Virtualization-Based Security Techniques on Mobile Cloud Computing: Research Gaps and Challenges

https://doi.org/10.3991/ijim.v13i04.10515

Boubakeur Annane (✉), Osman Ghazali
Universiti Utara Malaysia, Sintok, Kedah, Malaysia
jakhar256@yahoo.com

Abstract—The principle constraints of mobile devices are their limited resources such as processing capability, storage space and battery life. While cloud computing offers a vast computing resources services. A new idea emerged by including the cloud computing into mobile devices to augment the capacities of the mobile devices resources such as smartphones, tablet, and other personal digital assistant (PDA) which provides a robust technology called Mobile Cloud Computing (MCC). Although MCC have brought many advantages for the mobile users, it also stills suffer from security and privacy side of data while hosted on virtual machines (VM) on remote cloud's servers. Currently, the eyes of the security expert's community turned towards the virtualization-based security technique either on the Cloud or on the mobile devices. The new challenge is to develop secure methods in order to authenticate high sensitive digital content. This paper investigates the main challenges regarding the security and privacy issues in mobile cloud exactly focusing on the virtualization issue layer and give clear strengths and weaknesses of recent relevant virtualization security techniques existing in the literature. Hence, the paper provides perspectives for researchers in order to achieve as a future work.

Keywords—Mobile cloud computing, virtualization, security and privacy of information, user virtual machines

1 Introduction

Nowadays, Cloud Computing is an attractive technology that is known to have an increasing importance for users by delivering the services over the Internet. It is defined as an Information Technology (IT) paradigm that allows the user to exploit cloud services in on-demand way [1]. Three main services are provided: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). In IaaS, virtualization relies on sharing computing resources rather than having personal mobile devices to handle and to perform applications and tasks simultaneously and efficiently[3].

Mobile Cloud Computing (MCC) is considered as an important technology that has grown fast among individual and community of users. It combines cloud computing paradigm with mobile devices through wireless technology in order to avoid the devices' restricts resources capacities and leveraging the cloud computing services offering [2]. The mobile devices such as smartphone and tablets have several limitation resources capacities (CPU, memory and storage space) which inhibit the developers to provide powerful applications as well as hinder the users to enjoy the various mobile applications in their daily life [3]. Integrating cloud computing services with mobile computing is an interesting solution to solve the related issues. MCC allows users to move and to upload their applications, services, and data on the shared cloud servers for exploiting large storage capacity and high-computing resources when running intensive applications and remote data storage that exhaust the battery life of the mobile devices. Recently, the use of the mobile devices is not only retained for simpleapplications but also complex and crucial applications which deal with a sensitive data with various multimedia contents (texts, images, audios and videos) such as banking application, health, transport, etc. The moving of clients' services and data to the cloud technology raise many security challenges especially data security and privacy protection that become major and serious concerns because data is located in different distributed places.

Security is considered as amajor challenge against MCC environment. The mobile cloud security issues are inherited from cloud computing, so they are the same issues but also more critical on MCC because of incapacity of limited devices' resources (e.g.lack of CPU capability) to process intensive malware applications that protect the sensitive data compared to personal computers. The tenants' worries are concentrated on the migration to the cloud which might be faced more risks once they are sharing the same cloud resources with others tenants [4]. In MCC, the cloud service providers offer the sharing of their resources to the mobile users through one of the popular technique called virtualization that increases the efficiency and effectiveness of hardware utilization [5].Various users' virtual machines are running on the same cloud host when they share same cloud resources which lead to more additional security risks like violating the data once they share the same memory or CPU[6][7]. Consequently, an important question has to be highlighted whether the other cloud virtual machines' clients are trusted or not. Several robust security techniques have been proposed in this decade, a number of new techniques or improved versions of the latest approaches have been developed. However, most of the solutions proposed are not practical due to the critical change (eliminating side channels and removing such clocks as well as the hypervisor) in the cloud platform [5].In this work, we aim to collect and present some relevant virtualization-based security techniques currently available in the field and review in detail the topic that newly emerged various security challenges.

