ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/334655836

Universiti Utara Malaysia, Malaysia 1 Associate Professor and Deputy Dean of the School of Computing

Preprint · July 2019

DOI: 10.19101/IJACR.PID10

CITATIONS
0

READS
70

3 authors, including:

Alti Adel
Ferhat Abbas University of Setif
68 PUBLICATIONS **96** CITATIONS

SEE PROFILE

Some of the authors of this publication are also working on these related projects:

A Vehicular Ad hoc Networks(VANET) based cloud View project

Medical images data protection using blind watermarking techniques View project

All content following this page was uploaded by Alti Adel on 24 July 2019.

The user has requested enhancement of the downloaded file.

Research Article

International Journal of Advanced Computer Research, Vol 9(43)
ISSN (Print): 2249-7277 ISSN (Online): 2277-7970
http://dx.doi.org/10.19101/IJACR.PID10

A new secure proxy-based distributed virtual machines management in mobile cloud computing

Boubakeur Annane[1*], Osman Ghazali[2], and Adel Alti[3]
Ph.D. Student in School of Computing, Universiti Utara Malaysia, Malaysia[1]
Associate Professor and Deputy Dean of the School of Computing, Universiti Utara Malaysia[2]
Associate Professor, University Ferhat Abbas Setif-1, Algeria[3]

Received: 27-August-2018; Revised: 27-November-2018; Accepted: 30-January-2019
©2019 Boubakeur Annane et al. This is an open access article distributed under the Creative Commons Attribution (CC BY) License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Abstract
The mobile cloud computing as an excellent paradigm offers on-demand services, whereas users can be confident once using them. Nevertheless, the existing cloud virtualization systems are not secure enough regarding the mediocre degree of data protection, which avoids individuals and organizations to engage with this technology. Therefore, the security of sensitive data may be affected when mobile users move it out to the cloud exactly during the processing in virtual machines (VMs). Many studies show that sensitive data of legitimate users' VMs may be the target of malicious users, which lead to violating VMs' confidentiality and privacy. The current approaches offer various solutions for this security issue. However, they are suffering from many inconveniences such as unauthorized distributed VM access behavior and robust strategies that ensure strong protection of communication of sensitive data among distributed VMs. The purpose of this paper is to present a new security proxy-based approach that contains three policies based on secured hashed Diffie-Hellman keys for user access control and VM deployment and communication control management in order to defend against three well-known attacks on the mobile cloud environment (co-resident attacks, hypervisor attacks and distributed attacks). The related attacks lead to unauthorized access to sensitive data between different distributed mobile applications while using the cloud as a third party for sharing resources. The proposed approach is illustrated using a healthcare case study. Including the experimental results that show interesting high-efficiency protection and accurate attacks identification.

Keywords
Security and privacy, Virtualization, Secure proxy-based approach, Cloud co-residency attacks, Distributed connected VMs, Secure VMs communication.

1.Introduction
With the massive growing utilization of limited mobile devices in everyday life, the data exchange of distributed applications for such mobile devices becomes a major concern. In light of this urgency for managing the voluminous data, mobile computing is integrated within cloud computing, which brings a new technology called Mobile Cloud Computing (MCC) [1, 2]. With the MCC, the exchange of digital content has become easier and faster. The MCC relies on a virtualization mechanism while providing services for the cloud's users. Virtualization is a very promising mechanism in cloud computing, which increases the efficiency of exploiting shared hardware resources such as memory, cache, and CPU of servers [3].

In this context, researchers in [4−6] pointed out that virtualization has brought several security threats and issues. Many serious and various attacks have been illustrated in [5] that affect the virtualized systems such as Denial-of-Service (D.S) attack.

Recently, a number of critical distributed mobile applications raised the need to solve the security challenges on virtualization. Consequently, several works based on virtualization have been proposed in the literature [7−14]. However, all the proposed methods have common drawbacks that require high deployment cost in terms of high execution time and high computation complexity for implementation and not immediately adopted under continuous changing of cloud platforms. Moreover, researchers in [12] focused on virtual machine (VM) allocation policy to defend against the well-known attack which is called

*Author for correspondence

co-residency attack. Nevertheless, all related works are suffering from limitations such as robustness against attacks that target the VMs deployed on the different distributed hosts, secure communication failures and poor security-quality under known attacks on VMs.

