Review Article

International Journal of Advanced Computer Research, Vol 10(51)
ISSN (Print): 2249-7277 ISSN (Online): 2277-7970
http://dx.doi.org/10.19101/IJACR.2020.1048101

Research gaps based virtualization in mobile cloud computing

Boubakeur Annane[1*], Adel Alti[2] and Osman Ghazali[1]
School of Computing, University Utara Malaysia, Sintok, Kedah, Malaysia[1]
Department of Management Information Systems, College of Business & Economics Qassim University, Buraidah, KSA[2]

Received: 10-September-2020; Revised: 11-November-2020; Accepted: 15-November-2020

Abstract
Recently, mobile computing is known as a fast-growing utilization of people's daily life. However, the main challenge that faced this rapid advancement is the limited mobile devices' resources such as processing capability, storage space and battery life. With the development of cloud computing, mobile devices' resources are improved with the help of cloud services, which resulted an emerged technology named Mobile Cloud Computing (MCC). Although the MCC has several advantages for mobile users, it is also challenged by many critical issues like security and privacy of the mobile user's data that offloaded on the cloud' servers and processed on the virtual machines (VMs). In virtualization, various investigations showed that malicious users are able to break down the cloud security methods by spreading their VMs in order to alter or violate the user sensitive data that executed on cloud' VMs. This paper deeply analyzes the recent MCC based virtualization approaches and methods by criticizing them. We found out that no approach protects the data from being stolen while distributed VMs that deployed on different cloud servers exchanging data. Hence, the paper provides practical gaps related to virtualization in MCC and future perspectives.

Keywords
Security and privacy, Mobile cloud computing, Virtualization, Co-location, Hypervisor, Distributed attacks.

1.Introduction
MCC is a mix of cloud computing and mobile computing [1] where mobile devices leverage from cloud resources using a set of techniques in order to leave out their constraints and getting the mobile devices more resistible in terms of power consumption such as extending the battery life. Other mentioned definitions have described that mobile cloud is an infrastructure where the data computing and storage moved to a third party powerful entity (cloud) away from mobile devices [2]. *Figure 1* presents the architecture of mobile cloud computing.
There are three main services in cloud computing, the first one is Software as a Service (SaaS) which delivers the applications as a service for the client or the end-user over the internet [3]. Such kinds of these applications: DropBox, Gmail, Microsoft Office 356, Rackspace, Salesforce, and SAP Business ByDesign. The second service is Platform as a Service (PaaS) which allows developing applications in a platform using Application Programming Interfaces (API). Google App Engine, Amazon web services, and Microsoft Azure are the primary players known in this layer. The third main service in the cloud environment is Infrastructure as a Service (IaaS), this layer contains the hardware resources such as datacenters which provides storage and computation facilities using the virtualization for sharing the computing resources such as CPU, Memory of the cloud servers. Flexiscale [4], Amazon EC2 [5] and Amazon S3 [6] are examples of IaaS service providers.

One of the biggest issues in MCC environment is the security and privacy of the users' data. Most of the security issues of MCC are acquired from cloud computing, means they are similar issues and more critical on MCC due to the restricted devices' resources (e.g., the incapacity of CPU capability) to deal with serious malware application or complex calculation to ensure the sensitive information as like Personal Computers (PCs). There is a crucial need for a lightweight framework that guarantees security with minimum processing and communications overhead on mobile devices [7]. In MCC, the sharing

*Author for correspondence

of cloud's resources for users is handled by the help of virtualization technology that augments the efficiency of the utilization rate of the cloud's resources and services [8]. However, researchers in [9] indicated that virtualization had brought various security dangers and issues like Denial-of-Service (DoS) attacks. Other researchers in [10] showed that numerous attacks can affect the virtualization layer in the cloud systems, for example, co-resident (co-location) attacks, Distributed Denial-of-Service (DDoS) attacks, distributed attacks, and the hypervisor attacks which could circumvent the virtual machines (VMs) and steal/alter the users' sensitive information.

The previous researches indicate that VMs attackers need to be with the VMs users inside the same host before they would be able to make their side channels to violate any useful information [9]. Thus, using the VM allocation policy is one of the crucial factors that cloud providers can control and influence the possibility of co-location [11]. So, researchers in [12] have attempted to solve the problem by finding a robust and secure VMs allocation strategy to increase difficulties for attackers and stop the spread as well as co-location of malicious VMs with VMs' users and mitigates the possibility to perform co-location. However, the proposed works focused on the impact of how many VMs' attacker needs to be launched by malicious users to co-locate with the target legal VMs. This is one of the main reasons that allowing start and deploy a limited number of users' VMs in the cloud's servers as well as reduce the co-resident attacks. This kind of solution may enhance the security protection of deployed VMs, but effectively will affect the quality of cloud service provider (i.e.: scalability) which decreases the Service Level Agreement (SLA) between a cloud provider and a user. Moreover, the proposed works also studied strategies for co-locating attackers' under different VM allocation strategies. However, if the malicious VM's success to co-locate with a legal VM then the VM attacker built a malicious side-channel and get data from target VMs. Therefore, it is preferable to come up with an efficient approach that ensures the VMs protection even if the VMs co-location occurs in the cloud's servers.