The rest of this paper is organized as follows. Firstly, we present basic requirements of the virtualization techniques on Mobile Cloud Computing. We detail malicious attacks and quality measures are briefly reviewed. Then, we discuss the recent virtualization security techniques. Thereafter, some comparison and evaluation of different approaches are presented. Then, we present discussion and research gaps and challenges on security-based virtualization layer that we noticed in our point of view. Finally, in the last section, we conclude and present some future work.

2 Virtualization-Based Security Preliminaries

In MCC, the cloud services are provided for mobile users using virtualization technologies. The virtualization process can increase hardware utilization (efficiency) between 60% and 80% [8]. The virtualization is defined as a middle layer between the software and hardware layers in the cloud servers that allows the cloud provider to efficiently exploit their services and computing resources [9]. These resources can be shared among multiple virtual machines in order to run them simultaneously and share also benefits from available servers' resources (e.g. CPU, network bandwidth, Memory, etc.) [10]. The use of remote servers leads to leverage the huge processing capacity also extends the battery life by saving the energy [11][12].

The execution of mobile applications is considered as computational intensive tasks that require a huge resources consumption of mobile devices. Indeed, this kind of challenge has been defeated by the offloading technique. The computational intensive application is divided to many tasks and the latter are migrated to the cloud (remote servers) for fast processing and the results back to the mobile terminals afterward [13]. In the cloud end, once the mobile task is offloaded, an image of virtual machine of the mobile device (*called also phone clone*) is pre-installed for processing the mobile user's data and application which increase the efficiency of the cloud environment and decrease the maintenance overhead on the mobile devices [4][14]. Therefore, running the phones clones of the mobile devices on the same server and isolate them is the main role of the virtualization technology. However, several works [5] [6][15][17][18][20][21] showed that virtualization has brought several security threats and issues [9] that affect the virtualized systems such as Denial-of-Service (DOS) attacks. This kind of attacks hit insipid information like workload statistics to know whether the system is vulnerable or not. Moreover, virtualization techniques on MCC brings new security risks such as unauthorized access from malicious VMs, VMs to VMs attacks, confidentiality of mobile users data, challenges within VM monitor (Hypervisor) and communication in a virtualized environment[4][9]. Thus, ensuring security mechanism that prevents leakage of sensitive data and information from legitimate phone clones is not an easy task.

In terms of security, the virtualization-based technique sare regrouped into two main categories, hardware-based techniques and software-based techniques. For the first class, we distinguish two security techniques: secure application cloning on VM [15] and the protection of VMs from the malicious hypervisor [16].For the second, we consider also two techniques: security on VM techniques [17][18][19][20] as well as security techniques based load balancing on VM [5][21].Fig. 1 summarizes the important classes of virtualization-based security approaches.

The virtualization-based security techniques have five important proprieties [18][22]: efficiency, coverage, complexity, security, and robustness. Roughly speaking, the efficiency is the number of malicious VM that succeeds to co-locate with target (victim VM), divided by the total number of VMs lunched by the attacker. Otherwise, coverage is the number of malicious VM that succeeds to co-locate with target, divided by the number of target lunched by legitimate user. Complexity defined to any secure complex technique that needs high execution time and high computation complexity to perform them which consumes huge energy from the cloud servers. While security refers to the privacy of the VMs and sensitive data which means that no one could remove or extract the data without knowing the secure key. Similarly robustness designs the degrees of resistance against any kind of manipulation. The new approach must contain a trade-off between the five proprieties cited bellow.

Many researchers have undertaken to develop frameworks, policies, and approaches against this kind of challenges to ensure the security aspects for the mobile users. These methods are mainly focused on how to ignore the side channels attacks between VMs while the malicious VMs access the cloud servers [23][24][25][26]. However, all the methods proposed needs fundamental changes to the current commercial platform and they are not practical and not immediately deployed [18].Furthermore, other strong methods are hardware-based technique and not software techniques which lead to a high cost barrier[15].

