International Journal of Innovative Research in Computer Science and Engineering (IJIRCSE)
www.ioirp.com Volume – 1. Issue – 1. November 2014

MOBILE DEVICE MANAGEMENT

V.Vijayalakshmi[1], R.Vasugi[2]

[1]*HOD Cum Assistant Professor, Bharathiyar Arts And Science College For Women, India*

[2]*Assistant Professor, Bharathiyar Arts and Science College for Women, India*

[1]vijisylvia@gmail.com, [2]vasubhuvan11@gmail.com,

Abstract : **MDM functionality typically includes over the air distribution of applications, configuration and data settings for all types of mobile devices, including mobile phones, smart phones, table computers, mobile computers, mobile printers, mobile devices, etc. This applies to both company-owned and employee-owned devices across the enterprise or mobile devices owned by consumers. Consumer Demand is now requiring a greater effort for MDM and increased security for both the devices and the enterprise they connect to especially since employers and employees have different expectations on the type of restrictions that should be applied to mobile devices. By protecting the data and configuration settings for all mobile devices in the network, MDM reduce support costs and business risks. The intent of MDM is to optimize the functionality and security of a mobile communications network while minimizing cost and downtime.**

MOBILE DEVICE MANAGEMENT

Mobile Device Management is the ability to secure, monitor, manage and support mobile devices – typically involving remote distribution of applications, data and configuration settings for all types of mobile devices such as smartphones, tablets and notebook computers. With mobile devices and applications flooding the market, mobile device management is growing in importance. By optimizing the functionality of mobile devices while controlling and protecting the data and configuration settings for all mobile devices in a network, support costs and business security risks are lowered.

Mobile device management (MDM) is a type of security software used by an IT department to monitor, manage and secure employees' mobile devices that are deployed across multiple mobile service providers and across multiple mobile operating systems being used in the organization. Mobile device management software is often combined with additional security services and tools to create a complete mobile device and security Enterprise Mobility Management solution. The research firm defines mobile device management as "a range of products and services that enables organizations to deploy and support corporate applications to mobile devices, such as smartphones and tablets, possibly for personal use enforcing policies and maintaining the desired level of IT control across multiple platforms". Via the user-friendly online dashboard, MDM allows mobile tracking users can find and track connected devices in real time and view the routes employees take via Bing Maps. Send messages to any number of devices simultaneously without the associated charges, whilst being provided with instant delivery status.

Companies benefit from mobile device security when using mobile device management. For example, users can remotely lock mobile devices or completely erase sensitive company data from an abused, lost or stolen mobile device. Also offers secure communications between the MDM servers and devices in order to keep data secure. Devices and corporate data can be protected by remotely enforcing a strong password policy. Mobile device management also means the ability to manage mobile apps that are on each device. You can deploy, manage, block or remove rogue apps on individual or groups of devices, ensuring productivity is high, reducing the risk of dangerous mobile malware and maintaining data plan and call budgets. Multiple administrators can manage an account and detailed reports allow users to audit any associated activity, including call logs, call costs, messages sent and received as well as the apps that have been installed or removed. Via the administrations portal, users are instantly alerted to important events.

With mobile devices becoming ubiquitous and applications with the market, mobile monitoring is growing in importance. Numerous vendors help mobile device manufacturers, content portals and developers, test and monitor the delivery of their mobile content, applications and services. This testing of content is done real time by simulating the action of thousands of customers and detecting and correcting bugs in the applications. Companies are alarmed at the rate of employee adoption of mobile devices to access corporate data. MDM is now touted as a solution for managing corporate-owned as well as personal devices in the workplace. The primary challenge is the ability to manage the risks associated with mobile access to data while securing company issued mobile devices.

First and second generation of wireless networks are based on circuit switched infrastructure. These networks support voice and low data rate services such as short message service (SMS). However, the air interface technologies of such networks are inadequate to support high data rate services such as multimedia, streaming services, file transfer, and gaming. Next-generation wireless systems are designed to support these high data rate services. These networks are envisioned to have an IP-based infrastructure with the support of heterogeneous access technologies. IP-based wireless networks are better suited for supporting the rapidly growing mobile data and multimedia services, since they can bring the successful Internet service paradigm to mobile providers and users. In addition, IP-based wireless networks can integrate seamlessly with the Internet to allow mobile users to access the information, applications, and services available over the Internet. Moreover, IP technologies provide a better solution to integrate different radio technologies transparently in such a way that users perceive them as one communication network. Currently, several IP-based architectures are proposed for integrating heterogeneous wireless networks to provide ubiquitous communications.

DEVICE MANAGEMENT SPECIFICATIONS AND CONSTRAINTS

Location management enables the system to track the attachment points of MTs between consecutive communications. It includes two major tasks. The first is location registration or location update, where the MT periodically informs the system to update relevant location databases with its up-to-date location information. The second is call delivery, where the system determines the current location of the MT based on the information available at the system location databases when a communication for the MT is initiated. Two major steps are involved in call delivery: determining the serving database of the called MT and locating the visiting cell/subnet of the called MT. The latter is also called paging, where polling messages are sent to all the cells/subnets within the residing registration area of the called MT.