This paper examines some recent approaches that proposed to protect the user sensitive data deployed on the VMs in the cloud environment. Furthermore, it figures out the gaps of these approaches and their weaknesses in order to understand by researchers. The paper is organized as follows. Section 2 gives a review of mobile cloud computing challenges. Then, Security and privacy requirements is given in Section 3. Thereafter, some new security approaches based on virtualization are illustrated in detail in section 4. Furthermore, a comparison and evaluation of these approaches are provided in a table in section 5. The core of this paper and the practical gaps of the virtualization layer is presented in Section 6. Finally, section 7 gives some future works and concludes the paper.

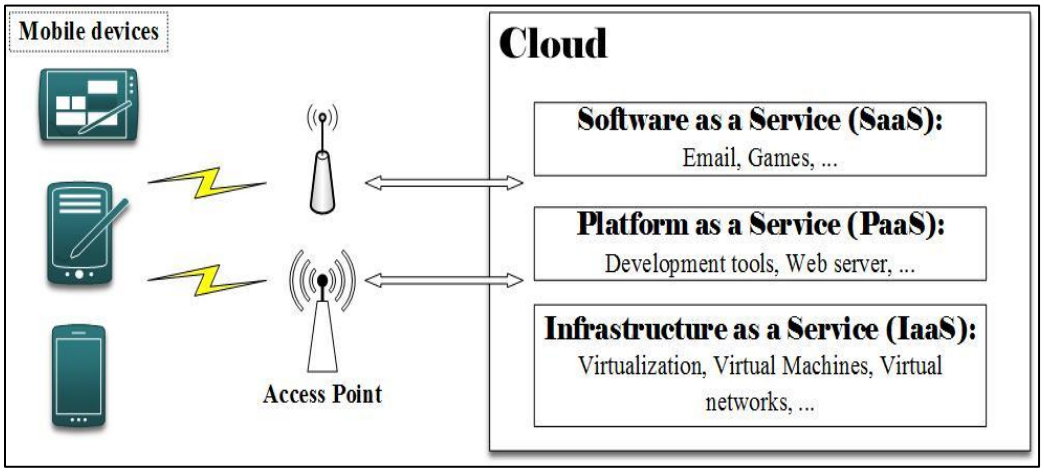

Figure 1 Architecture of mobile cloud computing

2.An overview of mobile cloud computing challenges

Both mobile devices consumers and cloud service providers have taken advantage of the mobile cloud computing environment. However, the MCC stills face different challenges that hinder it and make it more difficult compared to Cloud Computing [13, 14]. In this section, we give a short brief about the challenges that have faced by the mobile cloud before we introduce the related works.

1. **Mobile devices resources limitations:** mobile devices still face various limitations: storage capacity, processing power, and battery power compared with a desktop computer. Despite the improvements in different sides of mobile devices such as CPU, memory and battery life, they are incapable to run the power-intensive application in their local physical resources.
2. **Heterogeneity:** in the environment of mobile cloud, various mobile application services are interacted and running on different processor architectures and operating systems, and communicating through various protocols and communication supports. This may affect the quality of service like application response time, communication quality, and service delivery.
3. **Elasticity:** similar to cloud computing, elasticity and scalability are the main needed factors in MCC services. The cloud services provider needs to meet and satisfy all the mobile user requirements when they are over available resources. The interruption of services due to resource unavailability cause many problems between the end-user and cloud providers.
4. **Applications services issues**: the limited resources of mobile devices prevent the intensive task to be freely deployed and executed. However, the offloading technique needs to be applied for migrating the computationally intensive task from the device to the cloud environment. The most intensive task is running on the cloud server and a small part of the computational processing is executed in the mobile device. Consequently, the mobile user may face delay that affects negatively the quality of service.
5. **Security and privacy challenges:** Compared to cloud computing, security and privacy issues are increasing in MCC environment [15]. Therefore, running intensive applications over vast distances against malware within mobile devices are very complicated due to the constrained resources. Thus, executing complex algorithms is inconvenient as like normal computer. For instance, various intensive applications will be communicating over vast distances, the need for secure communications is critical; otherwise, sensitive data and information would be put at risk. In addition, communications and mobility should not be tracked; otherwise, it would violate privacy.

3.Prerequisites of security and privacy in MCC

The main prerequisites of security and privacy of MCC have been characterized by State United National defense, which are composed as follows [16, 17].