In this paper, we propose a new security proxy-based approach that contains three policies using secured Hashed Diff-Hellman keys for user access control, VM deployment and communication control management for the purpose of accurate attack identification and high-efficiency protection. This work contrasts with more security and data privacy side of the mobile user VMs ranging from the mobile device till offload to the cloud and until received by the authorized receiver. Such an approach is useful to solve the data security and to reach a high level of robustness to protect the data integrity and confidentiality in unsecured networks against different attacks (co-resident attacks, distributed attacks, and the hypervisor attacks). Another key motivation was to ensure a whole data security and privacy protection of sensitive data of the client mobile application and VM integrity of different distributed mobile applications via a secure proxy. The main contribution consists of a combination of three secure policies: (1) - mobile user control access policy for preventing both unauthorized access of malicious users to the cloud service provider and preventing allocation of VMs attackers, (2) hybrid-policy which combines the VM allocation policy with the hypervisor protection policy to guarantee both the phone clone (virtual machine) integrity and hypervisor integrity and (3) proxy-based security technique on the cloud using three hierarchical trusts levels that guaranty the privacy and the confidentiality of sensitive information exchanged between VMs. All these policies are based on secured hashed Diffie-Hellman Keys [15, 16] for user access control and VM deployment and communication control management. We evaluate our approach against a wide-range of attack scenarios in the health domain to demonstrate the superior performance of the proposed techniques.

The remainder of this paper is organized as follows: Section 2 details other related works. In Section 3, the proposed approach is explained in details. Section 4 illustrates our approach using the healthcare case study. Section 5 gives a Prototype Implementation of Secured Hash and Diffie-Hellman keys integrated into the approach. Finally, Section 6 concludes the paper and gives ongoing future works.

2.Related work

Several virtualization techniques were proposed for ensuring the security management of VMs. In MCC, the cloud services are provided for mobile users using virtualization technologies. IT research organization (InfoTech) considers that the distributed Host on different datacenters without virtualization leverage only 20% of the full capacity. The virtualization process can increase hardware utilization (efficiency) between 60% and 80% [17]. Virtualization is defined as a middle layer between the software and hardware layers in the cloud servers that allows the cloud provider to exploit their services and computing resources efficiently [5]. These resources can be shared among multiple VMs in order to run them simultaneously (at the same time) and share also benefits from available servers' resources (e.g., CPU, network bandwidth, Memory, etc.) [18]. In the cloud end, once the mobile task is offloaded, an image of VM of the mobile device (called also phone clone) is pre-installed for processing the mobile user's data, processes and application which augment the efficiency of the cloud environment and decrease the maintenance overhead on the mobile devices [1, 19]. Therefore, running the phones clones of the mobile devices in the same server and isolate them is the responsibility and the main aim of the virtualization technology.

For the cloud client, VMs help to tear out the maintenance of computing resources from the client device itself and enabling scalability of resources enough to accept any added functionality at any given time. For the cloud providers, VM increases the effectiveness and the efficiency of the hardware's utilization rate [12]. However, these benefits, virtualization technique when applied to MCC, it brings new security risks such as unauthorized access from malicious VMs, VMs to VMs attacks, confidentiality of mobile users' data, challenges within the VM monitor and communication in a virtualized environment [5]. Hence, ensuring security mechanism that prevents leakage of sensitive data and information from legitimate phone clones is not considered as an easy task. Many researchers have undertaken to develop frameworks, policies, and approaches against this kind of challenges to ensure the security aspects for mobile users. These methods mainly focused on how to ignore the side channels attacks between VMs while the malicious VMs access the cloud servers [7−11, 20]. However, all the methods proposed needs fundamental changes to the current commercial platform and they are not practical and not immediately deployed [21]. Other

solutions have been proposed by [9−11] to solve these security issues. However, all the proposed methods have common drawbacks that require high deployment cost in terms of high execution time and high computation complexity of implementing and not immediately adopted under continuous changing of cloud platforms. This is one of the reasons that motivates us to find a low-cost solution-based software implementation (not hardware) with the immediate practical realization.

