its discoverable mode. Because there are no intermediaries between the infected device and a potential victim it is difficult to remotely monitor this infection route.

SMS/MMS

Malicious software can spread to mobile devices by attaching a copy of itself to an SMS/MMS that is sent from the infected mobile device.

Internet Connectivity

Smartphones run similar risks as fixed devices to become infected through viruses contained in downloaded files, cross site scripting, etc.

Portable Memory

Usage of secure digital memory cards is commonplace in smartphones. Many smartphones such as the Samsung S8500 Wave [5] can support up to 32 GB SD memory cards. Cardtrap is a trojan that affects Symbian smartphones by installing several Windows viruses, worms and trojans to the phone's Multimedia Card (MMC) [6].

D. Limitations

Smartphones have traditionally had more limited computational capacity and storage, while the users have different expectations of the operating time of smartphones than they do for their laptop. While the regular operations of a smartphone can have significant impact on energy consumption, resource intensive security functions such as an anti-virus scan through all the data in the smartphone and real-time virus scanning (running in the background) can deplete battery resources rapidly. This implies that either such an approach to virus checking should **not** be done or that this operation should be offloaded to a resource rich computing environment.

III. EXISTING ARCHITECHTURE

A. Opera Mini

The Opera Mini architecture has been discussed in [8] and [9]. Opera Mini is a mobile web browser designed specifically for smartphones and PDAs. The architecture of Opera Mini which is very similar to the earlier Wireless Application Protocol (WAP) model. The mobile phone only needs to support Java in order to run the Opera Mini client.

Drawbacks

- The Opera Mini browser in the mobile phone fetches the contents of the website through the Opera Mini server which acts as a proxy server that can translate Hypertext Mark-up Language (HTML) with Cascading Style Sheets (CSS) into a more compact format.
- No end to end encryption performed, so confidentiality is compromised and if performed is at the cost of performance.
- No security is provided against social engineering attacks, Malware, DoS, and theft of the smartphone.

B. Blackberry Enterprise Architechture

The BlackBerry® Enterprise Architecture is an integrated solution from the Research in Motion (RIM) Group. This architecture consists of the BlackBerry Enterprise Server (BES) and the other components of the "BlackBerry Infrastructure". The BlackBerry Enterprise Architecture is considered a robust architecture in terms of security [10].

Drawbacks

- BlackBerry Architecture is a closed system hindering further exploration and/or exploitation.
- Security functions are limited to the BES and the BlackBerry infrastructure components.
- When the BlackBerry device communicates with another device outside the BlackBerry infrastructure, most of the security features may be unavailable.

C. Paranoid Android

Portokalidis et al. proposed Paranoid Android in [11]. Paranoid Android offers versatile protection for smartphones. This architecture views security as just another service at a higher level that can be hosted in the cloud. The basic idea is to run a synchronised replica of the smartphone in a security server in a cloud. Since the cloud server has abundant resources, intensive security checks are carried out in the clone in the security server of the cloud.

Drawbacks

- Paranoid Android architechture focuses on **attack detection** like Zero day attacks and memory resident attacks, DOS, Social engineering attacks, theft but cannot prevent their occurrences.
- No encryption of data is done in smartphones or during data transit, so no confidentiality is provided. The proxy server is not well protected – can get effected by threats like cache poisoning.
- It is susceptible to man – in – the – middle – attack as no secure connections are adopted.

D. Clone cloud Architecture

Distribution of computation between the smartphones and the cloud resources in the form of clone cloud architecture has been suggested by Chun and Maniatis [12]. The concept behind the clone cloud architecture is to seamlessly offload execution from the smartphone to a computing infrastructure. Resource intensive processes or

portions of processes are performed by the smartphone clone in the cloud. These results are then merged with the state of the smartphone which resumes execution. The clone can also be used as a backup if the smartphone is lost.

Drawbacks

This architecture doesn't security for smartphones though it presents an effective method for computation offloading from the mobile devices.

E. Smartphone Mirroring Architecture

Zhao et al. [13] propose a framework to keep the mirrors of smartphones on a computing infrastructure in a telecommunications network thereby offloading heavy computations to the mirror. The mirror server in the telecommunications network is capable of hosting a large number of virtual machines. Synchronisation between the smartphone and the mirror is achieved by replaying all the inputs to the smartphone in the same order at the mirror.