1. **Confidentiality:** it is referring to keep the user's data secret and safe in the cloud and it considers as one main security and privacy requirement. Accordingly, mobile users have risks once exploit cloud services. When the data sent and received over a public network, as well as executed and processed in public cloud datacenters, there is a possibility of retrieving the data by unauthorized or malevolent users.
2. **Integrity:** the integrity is ensuring the data consistency and accuracy related to users in the cloud side once is stored on the service providers. Whereas, the alteration of sensitive data is prohibited by unauthorized users and it leads to various users' losses such us their business [18].
3. **Availability:** ensuring the availability for mobile users means that all cloud services must be always available for users at any time and everywhere according to mobile user's needs and their usage contexts [18]. Ensuring the availability includes prohibiting the different type of attacks which destabilize the availability of services.
4. **Access control and authentication:** authentication is the operation of identification of user correct identity [19]. After the process of authentication is successful, it is necessary to identify the resources to which they have access and what type of execution can execute by the mobile user, such as viewing, editing, or deleting. These restricted operations called control access [20].
5. **Privacy:** Privacy ensured directly or indirectly while the requirements stated above are checked. Confidentiality, integrity, and authentication are three needed objectives that preserve the privacy of the cloud service of mobile users.

4.Virtualization breaches and existing approaches solutions

This section will provide a brief definition of the virtualization and some proposed works by researchers to overcome the challenges that related to the virtualization layer for both mobile cloud computing and cloud.

4.1Virtualization

Virtualization plays a key role whereas the cloud resources are shared among many users to help them achieve an efficient performance and exploiting the maximum capacity of the cloud's servers. The virtualization is defined in the IaaS, where many data centers contain various servers which deploying VMs that comprise huge data amount of users. An image of VMs of mobile devices also called phone clones are pre-created on these servers while offloading and performing mobile user's intensive applications and tasks [16]. Similarly, unauthorized users can deploy their VMs and obtain data from the legitimate user by constructing many malicious side channels using the same sharing resources (CPU cache, memory bus).

The main goal of virtualization is to run different virtual machines of different mobile users at the same time or simultaneously. Thanks to the Virtual Machine Manager (VMM) so-called Hypervisor, which ensures the management (e.g., creating, deleting, and migrating) of different VMs (phone-clones) and the isolation from each other. However, the hypervisor vulnerabilities can be exploited by an adversary to obtain access to users' virtual machines [10, 21, 22]. Many existing approaches have been proposed to overcome the issues related to the virtualization layer especially to protect the user's VMs and their sensitive data. *Figure 2* shows the main different approaches solution related to the virtualization layer.

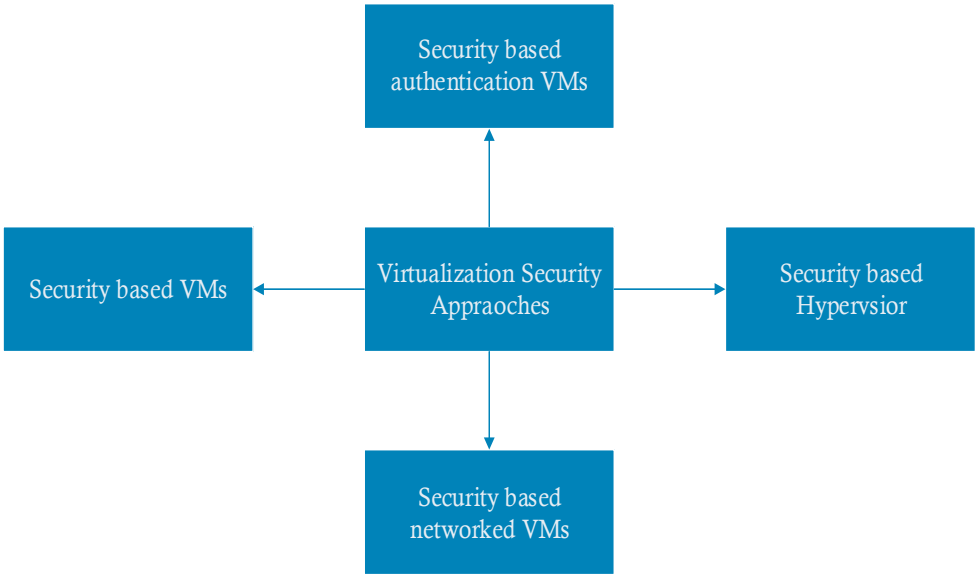

Figure 2 Main approaches solutions related to virtualization layer

4.2Existing virtualization based cloud security approaches

We have classified the virtualization security approaches into four types: Security based VMs, Security based hypervisor, Security based networked VMs, Security based authentication VMs. Each type of approach is dedicated for protecting the users' VMs from one or different attacks. In each approach, we will mention to which type of solution it belongs.