Other related works presented by [22, 23] consist of increasing the difficulties to establish co-resident attacks using the network-based measurement (e.g., same VMs IP addresses are considered co-resident). In these attacks, the hypervisor is the target to get the IP address of VMs. Such solutions can be broken and not a simple IP address hiding can protect victim VMs (i.e., the attackers do not only rely on VMs' IP addresses [12]. Moreover, [24, 25] have presented techniques consists of detecting the malicious VMs attacks (abnormalities features happen to CPU and RAM once the attackers want to retrieve sensitive information from VMs). Further, migrating the VMs from a host to another host on the cloud is a proposed solution by [13,14], but these solutions have led to consume more power as well as degrade the quality of service such as service level agreement (SLA) between cloud's client and the cloud service provider. Using VM allocation policies is one of our interests which can make difficulties in establishing co-resident attacks. Co-resident VMs (VMs running on the same physical server) are logically isolated from each other, but attackers can build many side channels to avoid the isolation and retrieve sensitive data from legal VMS (legal mobile user). Researchers in [4] have shown that an attacker can reach 40% as efficiency, which means that an attacker when spread 10 VMs attacker, 4 of them can co-locate with target VMs (victim). Such solutions have been only proposed in [12, 26] to tackle this issue [27]. We restrict our attention in this work to wide critical common attacks, namely co-resident attacks, distributed attacks, and the hypervisor attacks which affect the thin VMs and violate their sensitive information.

3.The proxy-based secure distributed virtual machines management in the mobile cloud computing

In this section, we present our approach to protecting sensitive data shared among distributed mobile applications against different common attacks on a virtualization layer such as co-resident attacks, hypervisor attacks and distributed attacks. Three well-known security policies are included in this approach that ensures the sensitive data safety via protected distributed mobile applications to be intercepted and altered while communicate which each other, which lead to achieving a high-security level on both cloud and mobile device parts. In order to enhance the security level for sharing sensitive data in the MCC and managing distributed VMs in a high abstraction level, the proposal combines three well-known security-based policies (i.e. co-resident attacks, hypervisor attacks and distributed attacks) with a new security proxy-based approach for modeling the privacy level of sensitive data exchanged between different distributed mobile applications while the cloud is used for sharing computing resources and its ability to manage VMs efficiently. This approach aims to significantly increase a distributed mobile application ability to be more robust and to cover a maximum protection space against thin VMs' attacks occurred inside and between different cloud hosts and also in the mobile device itself. Our approach is dedicated to isolating VMs over fraudulent exchanges of sensitive data. Fraudulent exchanges can occur due to unauthorized VM who aspire to share and to access the data through cloud host or the communication gateway. These attacks exactly performed while leveraging the virtualization techniques. The approach will also aim for reducing the cost in terms of security execution checking time and computational complexity (i.e., proxy-based as a principal gate) as another benefit that makes the solution more practical and desired for the current cloud platforms. We extended and adapted the work of [21] for distributed mobile application in order to increase the coverage and efficiency attack while reducing the attacked rate and the security checking time. *Figure 1* shows our proposal, whereby we integrate VMs secure interaction among various VMs deployed on different hosts or with the external environment (mobile user) along with three security policies: input and output interfaces, hypervisor, and untrusted sensitive data using a security-based proxy.

