Comparative Analysis of Virtualization Techniques for Mobile Cloud Computing

Varsha Grover[1], Gagandeep[2]
[1] Research Scolar Department of Computer Science
[2]Associate Professor Department of Computer Science
Punjabi University, Patiala

Abstract: In the era of the internet, Mobile Cloud Computing (MCC) has become a significant research topic of the scientific and industrial communities. MCC integrates the cloud computing into the mobile environment and overcomes obstacles related to the performance such as battery life, storage, and bandwidth, environment like heterogeneity, scalability, and availability, and security. Smart phones connect to internet to use all these web services. Connecting through internet smart phones facing the similar security problems as we face in personal computers. As if an unsuspecting user downloads a corrupted application from internet, the entire phone could be damaged. Due to these security reasons normally it seems that many users carry different phones to fulfill their personal and work needs. So to overcome these issues virtualization is a best choice .Apart from its attributes virtualization is one major concept used in mobile cloud computing. Virtualization is a framework or methodology of dividing resources of a computer into multiple execution environments. This paper proposes concept of virtualization and its techniques for MCC.

Keywords: mobile cloud computing, virtualization, virtualization technologies, virtualization software

I. INTRODUCTION

Mobile cloud computing has been devised as a new phrase since 2009. From a simple perspective MCC refers to an infrastructure where both data storage and processing occur outside the mobile device. It is a new paradigm for mobile applications where the processing and storage shifts the mobile device to powerful and centralized computing platforms located in clouds. Mobile Cloud is powerful to perform computations while mobile devices have limitation for computing [1].

Security and Privacy, Migration and Reliability, Virtualization are some of the challenges associated with MCC. Mobile Cloud can be considered as a virtual resource pool where all bottom layer hardware devices are virtualized. End users access desired resources through a browser and get data from cloud computing providers without maintaining their own data centers. Virtual machines (VMs) are often installed in a server in order to improve the efficiency to use resources. The technique of virtualization firstly proposed in 1960 by IBM, provides a graceful solution to the problems like security and optimum utilization of hardware resources. It allows multiple operating system instances to run concurrently on a single computer. Throughout survey, It has been found four useful techniques; Cells, Xen on ARM, KVM for ARM and ViMo, of virtualization in smart phones. In this paper, Comparative analysis of virtualization techniques based upon the security, power consumption, and performance has been carried out.

II. VIRTUALIZATION CONCEPTS

Virtualization is a technique which allows to create abstract layer of system resources and hides the complexity of hardware and software. Virtualization provides hardware independence, isolation of guest operating system and encapsulation of entire virtual machine grouped in a single file. Server virtualization, Client virtualization and Storage virtualization are three types of virtualization.

A. Server Virtualization:

This technique that involves partitioning a physical server into a number of small, virtual servers with the help of virtualization software. In server virtualization, each virtual server runs multiple operating system instances at the same time. Server virtualization attempts to increase resource utilization by partitioning physical servers into several multiple virtual servers. Server virtualization makes each virtual server look and act like a physical server by multiplying the capacity of every single physical machine.

B. Client Virtualization

This technology makes the system administrator to virtually monitor and update the client machines like workstation desktop, laptop and mobile devices. It improves the client machines management and enhances the security to defend from hackers and cybercriminals.

C. Storage Virtualization

This technique creates the abstraction of logical storage from physical storage. There are three kinds of data storage are used in virtualization, DAS (Direct Attached Storage), NAS (Network Attached Storage) and SAN (Storage Area Network). DAS is a conventional method of data storage where storage drives are directly attached to server machine. NAS is a shared storage mechanism, which connects through network. SAN is a storage device that is shared with different servers over a high accelerate network.

Following are the virtualization techniques should be considered while implementing the concept of virtualization[2].

a) *Emulation*

It is a virtualization technique, which converts the behaviour of the computer hardware to software program and lies in the operating system layer. Emulation provides enormous flexibility to guest Operating system (OS) and the speed of translation process is low compared to hypervisor and requires a high configuration of hardware resources to run the software.

b) *Virtual Machine Monitor*

A software layer that can monitor and virtualizes the resources of a host machine based on user requirements .It is an intermediate layer between OS and hardware. Hypervisor is classified as native and hosted. Native based hypervisor runs directly on the hardware whereas host based hypervisor runs on the host OS.

c) *Para Virtualization*

This technique provides special hyper calls that substitutes the instruction set architecture of host machine. It relates communication between hypervisor and guest operating system to improve efficiency and performance. Accessing resources in Para virtualization is better than the full virtualization, because all resources must be emulated in full virtualization.

d) *Full Virtualization*

Hypervisor creates isolated environment between the guest or virtual server and the host or server hardware. OS directly access the hardware controllers and its peripheral devices without cognizant of virtualized environment and requirement modifications.

III. RELATED WORK

Comparative analysis of virtualization techniques that are to security, power consumption, and performance has been carried out by the architecture in this paper as given following.