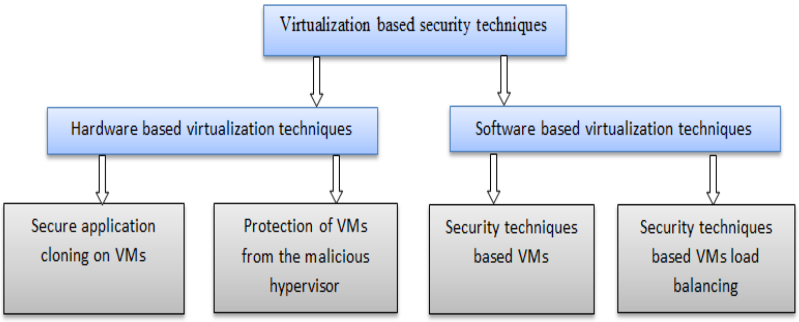

Virtualization based security techniques
Hardware based virtualization techniques
Software based virtualization techniques
Secure application cloning on VMs
Protection of VMs from the malicious hypervisor
Security techniques based VMs
Security techniques based VMs load balancing

Fig. 1. Classification of virtualization-based security techniques

3 Virtualization-Based Security Techniques

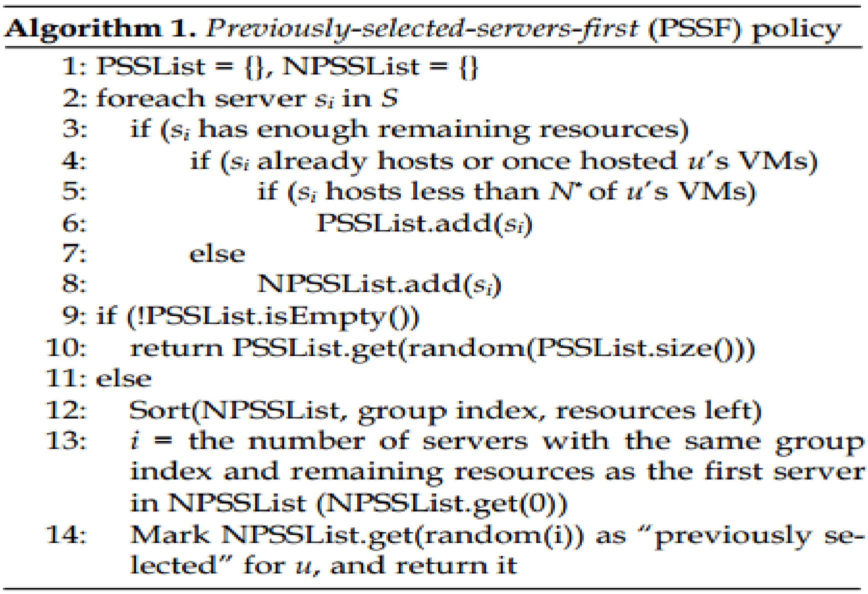
How to protect virtual machine (VM) and sensitive data is always one of the most important topics in the MCC. Recent security techniques have been used largely to tackle the security issues related to the virtualized environment in either Cloud or mobile cloud computing [5] [15-21].This section discussed some recent techniques on literature:

3.1 Virtualization-Based Security VM Techniques

Hardware virtualization-based technique for securing application cloning on VM: ZijiangHaoet al. [15] have presented a platform called Secure Mobile Cloud Platform (SMOC) for securing the mobile cloud environment. The platform allows the user to run their applications whether on the cloud or on the mobile devices itself. In contrast, the proposed platform includes two concepts. The first one is sharing resource which means that a mobile application can freely change the running location for getting better user experience, not explicitly (obligatory)on the cloud. This design provides more flexibility compared to other proposed approaches and techniques. The second concept is ensuring security even though the operating system of the mobile device has been attacked. A thin virtual machine shares its information and files with the mobile device once the mobile application running in the cloud. Conversely, the mobile device shares its files and information (devices inputs/outputs) with VM-cloud for running the application. Despite the benefits of this platform towards security concerns, there are many assumptions are not considered by the researchers such as untrusted hypervisor and untrusted public cloud provider. The proposed platform ensures the data security and privacy only when both assumptions (cloud provider and hypervisor) are assured. Thus, this platform ensures the security towards untrusted guest operating system which runs also unsecure applications.