Drawbacks

The mirroring smartphone approach does not concentrate on providing security services to the mobile phones. This architecture only connections through 3G networks- no Wi-fi or bluetooth connections.

II. PROPOSED ARCHITECHTURE

The basic concept behind the proposed architecture for smartphones is shown in Figure 1 where some of the security services are offloaded to the cloud environment. It portrays smartphones at one end and the cloud server offering the security services to the smartphone on the other end.

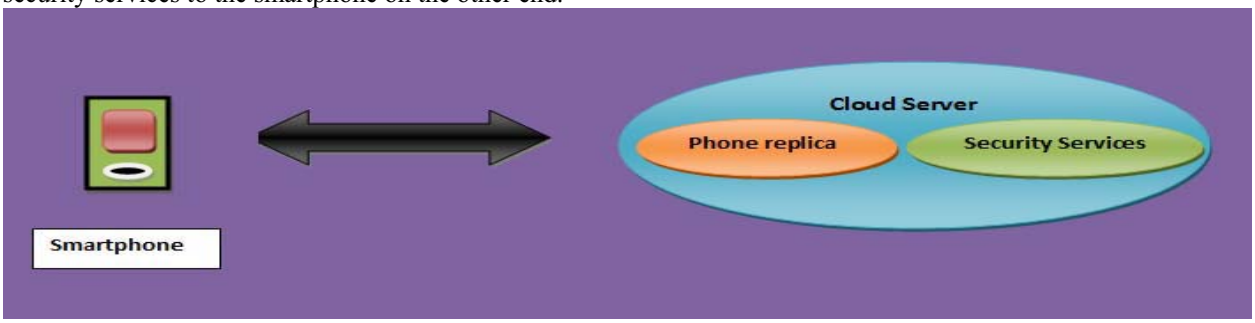

Figure 1. Basic proposed Architecture

The architectural framework depicted in Figure 2 is an extension of the basic concept depicted in Figure 1 and encompasses smartphones as the end device, a server farm in the cloud which includes a proxy server which controls the traffic in and out of the mobile device, and additional servers to realize cloud services that provide security services to smartphones.

Multiple virtual machines for the replicas could be run in the cloud server as and when needed. The security functions can be deployed either in the replica Virtual Machine (VM) or in the native OS of the cloud server based on the kind of functionality it provides to the smartphone. Each virtual machine uses hardware virtualization on top of the physical hardware of the cloud server.

A replica of a smartphone can be thought of as a copy maintained in the same state as the state of the smartphone. This means that the copy contains the smartphone OS files and files accepted by the user to be synced to the replica. There are many ways for creating and maintaining the replica in the cloud. The components of the proposed architecture include a sync module, an interpreter, and the controller in the smartphone; sync module and service manager in the replica and security functions in the cloud server; the cloud based proxy server and the backup servers. Figure 3 shows the components of the smartphone and the cloud in the proposed architecture.

A. Brief overview of components

The Sync Module in the phone and the replica VM are responsible for synchronizing the states of the smartphone and the replica. This synchronization can either occur at fixed time intervals or be an on-demand synchronization approved at the discretion of the controller in the smartphone. This controller can make its decision based on available bandwidth, estimation of possible energy consumption, and estimated energy consumption before the smartphone will be recharged. Furthermore, the controller can also be used to decide which security functions are most appropriate to offload depending on the network conditions in which the smartphone is most likely to operate and limitations of the specific smartphone based on its technical specifications. The service manager in the replica VM is responsible for the execution of the security functions and sending the results to the interpreter in the

smartphone. A cloud based proxy is used to provide anonymity service, intercept the incoming and outgoing traffic to be acted upon by the security functions, providing a caching service, and implementing a firewall service.