ViMo uses full virtualization technique in which there is no need of modification in guest OS. In typical systems, OS is present in supervisor mode of ARM and applications in ARM user mode. In case of ViMo virtualization ARM user mode further divided into two virtual modes. One is virtual user mode in which applications are present and the other is virtual supervisor mode in which guest OS is present. While ViMo places in ARM supervisor mode and consists on mainly five components. Code tracer detects the critical instructions in virtual machines which processed by CPU virtualizer. Memory Virtualizer isolates the memory of one virtual machine from the other virtual machine. Virtual interrupt controller the handles the interruption from virtual machines. Scheduler switches the virtual machines periodically[3].

In terms of Security in Vimo technique that is provided by the separating the tasks. It means special or secure tasks perform in secure mode and normal tasks perform in normal mode. Separating the modes will separate the resources of hardware in terms of virtualization. It means hardware resources like virtual CPU is individually assigned to each mode. Protected or secure mode can access all available hardware resources while a normal mode cannot access the secure resources. System cannot go directly from secure mode to normal mode without the help of monitor mode. If a system wants to switch from normal to secure mode, it generates a special interrupt and transfers to the monitor via CPU and then monitor transfers the mode[3].

Cells virtualization is a lightweight OS virtualization which uses single OS across all Virtual Private (VP). Each VP has a virtual private namespace and can use the hardware resources present in their virtual private name space. Cells achieve this type of advance smart phone virtualization by remapping the resources identifiers used by the processes present in each VP. File system, process identifiers, network addresses and many other identifiers are virtualized. For example file system is virtualized by mount name space which can be created by many independent virtual file systems that are used concurrently by each VP[4][5].

In Cells the concept of security maintains by isolating each VP to prevent interference of VPs with each other. Interference means frontend and backend VPs have separate access level to hardware resources for example if foreground VP have exclusive access to GSM module than background VP will not request to GSM. For this point of view cells have 4 security techniques to isolate each VP. User certificates virtualized by user name so that each VP namespace isolates from other VP namespace. Each VP has its own private name space where as available hardware resources are mentioned for that specific VP. This mechanism ensures that each VP using its own namespace mentioned resources and cell which provides this mechanism with the name of device namespace. There must be a separate file system for each VP which is done by mount file system. A VP must have no direct access to external devices. To prevent malicious activities Cell provides Cell-ID for prevention[4][5][14].

In Xen on ARM architecture applications can access hardware with the help of event channel which forms by the dialogue between back end driver and front end driver. Whenever a virtual guest OS requests any hardware resource , a virtual interrupt is generated and queued in the channel and then transferred to the destination via domain scheduler. Virtual CPU in XEN has two modes. One is supervisor mode and the other is user mode. User mode further divided into two modes that is user application mode and user process mode

For security point of view CPU is divided into two modes. One is unprivileged supervisor mode and other is privileged user mode. Virtual memory monitors (VMM) places in supervisor mode to protect it from unwanted modifications and guest OS. Applications are placed in user mode. User mode is privileged mode and guest OS cannot be placed in privileged (protected guest OSs from unwanted modifications) mode. Thats why user mode further divided into two modes. One is user process mode in which applications are kept and second is user supervisor mode in which guest OSs are kept to prevent them from undesirable modifications. From memory point of view Xen protects VMM memory space from guest OS memory space and users'. It also protects guests OS memory space from user application memory space and user processes memory from other user processes [6][7][8][9][10].

KVM guest OSs are not controlled by control panel instead of this guest OS applications that run as a process in Linux host applications and KVM acts as a module in kernel. if there is need of any resource VPs, then in case KVM sends request to hardware through kernel interface

Security in KVM on ARM is provided by separating user application memory space and kernel memory space is an important goal in KVM. This can be done by domain and access permissions. ARM architecture has 16 domains from 0 to 15 and each domain have 3 modes that are no access, Client and Manager. If a page is in no access domain, no access is provided to that page. If a page is in manager domain, it has all access, and if a page is in client domain its access checked from table. By modifying the guest kernel source code slightly user applications run in same CPU mode and sensitive instructions present only in assembler files and inline assembly [11][12].

IV. COMPARATIVE ANALYSIS OF VIRTUALIZATION TECHNIQUIES

To prove the effectiveness of all four mentioned architectures, A comparative analysis of these virtualization techniquies is observed . For ViMo 33% overhead is examined which is unacceptable for mobile devices due to their frequent use of smart devices .This overhead is due to the execution of critical instructions and frequent context switching between guest OS and ViMo which makes cache memory overloaded and performance decreases. For KMV/ARM experiments performed on dual core 1.7 GHZ Cortex A-15 ARM .

Table. 1 provides Comparative analysis of all four architectures. Highlighted features include platform, virtualization technique, security, performance overhead, power consumption, observed performance and isolation level of OS.