Encryption Protocol-based virtualization technique for trusting lunch of VM: Paladiet al.[17]proposed a framework for data and transaction security of infrastructure services. The proposed framework contains various protocols for trust and the storage protection operation called Domain-Based Storage Protection (DBSP) and other protocols for trusting the virtual machines deployment called Trust-Lunching. Trust VMs made a more suitable method that the virtual machines are running inside a trusted host using secure computing techniques. The proposed work realized several security analyses against attacks and the obtained results improve the robustness and the efficiency of this framework. For more details, before the deployment of guest VMs, the protocol of trust VMs is performed. The second protocol is used cryptography techniques outside the IaaS domain for ensuring the data confidentiality stored in the cloud. Hence, the work has presented a list of malicious host attacks against IaaS environment to produce both secure protocols. The proposed framework can be integrated to the existing cloud platform due numerous experimentations and tests that have been realized on tenants' sensitive data (e.g. public healthcare patients' data). However, this work has considering specified attacks on IaaS platform which not guarantee for other security threats such as hypervisor attacks, co-resident attacks and so on.

VM allocation policy for defending co-residency attack: Frequently, VM of different mobile users executed on the same physical host are logically isolated from each other. However, malevolent users can escape the logical isolation while sharing the same resources (CPU, memory, and cache) and capture sensitive and private information like crypto keys from co-resident virtual machines [6][7]. Han et al.[18] have proposed a new secure VM allocation policy called Previous Selected Servers First Policy (PSSF). The algorithm is shown in Fig.2. The aim of this policy is to defend against co-resident attack. However, the proposed algorithm lack of different security enhancement such as securing the mobile device VMs residing on it, live migration, securing the communication data between the VMs while located on mobile devices and the Cloud. The algorithm also lacking from distributed application security algorithm deployed whether on mobile and cloud. Also, this algorithm targeting only the co-resident attacks and it does not target the other attacks like distributed VMs attacks communication, hypervisor attacks, and mobile device data attacks.



Algorithm 1. *Previously-selected-servers-first* (PSSF) policy

```
PSSList = {}, NPSSList = {}
foreach server $s_i$ in $S$
    if ($s_i$ has enough remaining resources)
        if ($s_i$ already hosts or once hosted $u$'s VMs)
            if ($s_i$ hosts less than $N^*$ of $u$'s VMs)
                PSSList.add($s_i$)
        else
            NPSSList.add($s_i$)
if (!PSSList.isEmpty())
    return PSSList.get(random(PSSList.size()))
else
    Sort(NPSSList, group index, resources left)
    $i$ = the number of servers with the same group
      index and remaining resources as the first server
      in NPSSList (NPSSList.get(0))
    Mark NPSSList.get(random(i)) as "previously se-
      lected" for $u$, and return it
```

Fig. 2. PSSF Algorithm[18]

Mechanism-based Network measurement for detecting VMs co-residency: Si *et* al. [20]presented a new schema for detecting the VMs Co-residency attacks by getting the location of the particular VM. The covert side channel is a kind of attacks when the isolation between the VMs are broken which lead to steal sensitive information from the users. To clarify more, the simple way to know whether two VMs are on the host is to rely on network metrics by performing TCP traceroute steps to get the IP address of Hypervisor. If two hypervisor IP addresses are the same that means corresponding VMs are on the same host (Co-resident). The advantage of this solution is increasing the difficulties to establish co-location. However, the attacker can use another technique and ways to steal information from legitimate user VMs. Thus, not a simple hiding of the IP address of hypervisor can be efficient to solve the co-residency issues.

In table I, the virtualization-based security techniques on VM are compared in terms of strength and drawbacks.