4.2.1Secure Simulation Tool (SecNetworkCloudSim)

Annane et al. [23] have proposed a secure simulator that integrates a proxy named Proxy-3S which protects the communication that occurs between distributed VMs in the same Datacenter. Proxy-3S ensures the protection of users' sensitive data against three well attacks: co-resident, hypervisor attack, and communication attacks. This simulator is considered as security approach based to networked VMs, hypervisor and VMs itself. However, the main limitation of the proposed proxy is not detecting the malicious communication that occurs between the different VMs deployed in different datacenters. There is a crucial need to detect malicious VMs communication in different edges based on integrated

blockchain. Further, Proxy 3-S is only given better results based on the simulation tool (Not in a real cloud environment).

4.2.2Co-location-resistant cloud (CLR)

Azar et al. [24] have proposed a placement algorithm named Co-location resistant (CLR) which protects the VMs against two kinds of co-location attacks. The co-location attacks are divided into two sub-attacks in the public cloud. The first attack is complete co-location whereas the adversary aims to co-locate with all users VMs. Otherwise, on the fractional attack which is the second kind of attack. The adversary targets some of VMs and not all VMs. The objective of this approach is to deploy the legitimate VMs in such a manner that Adversary VMs cannot co-locate with user VMs. The algorithm is targeting the optimization as well as the security aspects. This solution is considered as security approach based VMs. However, it needs more improvement related to the isolation of the VMs once they are executed in the cloud environment. Furthermore, the algorithm has not considered the risks when the VMs are communicating with each other and transferring the data which can affect the deployed task of application to be run correctly as well affect the integrity and confidentially of user data deployed on VMs.

4.2.3Dependency based Virtual Machine Placement (DTMC)

The authors have presented an approach of virtual machines placement on the cloud for defending against two types of attacks: co-resident attack and hypervisor attack [25]. The security of the VMs that sharing the same resources is depending not only on operating system and application they are running, but also the security of the virtual machines manager and VMs located on the same server. The approach employs Discrete Time Markov Chain (DTMC) to analyze any security threats on VMs. The approach deal with security risks of VMs by migrating them periodically from a host to another one in order to find out a placement algorithm for safely prevent VMs from being retrieved. This solution is considered as security approach-based hypervisor. However, this kind of solution leads to extra power consumption and may reduce the performance of the service offered by the cloud provider for the clients, which may break the Service Level Agreement.

4.2.4Dynamic secure interconnection (DSI)

One novel mechanism was proposed by [26] which solved the security of users' data being processed by the shared and virtualized platform on the cloud environment named Dynamic Secure Interconnection (DSI). DSI isolates the cloud environment into several trust virtual zones where the users can securely deploy their tasks. A virtual zone hosted various VMs together on the same costumer's group in the cloud. As the VM is hosted using the same costumer's group, the VM is considered trusted. This mechanism helps to protect the VM's information security when VM migrating from one network to another. This solution is considered as security approach based to networked VMs only. However, the migration solution causes extra bandwidth consumption overhead that degrades the quality of services or service level agreement (SLA) among users and a cloud service provider.

4.2.5Model based secure healthcare cloudlet (MSHC)

Somula et al. [27] proposed a model-based healthcare cloudlet for providing fast latency of services and security for patient's data in mobile cloud computing. In this model, the user sends intensive processing tasks such as analyze medical records for processing on third party named cloudlet, and then the cloudlet sends and communicates to the remote cloud for processing. The concept of the proposed model is beneficial for minimizing the response time of users' service requested and preventing the power leakage of mobile devices. The proposed model claims to protect sensitive healthcare data from attacks. This solution is considered as security approach based VMs. However, relying on the cloud security systems may not protect the users' data from adversary due to the open and heterogeneous wireless communication medium, which causes risky and unsecured access to cloud services.

4.2.6Authentication technique based-secure communication (ATSC)

A new authentication technique based-secure communication in the mobile cloud has been proposed by [28] to protect the control access of tenants to the cloud. The technique is based on mutual verification between users and cloud providers where both sides need to provide their legitimacy to each other. Due to the limited storage capacity of mobile devices, mobile users are not able to store the huge details of cloud services anonymously. Therefore, the technique exchanges only session key once the successful authentication of mobile users to cloud services occurs which decreases the computational cost. The technique uses a third party know as Trusted Third Party (TTP) to send the private keys and public keys for both users and service providers to ensure registration and the authentication phases. The legitimacy of both components is checked via the hashing and cryptographic methods. This solution is considered as security approach based to authentication VMs.

4.2.7Hypervisor solution based virtual machines (HypSec)

Hypervisors are considered as main components in cloud computing because of their ability to create and manage the VMs of different users. the research work of [22] has proposed a new hypervisor design for protecting the integrity and confidentiality of the guest VMs. The new hypervisor named HypSec splits the hypervisor into different partitions whether trusted or untrusted. The untrusted partition process the complex task of the hypervisor without access to the VMs' data. The proposed work has not considered the attacks that came from the communication and interaction between the VMs. This solution is considered as security approach-based hypervisor.