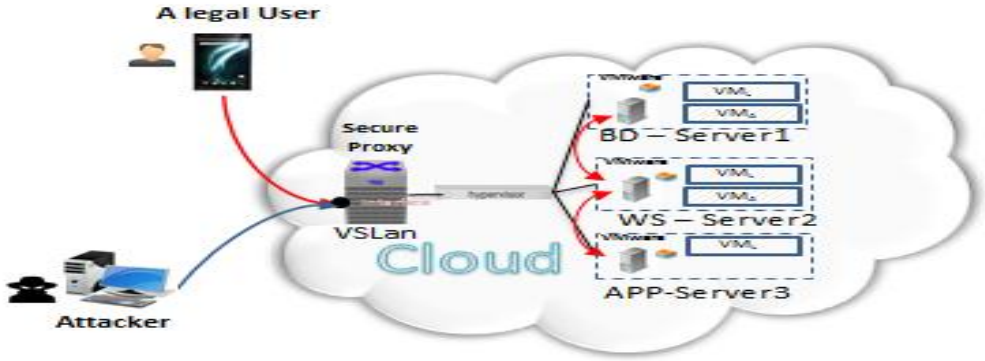

Figure 1 The secure proxy-based security virtual machine architecture

3.1Secure proxy-based conceptual model

The increasing need for an effective and efficient approach that can cover the maximum threats and risks which can occur for the legitimate VMs become a major concern. This is very helpful to answer the required protection of the user sensitive-data from being stolen, whether is hosted on the mobile device or the cloud (on same or different hosts). The most efficient approach for protecting and maintaining the user sensitive-data over malicious attacks has led a trade-off between costs (e.g., fast checking execution time, low computation complexity) and improved security. The proposed conceptual model is shown in *Figure 2*. The protection of sensitive data in the distributed mobile application becomes a major issue, and it involves a wide range of several activities from various actors with distinct sites exchange a great amount of data, which make the security of such data very costly. Therefore, sensitive data may be the target of malicious attacks due to the lack of privacy and confidentiality checking. Unauthorized access to such sensitive data can cause many problems such as privacy violations. For achieving the main objective, two policies and one technique are included:

1. Design a client control access and secure VM allocation policies on the different hosts in the cloud.
2. Design a hybrid-policy consist of VM allocation policy and Hypervisor policy in order to ensure the data VMs from being retrieved as well as guarantee the thin VMs integrity and hypervisor integrity.
3. To develop a proxy-based security technique on the cloud in order to protect the transferring of sensitive data between VMs.

The conceptual model of the research proposal contains five main steps. The first step is responsible for controlling that no authorized access of mobile users using the service cloud of the distributed application (critical banking intensive application and mobile health application) is verified. The second step is responsible for monitoring and evaluating the security policies of the proposed approach in terms of pre-known metrics (i.e., coverage and efficiency of attacks) related to the number of targets VMs and input/outputs sensitive communication getaways. The third step is responsible for filtering and controlling the potential attacked host for VMs and restricted channels that transfer data from the mobile to the cloud which means reducing the number of externally available hosts, reduce the time and the cost benefits of exploiting a computing resource. This step aims to enhance the security level for sharing security analysis results using the Share Secure Result component to the proxy. It is responsible for providing security directives to the policies proposed on the approach. Finally, the last step called reallocation of VMs update the VMs allocation based on the proxy directives.

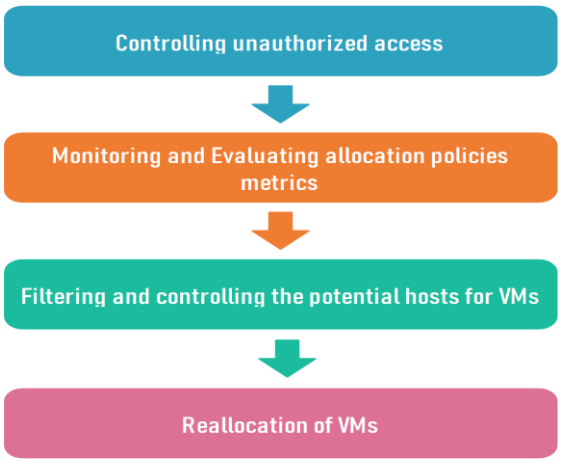

Figure 2 The secure proxy-based conceptual model

3.2Proxy-based security policies for distributed VMs management

Proxy-based Security Policies for distributed VMs Management contains three policies namely Mobile User Control Access Policy, Hypervisor Policy and VMs communication Policy.

3.2.1Mobile user control access policy

Firstly, before mobile user access to a service cloud provider for deploying their requested tasks, they authenticate by entering (Identifier, Password). The secure proxy checks if the mobile user has access or no (control access requirement). If a user exists in a Black List then return access denied. Else, the proxy has a User Authentication Table includes all the users that have access to the cloud service. In the case of the user provides correct identifier, and password (e.g., exists on the User Authentication Table), so we call hypervisor to allocate VM in any available host (server side). Elsewhere, the proxy increases the probability of unauthorized access and the user re-enter the identifier and the password. When the probability of unauthorized access becomes greater than a given threshold, the proxy detects the malicious mobile user, update the blacklist table and return access denied. After that, the mobile device that gets access will classify on User Trust Level Table as fully trust mobile device. The secure proxy classifies in the green level, the mobile device that provides the true identifier and password. *Figure 3* shows the secure mobile user control access policy included in the proposed proxy.

```
Enter the user identifier and the user password
If secure proxy finds a user exists in a blacklist then
   Deny the status of the user
else
while (the user identifier and the user password are not existing)
   Increase the probability of unauthorized access
   If  probability of unauthorized access greater than probability threshold then
      Insert the user in a black list  and deny the status of the user
   else
      Enter the user identifier and the user password and check again
End while
Authorized the status of the user
The user's virtual machine is allocated in the cloud host
Give the user a full authorization access (i.e. green trust level)
```