Table 1. Comparison of Different Virtualization-Based Security Techniques on VM

Authors	Technqiue	Strengths	Drawbacks
Zijiang Hao *et* al.[15]	Hardware virtualization-based technique.	-The security of mobile device operating system is ensured even when the latter is attacked. -The freely execution location of mobile application whether on the mobile device or cloud.	-The proposed workassume that both hypervisor and cloud are always secure, so if the adversary succeeds to penetrate them, the data of the user would be in risks -Dynamic migration of mobile application within VMs on the cloud.
Paladi*et* al. [17]	-Protocol-based for trusted lunch of VM- encryption-based technique to protect the stored data using a trusted third-party entity	Ensure the confidentiality of sensitive data and information of the user	The framework handles specified attacks on IaaS platform that not guarantee for other security threats such as attacks on network communication, data geo-localization.
Han *et* al. [18]	VM allocation policy.	The policy protects the VMs allocated on the same host to be co-located from malicious user	-The policy does notsecure the interaction between VMs that allocated on different host -The policy does not secure the mobile user data while moving from the mobile device to the cloud. -The absence of data isolation while VMs communicate between each other. -Decrease the efficiency and coverage attacks only on the host.
Si *et* al. [20]	Mechanism -based Network measurement	Increasing the difficulties for malicious user to make co-location on the user VMS	Simple hiding of the Hypervisor IP address is not sufficient and the adversary can use another way to steal information from VMs

3.2 Virtualization-Based Load Balancing Security Techniques on VM

Dynamic allocation and migration for phone clones for preventing the covert channel attacks: Vaezpour et al.[21] have proposed a security scheme called Security-aware Provisioning and Migration Scheme (SWAP) for provisioning and migrating thin virtual machine or phone clone for preventing the covert channel attacks[21]. This kind of attack is a constructed link between VMs where the CPU cache and the memory bus are exploited to steal information from legitimate phone clones in a virtualized environment [6]. The goal of this work is to reduce the risks of covert channel when cloud provider does not have enough resources to isolate the foreigner's phones clones on the mobile cloud environment. The proposed scheme includes two techniques. The first one is provisioning of new phone clones where this technique works with mobile communication history to avoid users' phone clone to host with other strangers' thin virtual machine. The second technique is responsible for migrating the phone clones from one host to another when the threats of attacks increase. The first and second algorithm is used to allocate the phones clones on the specifics host by implemented various condition. The algorithm based on the communication history between the mobile users when the virtual machines represent node and communication between virtual machines represent the edges. Thus, both algorithms allocate the phones clones based on communication history between the mobile users. The phones clones that have communication link would not attack each other and may allocate in the same host. The third algorithm is for moving the phone clone from a host to another one in order to prevent the risks of retrieving the content of the phones clones from another adversary. The proposed solution has successfully kept little risks on phone clones compared with other proposed techniques. The main shortcoming of the proposed approach is that researchers of this works are assumed that two phone clones in the same host do not attack each other when they have a link of communication between them. This work does not consider different scenarios (co-resident attacks, hypervisor attacks) which can happen and produce several security threats on phone. The authors have presented three algorithms in this proposed schema.

Context-aware VM-allocation policy for defending against co-resident attacks: Han *et* al.[5] proposed an approach to minimize the co-resident attacks incloud environment. This work improved VM allocation policy, which extends PSSF tool (Previous Selected server first) [18] with three additional policies: security, power consumption, and load balance to enhance the effectiveness and the efficiency of the cloud platform environment .Moreover, they apply several experiments on the simulation cloud platform CloudSim and the obtained results show a remarkable robustness against co-resident attacks. However, the authors have only studied one type of attacks: co-resident attack occurred only inside one host and not distributed on different hosts. They also did not consider the migration attacks, which can make uplarge serious risks on VMs and increase the possibility of co-locating with VM victims.

Table II illustrates a comparison between different virtualization-based load balancing techniques on VMin terms of strength points and drawbacks remarked.

Table 2. Comparison of Different Virtualization-Based Load Balancing Security Techniques on VM

Authors	Techniques	Strengths	Drawbacks
Vaezpour et al.[21]	1-Model-based users' communication relationship and the potential risks when co-locating phone clones. 2- Minimizing potential risks based on clique-covering technique. 3-Migration strategy based on a decay function time varying feature of covert channel.	-Successfully minimized the risk of phone clones' attacks compared with naïve provisioning and migration algorithm. -Trade-off between security and load balancing	The works does not assume that two phone clones in the same host can attack each other when they have a link of communication between each other
Han *et* al.[5]	Load balancing VM-allocation policy	-The policy protects the VMs allocated on the same host to be co-located from malicious user -Trade-off between security, load balancing, power consupmtion	-The absence of data isolation while VMs communicate between each other (such tasks of distributed application). -Migration of VMs: they do not consider the migration attacks which can happen due to the vulnerabilities of migration algorithm