4.2.8Hybrid RSAECC Based Secure Communication in MCC

The proposed research work aimed to secure the mobile cloud environment by providing a model based on the authentication protocol for the mobile users that intend to leverage the cloud services [29]. The model uses a hybrid encryption and decryption technique, RSA (Rivest–Shamir–Adleman) and ECC (Elliptic-curve cryptography). The asymmetric combination model shows a high protection efficiency with less encryption and decryption time compared to existing solutions. However, this research work did not take into account the attacks that can occur in the virtualized environment which can circumvent the cryptography methods and steal the data that process on hardware resources such as CPU and Memory as well as the VMs' communication. This solution is considered as security approach based to networked VMs only.

5.Comparative study of related works

All of the above-described related works provide mechanisms for dealing with some common attacks and computation complexity of data security and privacy on the MCC based virtualization.

Table 1 Illustrates the comparison process of different solutions regarding several attacks

Proposed solution	Problem issues	Techniques used	Evaluated parameters	Strengths	Drawbacks
SecNetworkCloudSim [23]	VMs' sensitive data attack	Virtualization based Proxy technique to protect any sensitive user information.	- VMs' sensitive data Integrity. - Execution time.	- Proxy-3S is the only solution that ensures the protection of users' sensitive data against three well attacks: co-resident, hypervisor attack and communication attacks. - Less execution time.	- Proxy-3S is not detecting the malicious communication that occurs between the different VMs deployed in different datacenters - Proxy 3-S is only given better results based on simulation (Not in a real cloud environment)
CLR [24]	VMs co-residency	- Secure VMs placement algorithm - Cryptography-based Technique	VMs' data integrity	Ensure the protection of VMs against fractional and complete co-location	- Strong isolation between user VMs running on the cloud -Secure communication between VMs once distributed application tasks communicate with each other resources to run the content of VMs.

Proposed solution	Problem issues	Techniques used	Evaluated parameters	Strengths	Drawbacks
DTMC [25]	Co-resident attack and hypervisor attack	- Migration VMs- based Technique - Discrete Time Markov Chain	VMs' integrity	Protect user VMs whenever the possibility of co-location risks become higher by performing periodic migration from host to host.	- A power Consumption continuously increasing while migrating the corresponding VMs - May reduce the service performance offered for client which can break down the service agreement. - Migration is not always practical if the other hosts do not have enough resources to run the content of VMs.
DSI [26]	Malicious VMs	- Isolation of cloud environment into several trust virtual zones - Classify the same costumers VMs in same group in order to be among VMs' trust collection. - Migration policy performed if threats detected on VMs.	VMs' integrity	This mechanism helps to protect the VM's information security when VM migrating from one network to another	- The migration solution causes extra bandwidth consumption overhead that degrades the quality of services or service level agreement (SLA) among users and a cloud service provider.
MSHC [27]	Health- data retrieving attacks	- Model-based healthcare cloudlet for providing fast latency of services and security for patient's data	Patient Data security	The model minimizes the response time of users' service requested and prevents the power leakage of mobile devices	- The approach does not protect the users' data from adversary due to the open and heterogeneous wireless communication medium, which causes risky and unsecured access to cloud services.
ATSC [28]	Malicious access to cloud services	- Mutual verification between users and cloud providers where	-Verificationof Time - Data security	The technique exchanges only session key once the successful authentication of	Impact on response time for services that users require from the cloud provider

Proposed solution	Problem issues	Techniques used	Evaluated parameters	Strengths	Drawbacks
		both sides need to provide their legitimacy to each other.		mobile users to cloud services occurs which decreases the computational cost (Verification Time).	because the technique uses a third party know as Trusted Third Party (TTP).
HypSec [22]	Hypervisor-attack	Technique based on trusted partition of hypervisor	Hypervisor-integrity	Protecting the integrity and confidentiality-y of the guest VMs	The proposed work has not considered the attacks that came from the communication and interaction between the VMs.
RSAECC [29]	Authentication and communication of mobile users and services.	- Hybrid encryption and decryption technique, RSA and ECC	- Data integrity - Execution time	high protection efficiency with less encryption and decryption time compared to existing solutions	The technique proposed Does not take into account the attacks that can occur in the virtualized environment

For summarizing the research works stated in the *Table 1*. Most of the proposed solutions contain the main limitation which is the lack of safe interaction and protection among distributed VMs on the cloud. Han et al. [30] have presented two secure metrics to measure any attacks that occurred on the cloud server. However, they did not take into account the protection of distributed attacks (e.g: numerous VMs located in different servers and interacted with each other). The only solution that tried to protect the distributed attacks has proposed by [23]. However, their Proxy 3-S allocates a VM in a specific host. This VM must run on that specific host to be controlled by the proxy. A malicious VM can change its location in the same host to co-locate in other placement. Thus, it is necessary to detect any Co-placement of VMs. The proxy will be able to detect the malicious placement of VMs from a specific host. Depend on the identifier of the VM and identifier of the host, the proxy detects that identifier VM is not assigned to a specific identifier host.