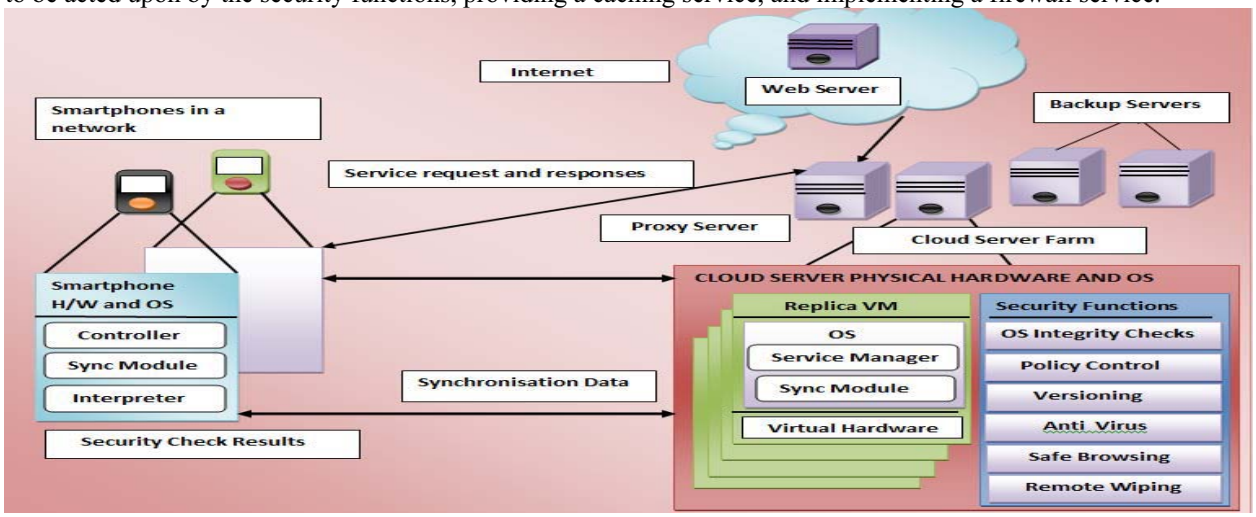

Figure 2. Extension of basic concept

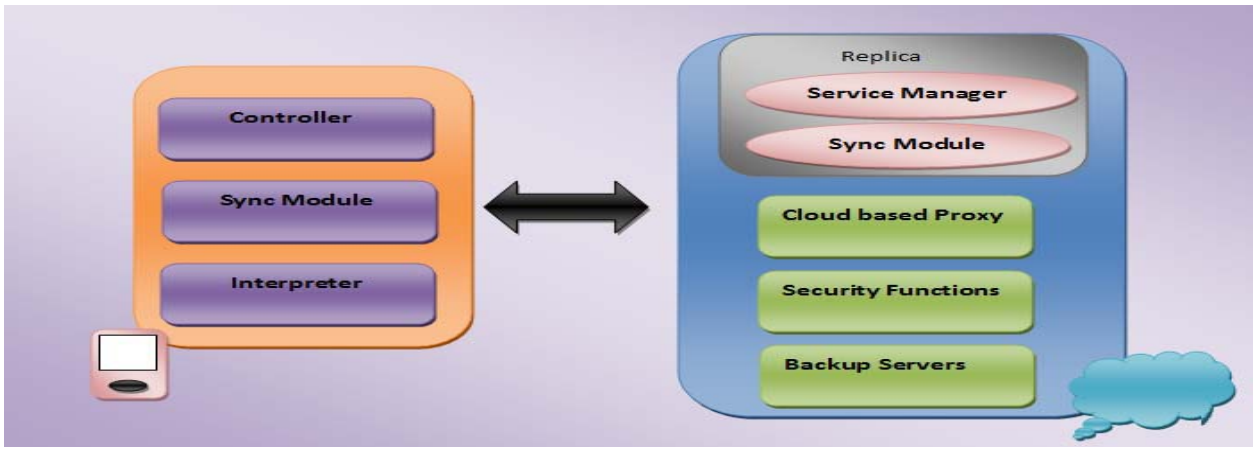

Figure 3 Components of the smartphone and cloud

B. Assumption of this architecture

The following set of assumptions has been made in this architecture:

- All kinds of smartphones are taken into consideration, ranging from lower to higher end models. Battery resources are scarce in every smartphone even though higher end models may offer better CPU performance.
- This architecture is mainly targeted for deployment in a corporate setting and the cloud infrastructure can be *in house* in the case of very high security requirements.
- Cloud servers are capable of hosting any number of replicas as required. The cloud server farm is trusted by the smartphone users as all their information is also stored in the cloud.
- Smartphones are connected to the cloud through a high throughput, low delay internet connection (preferably Wi-Fi or 3G link).
- The targeted infection channel is the internet; although the architecture can be extended and used to monitor other infection channels.
- All the network connections involved are secure *end-to-end.*

Sync Module

The sync module in the phone and the replica are responsible for keeping the states of the smartphone and replica synchronized. A smartphone user is allowed to choose the files which he wants to synchronize to the cloud server by

the use of the sync folder in the smartphone. In addition to these files, the smartphone operating system files are also synchronized. In general, we assume a synchronization of a replica and the smartphone is complete at time "t", if at time "t" the replica in the cloud has an identical copy of the smartphone operating system files and the files which the user accepted to synchronize. In case of high security requirements, strict synchronization i.e frequent synchronization should be enabled. In other cases, loose synchronization (less frequent) could be adopted.