Table 1: Comparative analysis of virtualization techniques

	XEN	CELLS	KVM	VIMO
Platform	Open Source	Open Source	Open Source	Open Source
Virtualization Technique	Para	Para	Para	Full
Security	High	High	High	High
Performance Overhead	Moderate	Low	High	High
Power Consumption	Low	Very low	Low	Low
Performance	Very High	Good	Poor	Poor
OS Isolation	Strong	Strong	Strong	Strong

V. CONCLUSION

In conclusion, none of the virtualization technologies can be marked as best or worst because every technologies are efficient enough in their own way of computing.In this paper comparsion of virtualization techniquies Cells, Xen on ARM, KVM for ARM and ViMo has been analysed. It has been found that out of all techniquies Cells technique is best in terms of performance,security,powerformance overhead and power consumpation. OS isolation is strong in all these techniques and these techniquies work on open source platform. In future, we plan to explore them more for real time scheduling, compatibility and scalability.

VI. REFERENCES

[1]. Hoang T. Dinh, Chonho Lee, Dusit Niyato and Ping Wang ,"A survey of mobile cloud computing: architecture, applications, and approaches," School of Computer Engineering, Nanyang Technological University (NTU), Singapore, pp 1587-1611, 2013.

[2]. Durairaj.M, Kannan.P, A Study in Virtualization Techniques and Challenges in Cloud Computing, International Journal of Scientific and Technology Research, vol. 3, pp 147-151, 2014.

[3]. .C. Oh, K.H. Kim, K.W. Koh and C.W. Ahn "ViMo (Virtualization for Mobile): A Virtual Machine Monitor Supporting Full Virtualization For ARM Mobile Systems," Proc. Advanced Cognitive Technologies and Applications, COGNITIVE, 2010.

[4]. J. Andrus, C. Dall, A. Van't Hof, O. Laadan, and J. Nieh, "Cells : A Virtual Mobile Smartphone Architecture," Proc. ACM. SOSP, pp. 173- 187, 2011.

[5]. White Paper, "The ThinVisor Mobile Device Virtualization Architecture", CELLROX, November 2011.

[6]. R. Bhardwaj, P. Reames, R. Greenspan, V.S. Nori and E. Ucan, "A Choices Hypervisor on the ARM Architecture," 2006.

[7]. J. Hwang, S. Suh, S. Heo, C. Park, J. Ryu, S. Park, C. Kim and A.V. History, "Xen on ARM : System Virtualization using Xen Hypervisor for ARM-based Secure Mobile Phones," Proc. IEEE Consumer Communications and Networking Conference, CCNC, pp. 257–261, 2008.

[8]. M. Lemay, D. Jin, S. Reddy and B. Schoudel "Porting the Xen Hypervisor to ARM."

[9]. S. Seo, "Research on System Virtualization using Xen Hypervisor for ARM based secure mobile phones," Proc. IEEE Consumer Communications & Networking Conference, CCNC, 2008.

[10]. Suh, "Secure Architecture and Implementation of Xen on ARM for Mobile Device," Proc. 4th Xen Summit, IBM T.J. Watson, April 2007.

[11]. C. Dall and J. Nieh, "KVM for ARM." Proc. Annual Linux Symposium, 2010.

[12]. C. Dall and J. Nieh, "KVM/ARM : Experiences Building the Linux ARM Hypervisor," Technical reports, Department of Computer Science, Columbia University, 2013.

[13]. S. Oh, K. Koh, C. Kim, K. Kim, and S. Kim, "Acceleration of Dual OS Virtualization in Embedded Systems," Proc. Computing and Convergence Technology, ICCCT, pp. 1098–1101, 2012.

[14]. C. Dall, J. Andrus, A. Van't Hof, O. Laadan, and J. Nieh, "The Design, Implementation, and Evaluation of Cells: A Virtual Smartphone Architecture," ACM Transactions on Computer Systems (TOCS), 30(3), pp. 1–31, Aug. 2012.

[15]. Y.W. Jung, K.W. Koh, C.W. Ahn, and S.W. Kim, "Type-2 micro virtual machine monitor for ARM-based mobile systems," Proc. IEEE/ACIS, pp. 565–566, 2013.

Dr. Gagandeep received her Ph.D degree in computer science from Punjabi University, Patiala in 2012 on the topic "Analysis and Development of Testing Techniques for Component-based Software Systems". Currently, she is working as Associate Professor in the Department of Computer Science, Punjabi University, Patiala. She has more than 20 years of teaching and research experience. She is currently involved in research work on data security, virtualization techniques and computational offloading mechanism for cloud and mobile computing.

Varsha Grover is Pursuing Ph.d from Punjabi University in computer science department on the topic " Secure Virtualization techniques for Mobile cloud computing. Currently, she is working as Assistant Professor in the Department of Computer Science, Patel Memorial National College, Rajpura. She has more than 7 years of teaching and research experience.