6.Problem statement

Frequently, the VMs of various users processed on the same physical server (host) are consistently separated from each other. However, illegitimate users (consider as attackers) can break up the logical separation while exploiting and sharing the same cloud resources (Memory, CPU, and cache) and retrieve sensitive and private data like crypto keys from other VMs (co-location) [9, 26]. Some proposed solutions [27−29] attempt to tackle this type of threat "VM to VM attacks" by ignoring the side channel constructed between co-location VMs which is not allowed by the cloud policies [30]. Moreover, the suggested frameworks demand major changes to be implemented in the existing cloud commercial platform. Consequently, the proposed methods are impractical due to high deployment cost (i.e.: high execution time and high computation complexity). The main question to be highlighted by researchers is how to mitigate the VM Co-resident and the hypervisor attacks, also the attacks on remote VMs located on a different host. Other secondary questions to be addressed: (1) How to define the identity of the remote client and how to manage the privacy and confidentiality of VMs allocation requests of the mobile client on the cloud? (2) What are the methods that can be exploited for ensuring both virtual machine integrity and hypervisor security?

In the virtualization layer, there are numerous types of communication occurred between VMs for exchanging sensitive information between each other, for example, an intensive application which is splitted to various small applications and distributed on different servers). After the examination of the most limitations that exist on several co-location security approaches and techniques proposed by previous researchers [30]. We found out that no approach protects the data from being stolen while interacting between the VMs). For example, in

Figure 3 the VM 1 in host 1 communicates with VM 1 in host 2 to exchange information that can lead the attacker to steal the private data exchanged between them. Hence, the only solution which was proposed by [31] is a hardware-based technique with a high-cost barrier. Thus, an important question to be highlighted is how to protect the exchanged information between the VMs (distributed application) deployed in different host on the cloud side?

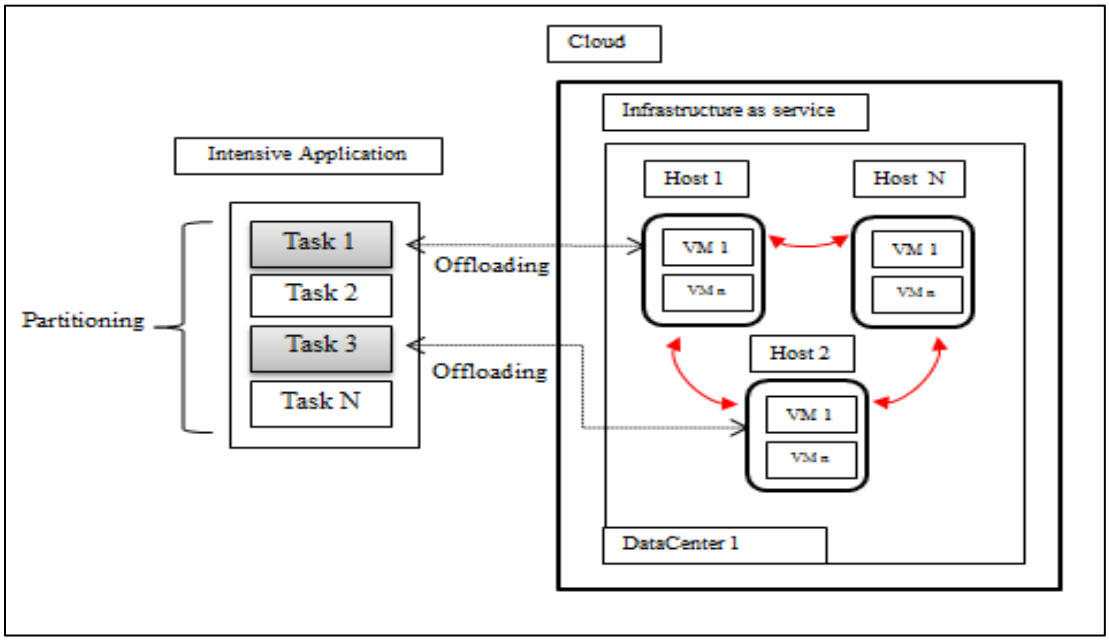

Figure 3 Communication of intensive application's tasks while deployed on Thin Virtual Machines

In order to answer the questions above, we suggest for researchers:

1. To design a user control access policies for prohibiting the unauthorized users to access to the cloud services and spreading malevolent VMs.
2. To design secure VMs manager policies, which protect the VMs allocation on the cloud hosts as well as protects the hypervisor from being retrieved by unauthorized malicious VMs.
3. To design a VMs communication policy and ensure the integrity and privacy of private data transferred among VMs. We believe that such a hybrid-policy would provide large protection against co-resident VM, VMM attacks, and communication attacks.