Controller

The controller component is present in the smartphone and is responsible for tracking the data that needs to be sent to the replica to achieve synchronization. Determining the kind of data that needs to be sent depends on how synchronization is achieved. In the Proposed architecture, tracking user inputs to the smartphone could be a set of data that can be used as any change to the state of the smartphone is stimulated by some user action on it, or via the network, or via some Input/Output (I/O) device or sensor on the smartphone. The network inputs are already made available at the replica through the proxy server. To maintain the consistency in the file system of the smartphone and the replica, any new file that has been added to the file system of the smartphone (from sources other than the internet in case of continuously connected operation) is also sent to the replica.

The controller is also responsible for making the phone-replica synchronization decisions as required. As mentioned earlier, the controller can make its decision based on available bandwidth, estimation of possible energy consumption, and estimated energy consumption before the smartphone will be recharged.

Interpreter

The interpreter in the smartphone receives the results from the service manager in the cloud and interprets them. Based on the result obtained, it acts on them according to an established policy and appropriately imitates the user or waits for a user action.

Service Manager

A service manager in the replica VM controls the execution of the various security functions that are present in the cloud server and provided as a cloud service to smartphones. It assumes responsibility to invoke the security functions and sends results to the interpreter in the smartphone.

Cloud based proxy

A cloud based proxy is appropriate for the architecture as it can scale well and support an enterprise's set of smartphones by offering them a pool of services. The proxy server is deployed in the cloud server farm.

The cloud based proxy can act as a firewall to the enterprise's network. To do so, the network traffic in and out of the smartphone must go through the proxy server. In this way, it is possible to apply security checks to the incoming traffic *before* forwarding this traffic to the smartphone, thereby making it possible to achieve attack prevention. This is possible but it incurs the cost of additional delay – and the assumption is that this added delay will be acceptable to ensure security.

A safe browsing service can be offered to the smartphones by scanning the requested web pages for any malicious behavior and the user can be notified accordingly.

Anti-virus scanning can be applied to the incoming traffic, thereby protecting the smartphone from getting infected. The requested web pages could be cached by the proxy server for quick retrieval by the smartphones when accessed in the future. The cached requests and responses can reduce the bandwidth consumption of the smartphones.

Furthermore, the replica hosted in the cloud server can query the proxy server to obtain the required data during synchronization. The proxy server will also provide an anonymity service to the smartphone hiding the identity of the smartphone in the enterprise network.

Backup Servers

Backup servers in the cloud can be used to host the smartphone replicas in case of failure of the main server, thereby enabling a replacement phone to provide the same services as the original phone or another replica to provide the same services as another replica with minimal disruption beyond the delay to initialize the required processes.

Security functions

The proposed architecture lists some of the many security functions that can be provided as a cloud service to smartphones. The security functions can be placed in the native OS of the cloud server or in the emulated replica. The choice of location depends on the kind of security function provided by the service. The security functions to be implemented in the initial prototype are:

- Anti-virus,
- OS integrity checks,
- Policy control,
- Browser protection,
- Versioning and Remote Wiping, and

- Secure Storage.

C. Proposed architecture apply in corporate organization

The Proposed architecture can be deployed in a corporate organization set up. It is often seen that an organization provides its employees with a laptop to be used for official purposes and to connect to the corporate network from home if necessary. This situation might soon change allowing the employer to provide smartphones instead of laptops to its employees. Then the user connects to the corporate network from his/her smartphone instead of a laptop.

Secure storage services provided by the cloud server can be used to access confidential information like non-disclosure agreement documents, project documents etc. Access control policies and monitoring services in the cloud can be used to log the activities of the specific user for future references if necessary.

Policy control service can be used to enforce the policies for the employee using the smartphone. Safe browsing and anti-virus scanning services ensure real time protection to the smartphones preventing them from getting infected through the Internet connection.