1. The Open Mobile Alliance specified a Platform Independent device management protocol called OMA device management. The specification meets the common definitions of an open standard meaning the specification is freely available and implementable. It is supported by several mobile devices, such as PDAs and mobile phones.
2. Message is text SMS-based provisioning protocol (ringtones, calendar entries but service settings also supported like: ftp, telnet, SMSC number, email settings, etc...)
3. OMA Client is a binary SMS based service settings protocol.
4. Nokia-Ericsson OTA is binary SMS-based service settings provisioning protocol, designed mainly for older Nokia and Ericsson mobile phones.

Over the air capabilities are considered a main component of mobile network operator and enterprise-grade mobile device management software. These include the ability to remotely configure a single mobile device, an entire fleet of mobile devices or any IT-defined set of mobile devices; send software and OS updates; remotely lock and wipe a device, which protects the data stored on the device when it is lost or stolen; and remote troubleshooting. Commands are sent as a binary SMS message. Binary SMS is a message including binary data. Mobile device management software enables corporate IT departments to manage the many mobile devices used across the enterprise; consequently, over-the-air capabilities are in high demand. Enterprises using SMS as part of their MDM infrastructure demand high quality in the sending of messages, which imposes on SMS gateway providers a requirement to offer a high level of quality and reliability.

In wireless mobile computing, to be portable, devices must be small, light and operational under wide environmental conditions. Also, in the context of ubiquitous or pervasive computing, computational power is embedded in numerous small devices. In particular:

- Portable devices have small screens and small, multifunction keypads; a fact that necessitates the development of appropriate user interfaces.
- Portable or embedded devices have fewer resources than static elements, including memory, disk capacity and computational power than traditional computing devices.
- Portable devices rely for their operation on the finite energy provided by batteries. Even with advances in battery technology, this energy concern will not cease to exist. The concern for power consumption spans various levels in hardware and software design.
- There are higher risks to data in mobile devices, since it is easier for mobile devices to be accidentally damaged, stolen, or lost.

An additional issue is scalability. The number of portable computing devices is in the order of billions. Storing and managing information in such systems is a formidable task.

To deal with the characteristics of mobile computing, especially with wireless connectivity and small devices, various extensions of the client/server model have been proposed. Such extensions advocate the use of proxies or middleware components. Proxies of the mobile host residing at the fixed network, called server-*side* proxies, perform various optimizations to alleviate the effects of wireless connectivity such as message compression and re-ordering. Server-side proxies may also perform computations in lieu of their mobile client. Proxies at the mobile client undertake the part of the client protocol that relates to mobile computing thus providing transparent adaptation to mobility. They also support client caching and communication optimizations for the messages sent from the client to the fixed server. Finally, mobile agents have been used with client/server models and their extensions. Such agents are initiated at the mobile host, launched at the fixed network to perform a specified task, and return to the mobile host with the results.

Another concern in terms of software architectures is adaptability. The mobile environment is a dynamically changing one. Connectivity conditions vary from total disconnections to full connectivity. The resources available to mobile computers are not static either, for instance a “docked” mobile computer may have access to a larger display or memory. Furthermore, the location of mobile elements changes and so does the network configuration and the center of computational activity. Thus, a mobile system is presented with resources of varying number and quality. Consequently, a desired property of software systems for mobile computing is their ability to adapt to the constantly changing environmental conditions.

IMPLEMENTATION

Typically solutions include a server component, which sends out the management commands to the mobile devices, and a client component, which runs on the handset and receives and implements the management commands. In some cases, a single vendor may provide both the client and the server, in others client and server will come from different sources.

The management of mobile devices has evolved over time. At first it was necessary to either connect to the handset or install a SIM in order to make changes and updates; Scalability was a problem one of the next steps was to allow a client-initiated update, similar to when a user requests a Windows Update. Central remote management, using commands sent over the air, is the next step. An administrator at the mobile operator, an enterprise IT data center or a handset OEM can use an administrative console to update or configure any one handset, group or groups of handsets. This provides scalability benefits particularly useful when the fleet of managed devices is large in size.

Device management software platforms ensure that end-users benefit from plug and play data services for whatever device they are using. Such a platform can automatically detect devices in the network, sending them settings for immediate and continued usability. The process is fully automated, keeps a history of used devices and sends settings only to subscriber devices which were not previously set, sometimes at speeds reaching 50 over-the-air settings update files per second. Device management systems can deliver this function by filtering option. Most mobile device management solutions provide organizations with end-to-end security — meaning the, mobile applications network and data used by the mobile device (in addition to the mobile device itself) are managed by an organization's IT department with a single mobile device software product.

Some enterprise MDM solutions combine mobile security and expense management in a single product. Depending on the vendor and what specific features it supports, you can typically expect mobile device management software to contain some or all of the following features: management and support of mobile applications, mobile policy management, inventory management, security management and telecom service management.

REFERENCES

1) Michael Johnson - Mobile Device Management: What You Need to Know for It Operations Management , Emereo Pvt Ltd , 2011

2) Findlay Shearer - Power Management in Mobile Devices

3) Data Management for Mobile Computing – Evaggelia Pitoura , George Samaras