3.3 Virtualization Based Security Techniques on Hypervisor

Hardware-Assisted Secure VMs under a vulnerable hypervisor: Jinet al.[16] have proposed a new design for hardware based VM protection. The approach is called H-SVM, which is a Hardware-Assisted Secure Virtual Machine. The proposed mechanism protects the guest virtual machine for monitoring the malicious VM or hypervisor by isolating its memory virtualization. The authors have proposed a new flexible and efficient mechanism of memory protection by allowing restricted roles for the hypervisors and decoupling the memory isolation from memory allocation that is usually executed by the hypervisor. Therefore, the handler (processor)takes some roles of hypervisor such as scheduling VMs. The mechanism of changing the hardware architecture presents drawbacks regarding the deployment cost and not suitable for immediate deployment.

Mechanism-based Linux kernel Mandatory Access Control (MAC) for securing VMs Deployment: Liang et al.[19] have proposed an approach for securing the VMs deployment. This approach reinforces the isolation among the virtual machines and controls the availability of resources by using a security system mechanism called the Mandatory Access Control (MAC). The use of the MAC controls the access of a one process to another. They used the hypervisor that is running on the server operating system to secure the isolation of guest VMs. In addition, they implemented a secure channel for migrating the VMs whenever the risks threat becomes higher. Despite the benefits of the solution proposed, authors have assumed that the hypervisor is trusted and other studies proved that several crucial attacks may come from untrusted hypervisor. Therefore, the authors do not give an evaluation that makes their solution more understandable.

Table III shows a comparison between different virtualization-based security techniques on hypervisor in terms of strength points and drawbacks.

Table 3. Comparison of Different Virtualization Based Security Techniques on Hypervisor

Authors	Techniques	Strengths	Drawbacks
Jin*et al.*[16]	Hardware-Assisted Secure VM	-The work ensures the protection of the virtual machines under a vulnerable hypervisor.	-Hardware architecture changes are not practical due to high deployment cost in the current cloud platform
Liang *et al.*[19]	Mechanism-based Linux kernel Mandatory Access Control (MAC) for securing VMs	-The Security of deployed VMs via isolating technique.-Online VMs migration by introducing secure channel among them.	-A compromised or untrusted hypervisor will lead unguaranteed secure status of VMs.

4 Virtualization-Based Security Challenges

From the above table, it can be clearly seen that previous research works have many limitations regarding several reasons. First reason, such proposed solutions lack of mechanism that ensures the communication between VMs located on different servers. To clarify, researchers in [18] have done a great idea whereby provided two metrics for measuring the attacks(coverage and efficiency), but they do not consider the issues on data interaction between the VMs that attacker can violate while they communicate. The second reason, some solutions they assume that hypervisor is always protected unless the attacker can get the control of the Hypervisor, which directly controls the whole VMs. Finally, other solutions provided security for phone clones on the cloud side, but not on mobile devices. To perform security of mobile distributed applications using virtualization, we must include numerous challenging aspects in MCC: scalability, credibility and robust communication techniques. The presented secure mobile distributed applications are containing three main challenges can better perform the VM security and data privacy:

Virtualization-based scalability: The overload problem is one of the main reason that triggering the construction of virtualization-based load balancing system. To clarify, once the number of mobile users' requests for services is increasing, thus it makes a great challenge in which known as the load-balancing problem. A personalized security system [5] enables to handle the large scale of virtual machines and intensive applications management in cloud systems.

Virtualization-based credibility: Trustworthiness problem represents one of the great difficulties faced by security on MCC. The use of trust and information confidence on MCC allows making the cloud provider more reliable and capable to solve the problem of data credibility. Several researchers ensure the trustworthiness of cloud system by finding the trust server, in [27] with reputation value more than 0.8. This value according to his past feedback, this trust value enables to help mobile users for making the right offloading and solve the security problems such as integrity and confidentiality.

Virtualization-based distributed VMs with robust encryption communication technique: Mobile-based virtualization provides capabilities of exploiting and managing distributed heterogeneous application in the Cloud. Virtualization techniques provided a resource sharing mechanism that protects the sensitive data dynamically by isolating any malicious user task. The basic idea is to stop directly the attacker by passing on Cloud hypervisor and adapt advance virtualization-based hash techniques to preserve data integrity and confidentiality.