7.Conclusion and future works

With the increased number of mobile users on MCC, the security of the virtualization layer in cloud computing are becoming a target for malicious users to violate the sensitive data from the VMs. For that reason, many virtualization approaches have been proposed to overcome this issue. However, these approaches still not able to protect the interaction between the VMs once any exchange of information occurred. Several future directions still need to be carried out to protect the users' data. Firstly, the approaches need to be tested and evaluated using real cloud systems (Amazon EC2, Google App Engine) and open source Hypervisors like Xen and KVM to evaluate the approach performance in preventing malicious users' access to the cloud, c-location, and remote co-location (distributed attacks). As well, test the secure approaches with real intensive and sensitive applications like banking application and healthcare application that will be more effective and give real results about the performance of the approaches. Secondly, reducing the security management checking time is considered as the main challenge that needs to be carried out in the proposed approaches. As mention as a limitation of previous research, they make delays for controlling and verifying the whole VMs number on the cloud, which may cause a decrease in the cloud provider service quality and lose the trust of the cloud's tenants. Thus, incorporating the optimization method will be an excellent future work to reduce the security checking

time and make the proposed approaches more robust, flexible and adaptive for the current cloud systems.

Acknowledgment
None.

Conflicts of interest
The authors have no conflicts of interest to declare.

References
[1] Moorthy V, Venkataraman R, Rao TR. Security and privacy attacks during data communication in software defined mobile clouds. Computer Communications. 2020; 153:515-26.
[2] Shakarami A, Ghobaei-Arani M, Masdari M, Hosseinzadeh M. A survey on the computation offloading approaches in mobile edge/cloud computing environment: a stochastic-based perspective. Journal of Grid Computing. 2020:1-33.
[3] Tabrizchi H, Rafsanjani MK. A survey on security challenges in cloud computing: issues, threats, and solutions. The Journal of Supercomputing. 2020:1-40.
[4] https://flexiscale.com/. Accessed 20 June 2020.
[5] https://aws.amazon.com/fr/ec2/. Accessed 20 June 2020.
[6] https://aws.amazon.com/fr/s3/. Accessed 20 June 2020.
[7] Noor TH, Zeadally S, Alfazi A, Sheng QZ. Mobile cloud computing: challenges and future research directions. Journal of Network and Computer Applications. 2018; 115:70-85.
[8] Asvija B, Eswari R, Bijoy MB. Security in hardware assisted virtualization for cloud computing—State of the art issues and challenges. Computer Networks. 2019; 151:68-92.
[9] Compastié M, Badonnel R, Festor O, He R. From virtualization security issues to cloud protection opportunities: an in-depth analysis of system virtualization models. Computers & Security. 2020.
[10] Sgandurra D, Lupu E. Evolution of attacks, threat models, and solutions for virtualized systems. ACM Computing Surveys. 2016; 48(3):1-38.
[11] Han Y, Chan J, Alpcan T, Leckie C. Virtual machine allocation policies against co-resident attacks in cloud computing. In international conference on communications 2014 (pp. 786-92). IEEE.
[12] Han Y, Alpcan T, Chan J, Leckie C. Security games for virtual machine allocation in cloud computing. In international conference on decision and game theory for security 2013 (pp. 99-118). Springer, Cham.
[13] Aliyu A, Abdullah AH, Kaiwartya O, Hussain Madni SH, Joda UM, Ado A, et al. Mobile cloud computing: taxonomy and challenges. Journal of Computer Networks and Communications. 2020.
[14] Zhang J, Chen B, Zhao Y, Cheng X, Hu F. Data security and privacy-preserving in edge computing paradigm: Survey and Open Issues. IEEE Access. 2018; 6:18209-37.
[15] Dixit P, Gupta AK, Trivedi MC, Yadav VK. Traditional and hybrid encryption techniques: a survey. In networking communication and data knowledge engineering 2018 (pp. 239-48). Springer, Singapore.
[16] Mollah MB, Azad MA, Vasilakos A. Security and privacy challenges in mobile cloud computing: survey and way ahead. Journal of Network and Computer Applications. 2017; 84:38-54.
[17] Fan Y, Lin X, Tan G, Zhang Y, Dong W, Lei J. One secure data integrity verification scheme for cloud storage. Future Generation Computer Systems. 2019; 96:376-85.
[18] Dinh HT, Lee C, Niyato D, Wang P. A survey of mobile cloud computing: architecture, applications, and approaches. Wireless Communications and Mobile Computing. 2013; 13(18):1587-611.
[19] Veerabathiran VK, Mani D, Kuppusamy S, Subramaniam B, Velayutham P, Sengan S, et al. Improving secured ID-based authentication for cloud computing through novel hybrid fuzzy-based homomorphic proxy re-encryption. Soft Computing. 2020:1-6.
[20] Agrawal N, Tapaswi S. A trustworthy agent-based encrypted access control method for mobile cloud computing environment. Pervasive and Mobile Computing. 2019; 52:13-28.
[21] Perez-Botero D, Szefer J, Lee RB. Characterizing hypervisor vulnerabilities in cloud computing servers. In proceedings of the 2013 international workshop on security in cloud computing 2013 (pp. 3-10).
[22] Li SW, Koh JS, Nieh J. Protecting cloud virtual machines from hypervisor and host operating system exploits. In {USENIX} security symposium ({USENIX} security 19) 2019 (pp. 1357-74)
[23] Annane B, Alti A, Ghazali O. Secnetworkcloudsim: an extensible simulation tool for secure distributed mobile applications. International Journal of Communication Networks and Information Security. 2020.
[24] Azar Y, Kamara S, Menache I, Raykova M, Shepard B. Co-location-resistant clouds. In proceedings of the 6th edition of the ACM workshop on cloud computing security 2014 (pp. 9-20).
[25] Li M, Zhang Y, Bai K, Zang W, Yu M, He X. Improving cloud survivability through dependency based virtual machine placement. In SECRYPT 2012 (pp. 321-6).
[26] He L, Huang F, Zhang J, Liu B, Chen C, Zhang Z, et al. Dynamic secure interconnection for security enhancement in cloud computing. International Journal of Computers Communications & Control. 2016; 11(3):348-57.
[27] Somula R, Anilkumar C, Venkatesh B, Karrothu A, Kumar CP, Sasikala R. Cloudlet services for healthcare applications in mobile cloud computing. In proceedings of the international conference on data engineering and communication technology 2019 (pp. 535-43). Springer, Singapore.
[28] Jegadeesan S, Azees M, Kumar PM, Manogaran G, Chilamkurti N, Varatharajan R, et al. An efficient anonymous mutual authentication technique for