IV.CONCLUSION

The aim of this paper was to explore and identify the security functions that can be offered as a cloud service to smartphones. The motivation behind this paper being the fact that the smartphones are not powerful enough in terms of battery and CPU power to support the various security functions that are needed for today's smartphone usage. We propose a generic architecture in Cloud for Smartphones. Since smartphone usage for official purposes and in corporate network has attracted more attention by posing significant risk, the architecture was tailored to suit its deployment in an organization. The architecture used the idea of hosting replicas for smartphones in the cloud and executing the security functions on (or by) them. The various components and their functionalities needed for successful deployment of this architecture were detailed.

Some of the security functions that can be offered in cloud were identified and included in the architecture.

The following are the key aspects of the proposed architecture:

- Generic for all smartphone platforms
- Capable of providing various security services as a cloud offering as required
- Tailored to the needs of a corporate organization, might be modified to be suitable for home users
- Handles threats that attack smartphones through the Internet
- Provides protection to smartphones only when they are connected to the Internet
- Offers flexibility in terms of adding and removing security functions
- The system operates transparent to the user to avoid any privacy breach, by keeping him/her informed of what data is being kept in the cloud.
- Energy consumption at the smartphone occurs only for the synchronization process and it is common for all the security services

REFERENCES

[1] Gartner Reserch , Accessed 3rd March 2011 , http://www.gartner.com/technology/home.jsp

[2] Cisco 2010 Annual Security Report, January 2011, Accessed 27th June 2011, http://www.cisco.com/en/us/prod/collateral/vpndevc/security_annual_report_2010.pdf

[3] U.S. Federal IT Market Forecast 2011 – 2015, Market Research Media, September 2010 update, Accessed 24th Feruary 2011 http://www.marketresearchmedia.com/2009/05/23/us-federal-it-spending-forecast-2010-2015/

[4] A.Azfar, Multiple Escrow Agents in VoIP, Masters Thesis, School of Information and Communication Technology, Royal nstitute of Technology (KTH), Stockholm, Sweden, TRITA-ICT-EX-2010: 109, June 2010 http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORT/100607-Abdullah Azfar-with- cover.pdf

[5] Samsung Mobiles, Samsung Wave II S8530, Accessed 20th March 2011 http://www.samsung.com/in/consumer/mobile-phone/mobilephone/touch-phone/GTS8530HKATHR/index.idx?pagetype=prd_detail&tab=specicattion

[6] F-Secure Labs, Trojan: SymOS/Cardtrap.M, Accessed 26th February 2011 http://www.f-secure.com/v-descs/trojansymboscardtrapm.shtml

[7] Gartner Survey Shows U.S. Consumers More Likely to Purchase a Smartphone Than Other Consumer Devices in 2011, Gartner Press Release, February 17, 2011, Accessed 27th June 2011. http://www.gartner.com/it/page.jsp?id=1550814

[8] Opera Mini, Wikipedia, Accessed 13th March 2011.
http://en.wekipedia.org/wiki/OperaMini

[9] Opera Software, Accessed 7th March 2011
http://www.opera.com/mobile/help/faq/#security

[10] M.D. Lopez, Research Report : Successful Mobile Deployments Require Robust Security, May 25 , 2009, Accessed on 20th February 2011
http://us.BlackBerry.com/ataglance/get_the_facts/Successful_Mobile_Deploments.pdf

[11] 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 (ACSAC 2010), December 6-10, 2010, Austin, Texas , US

[12] B. – G. Chun, P.maniatis, Augmented Smartphone Applications Through Clone Cloud Execution, In: Proceedings of the 12th conference on Hot topics in operating systems (HotOS 2009), May 18-20, 2009, Monte Verita, Switzerland

[13] B. Zhao, Z.Xu, C. Chi, S. Zhu, and G.Cao, Mirroring Smartphones for Good: A Feasibility Study, ZTE Communications, 18th March 2011, Accessed 3rd May 2011
http://wwwen.zte.com.cn/endata/magazine.ztecommunications/2011Year/no1/articles/201103/t20110318_224543.html

[14] R. Mehul, "Discrete Wavelet Transform Based Multiple Watermarking Scheme", in *Proceedings of the 2003 IEEE TENCON*, pp. 935-938, 2003.