5 Conclusion and Future Works

With the appearance of new technologies, preserving security and authenticity of mobile application that exchanges sensitive data becomes a fundamental and necessary requirement on the cloud environment. Over previous years, a number of different researchers has proposed various virtualization-based techniques, but each method has a number of associated advantages as well as drawbacks. To clarify, the user thin virtual machines communicate with each other to exchange private and sensitive information (e.g. distrusted application executed in the different host). We have studied the limitations of most existing virtualization security co-location techniques proposed in the literature. As a result, we have identified that the main limitation is the absence of protecting sensitive information exchanged between mobile application's tasks deployed on different VMs on the cloud. In future work, we will present a new approach that contains three secure policies to protect user sensitive data against co-resident attacks, hypervisor attacks as well as preserve the communication of user sensitive data when deployed on different cloud host. Furthermore, we aim to provide for mobile users many advantages such as detection of unauthorized access, hypervisor security control on sensitive data and offers high confidentiality during the exchanging sensitive data among VMs.

6 References

[1] M. Deng and M. Petkovi, "A home healthcare system in the cloud – addressing security and privacy challenges," 2014.

[2] Y. Zhang, X. Chen, J. Li, D. S. Wong, H. Li, and I. You, "Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing," Inf. Sci. (Ny). 2015. https://doi.org/10.1016/j.ins.2016.04.015

[3] M. R. Rahimi, J. Ren, C. H. Liu, A. V. Vasilakos, and N. Venkatasubramanian, “Mobile cloud computing: A survey, state of art and future directions,” Mob. Networks Appl., vol. 19, no. 2, pp. 133–143, 2014. https://doi.org/10.1007/s11036-013-0477-4

[4] M. B. Mollah, M. A. K. Azad, and A. Vasilakos, “Security and privacy challenges in mobile cloud computing: Survey and way ahead,” J. Netw. Comput. Appl., vol. 84, pp. 38–54, 2017. https://doi.org/10.1016/j.jnca.2017.02.001

[5] Y. Han, J. Chan, T. Alpcan, and C. Leckie, “Using Virtual Machine Allocation Policies to Defend against Co-resident Attacks in Cloud Computing,” vol. 5971, no. c, pp. 1–14, 2015. https://doi.org/10.1109/tdsc.2015.2429132

[6] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, “Hey, You, Get Off of My Cloud : Exploring Information Leakage in Third-Party Compute Clouds,” pp. 199–212, 2009. https://doi.org/10.1145/1653662.1653687

[7] Y. Zhang, A. Juels, M. K. Reiter, and T. Ristenpart, “Cross-VM Side Channels and Their Use to Extract Private Keys,” pp. 305–316; 2009. https://doi.org/10.1145/2382196.2382230

[8] F. Hu et al., “A Review on Cloud Computing : Design Challenges in Architecture and Security,” pp. 25–55, 2011.

[9] D. Sgandurra and E. Lupu, “Evolution of Attacks, Threat Models, and Solutions for Virtualized Systems,” vol. 48, no. 3, pp. 1–38, 2016. https://doi.org/10.1145/2856126

[10] M. M. Hassan, W. N. Ismail, and B. Song, “SPECIAL SECTION ON ADVANCES OF MULTISENSORY SERVICES AND Mobile Cloud-Based Big Healthcare Data Processing in Smart Cities,” 2017.

[11] A. Ellouze, M. Gagnaire, and A. Haddad, “A Mobile Application Offloading Algorithm for Mobile Cloud Computing,” 2015. https://doi.org/10.1109/mobilecloud.2015.11

[12] N. M. Dhanya and G. Kousalya, “Adaptive and Secure Application Partitioning for Offloading in Mobile Cloud Computing,” vol. 1, pp. 45–53, 2015. https://doi.org/10.1007/978-3-319-22915-7_5

[13] M. Shiraz, A. Gani, R. H. Khokhar, and R. Buyya, “A Review on Distributed Application Processing Frameworks in Smart Mobile Devices for Mobile Cloud Computing,” vol. 15, no. 3, pp. 1294–1313, 2013. https://doi.org/10.1109/surv.2012.111412.00045

[14] J. Sahoo, “Virtualization : A Survey on Concepts, Taxonomy And Associated Security Issues.” 2010.