providing secure communication in mobile cloud computing for smart city applications. Sustainable Cities and Society. 2019; 49:101522.
[29] Sridhar S, Smys S. Hybrid RSAECC based secure communication in mobile cloud environment. Wireless Personal Communications. 2020; 111(1):429-42.
[30] Han Y, Chan J, Alpcan T, Leckie C. Using virtual machine allocation policies to defend against co-resident attacks in cloud computing. IEEE Transactions on Dependable and Secure Computing. 2015; 14(1):95-108.
[31] Hao Z, Tang Y, Zhang Y, Novak E, Carter N, Li Q. SMOC: a secure mobile cloud computing platform. In conference on computer communications 2015 (pp. 2668-76). IEEE.

Boubakeur Annane is a Ph.D Graduate student from School of Computing, at Universiti Utara Malaysia, Malaysia. He is currently a Part time Tutor at Unicaf University, Cyprus. He is a member of the InterNetworks Research Laboratory. He is also a member of the IEEE. Dr. B. Annane has published several numbers of articles in international journals and conferences. His research interests are Mobile Cloud Computing, Cloud Computing, Data Security and Privacy, Virtualization, Network and Distributed System Security.
Email: boubakeur.annane@gmail.com

Adel Alti is an Associate Professor at University Ferhat Abbas Setif-1 Algeria since 2013. Adel holds a Ph.D. degree in Software Engineering from University Ferhat Abbas Setif-1, Algeria, 2011. He did his Postdoc at Department of Technology & Exact Sciences, University of Biskra in 2013. He is a header of the Smart Semantic Context-aware Services research group of Network and Distributed System Laboratory. In 2017, Adel was the Head of Scientific Community of Computer Science Department, Sciences Faculty, University Ferhat Abbas Setif-1 Algeria. His area of interests includes Mobility, Cloud Computing, Pervasif and Ubiquitous Computing, Automated Software Engineering, Mapping Multimedia Concepts into UML, Context-aware Quality Software Architectures and Automated Service Management, Security, Context and QoS. He supervised a number of PhD and Master Students. Dr. A. Alti has published number of books' chapters, and articles in international journals and conferences. He is member of IEEE Computer Society.
Email: alti.adel@univ-setif.dz

Osman Ghazali is an Associate Professor and Deputy Dean of the School of Computing, Universiti Utara Malaysia. Osman holds a Ph.D. degree in Information Technology (Networking) from Awang Had Salleh Graduate School, Universiti Utara Malaysia (AHSGS). He did his post-doctoral as a research scientist at the School of Engineering & Applied Science, Aston University (EAS) in 2012. In 2011, Osman was the Head of Computer Science Department, School of Computing, Universiti Utara Malaysia. Before that, from 2009 to 2011, he was the Technical Chairperson at the University Teaching and Learning Center, Universiti Utara Malaysia. Dr. Osman has more than 100 publications as refereed book chapters and refereed technical papers in journals and conferences. He is a senior member of the InterNetworks Research Laboratory. He is also a member of the IEEE and the ACM.
Email: osman@uum.edu.my