[15] Z. Hao, Y. Tang, Y. Zhang, E. Novak, N. Carter, and Q. Li, “SMOC : A Secure Mobile Cloud Computing Platform,” pp. 2668–2676, 2015. https://doi.org/10.1109/infocom.2015.7218658

[16] S. Jin, J. Ahn, J. Seol, S. Cha, J. Huh, and S. Maeng, “H-SVM : Hardware-assisted Secure Virtual Machines under a Vulnerable Hypervisor,” vol. 9340, no. c, pp. 1–14, 2015. https://doi.org/10.1109/tc.2015.2389792

[17] N. Paladi, C. Gehrmann, and A. Michalas, “Providing User Security Guarantees in Public Infrastructure Clouds,” vol. 7161, no. c, pp. 1–14, 2016. https://doi.org/10.1109/tcc.2016.2525991

[18] Y. Han, J. Chan, and C. Leckie, “Virtual Machine Allocation Policies against Co-resident Attacks in Cloud,” no. 1, pp. 786–792, 2014. https://doi.org/10.1109/icc.2014.6883415

[19] H. Liang, C. Han, and D. Zhang, “A Lightweight Security Isolation Approach for Virtual Machines Deployment,” pp. 516–529, 2015. https://doi.org/10.1007/978-3-319-16745-9_28

[20] Y. Si, G. Xiaolin, L. Jiancai, Z. Xuejun, and W. Junfei, “Detecting VMs Co-residency in the Cloud : Using Cache-based Side Channel Attacks,” vol. 2, pp. 73–78, 2013. https://doi.org/10.5755/j01.eee.19.5.2422

[21] S. Y. Vaezpour, R. Zhang, K. Wu, J. Wang, and G. C. Shoja, "Journal of Network and Computer Applications A new approach to mitigating security risks of phone clone co-location over mobile clouds," J. Netw. Comput. Appl., pp. 1–14, 2016. https://doi.org/10.1016/j.jnca.2016.01.005

[22] H. Suo, Z. Liu, J. Wan, and K. Zhou, "Security and privacy in mobile cloud computing," 2013 9th Int. Wirel. Commun. Mob. Comput. Conf., pp. 655–659, 2013.

[23] B. C. Vattikonda, "Eliminating Fine Grained Timers in Xen Categories and Subject Descriptors," pp. 41–46, 2011.

[24] J. Wu, L. Ding, Y. Lin, and N. M. Y. Wang, "XenPump : A New Method to Mitigate Timing Channel in Cloud Computing," 2012. https://doi.org/10.1109/cloud.2012.28

[25] A. Aviram, S. Hu, and B. Ford, "Determinating Timing Channels in Compute Clouds," pp. 103–108, 2010.

[26] J. Shi, X. Song, H. Chen, and B. Zang, "Limiting Cache-based Side-Channel in Multi-tenant Cloud using Dynamic Page Coloring," pp. 194–199,2011. https://doi.org/10.1109/dsnw.2011.5958812

[27] XU, Deliang, FU, Cai, LI, Guohui, et X, LIU. Virtualization of the Encryption Card for Trust Access in Cloud Computing. IEEE Access, 2017, vol. 5, p. 20652-20667. https://doi.org/10.1109/access.2017.2754515

7 Authors

Boubakeur Annane received his bachelor degree in Computer Science in 2011 from Ferhat Abbas Sétif 1 University, Setif, Algeria, and his Master in Fundamental Computer Science in 2014 from Kasdi Merbah Ouargla University, Ouargla, Algeria. Currently, he is a PHD student in School of Computing, Universiti Utara Malaysia, Malaysia. His research interests are Mobile Cloud Computing, Cloud Computing, Data Security and Privacy, Virtualization, Network and Distributed System Security.

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.

Article submitted 2019-02-06. Resubmitted 2019-03-15. Final acceptance 2019-03-17. Final version published as submitted by the authors.