Figure 3 Secure mobile user control access policy

3.2.2Hypervisor policy

The secure proxy classifies in the green level, the mobile device that provides the true secure keys. Otherwise, the degrade mobile device to a lower level (orange or red) depends on the probability of the unauthorized access session. As a result, the mobile devices that have level 3 (red statue) will directly assign to another table named as a black list table and make access session denied. So, the proxy notifies the hypervisor of malicious detection and sends the order to the hypervisor to un-deploy all VMs and communication channel of the mobile device. *Figure 4* shows the secure hypervisor policy included in the proposed proxy.

3.2.3 VMs communication policy

When a given VM demand to establish a communication channel with another VM. The target VM asks the source VM to provide VM secret keys. In permanence when sending the data, the target VM continues to send its secret keys to the source VM. Otherwise, degrade VM to a lower level (orange or red) depends on the probability of unauthorized communication. As a result, the VM that has level 3 (red statue) will directly assign to another table named as local black list table and make access communication denied. So, the VM notifies the hypervisor to malicious VM detection, and so on to Proxy and increase the probability of unauthorized access. If a probability of unauthorized access exceeds the probability threshold, then the proxy sends the order to the hypervisor to undeploy all VMs and communication channel of the mobile device. *Figure 5* presents the secure VMs communication policy included in the proposed proxy.

4.Healthcare security: secure patient case study

This section illustrates the proposed secure proxy-based approach using an example of distributed health mobile application which exchanges sensitive

data between different sites on the cloud environment. This application contains many tasks (uploaded on VMs on the cloud) that communicate with each other in order to exchange sensitive and private information (e.g., temperature, blood analyses, etc.). The application starts when a patient has a heart disease and continuously sends his information body state in order to ensure high-quality medical treatment. Our proposed model holds the exchange of patient sensitive information between the medical staff.

Figure 6 shows the model of distributed heart disease mobile application. We handled the case where a cardiologist receives the Blood test result normally and there are no malicious attacks. Thus, we illustrated this use case by modeling the interactions between different healthcare elements (medical laboratory and cardiologist) using our secure proxy. The figure clarifies the indispensable steps to ensure sensitive information, communication among VMs as well as the three integrated policies.

```
Repeat
   Ask the user identifier and their secret key of current session
   If secure proxy finds the user identifier and their secret key are correct then
      New virtual machine is allocated in the cloud host;
   else
      Increase the probability of unauthorized access session;
   If probability of unauthorized access session greater than the first probability threshold then
      Set the user in a  medium authorization access category (i.e. orange trust level);
   If probability of unauthorized access session greater than the second probability threshold then
      Set the user in a third authorization access level (i.e. red trust level);
    If probability of unauthorized access session greater than the third probability threshold then
      Insert the user in a black list and deny the status of the user;
Until (the status of the user is denied or out of sessions time)
 If the status is denied then
    Send notification to the hypervisor
    Stopped all the user VM's machines
    Stopped all communication channels of each VM's machines of the user
    Send notifications to other mobile users
 End If
```

Figure 4 Secure hypervisor policy

```
Repeat
   Ask the target virtual machine identifier and its communication key
   If secure proxy finds the virtual machine identifier and its communication key are correct then
      Establish new communication channel among VMs and start providing data
  else
      Increase probability of unauthorized communication;
   If probability of unauthorized communication greater than the first probability threshold then
      Set the VM in a  medium authorization access category (i.e. orange trust level);
   If probability of unauthorized communication greater than the second probability threshold then
      Set the VM in a  low authorization access category (i.e. red trust level);
   If probability of unauthorized communication greater than the third probability threshold then
      Insert VM in a blacklist  and deny the access communication
Until (the status  of the user is denied or out of communication)
If access session denied then
    Send notification to the proxy module
    Stopped all communication channels of the target VM
    Increase the probability of unauthorized access
    If probability of unauthorized access greater than probability threshold then
      Insert the VM target in a black list and deny the status of communication channel
    End If
End If
```

Figure 5 Secure VMs communication policy

4.1Detection of unauthorized access on a healthcare case study

Figure 7 ensures the detection of unauthorized access in the cloud, according to the response of the first policy. Once the proxy detects an unauthorized access, it puts the mobile user in the proxy's blacklist and shares other users about the detected attacker.

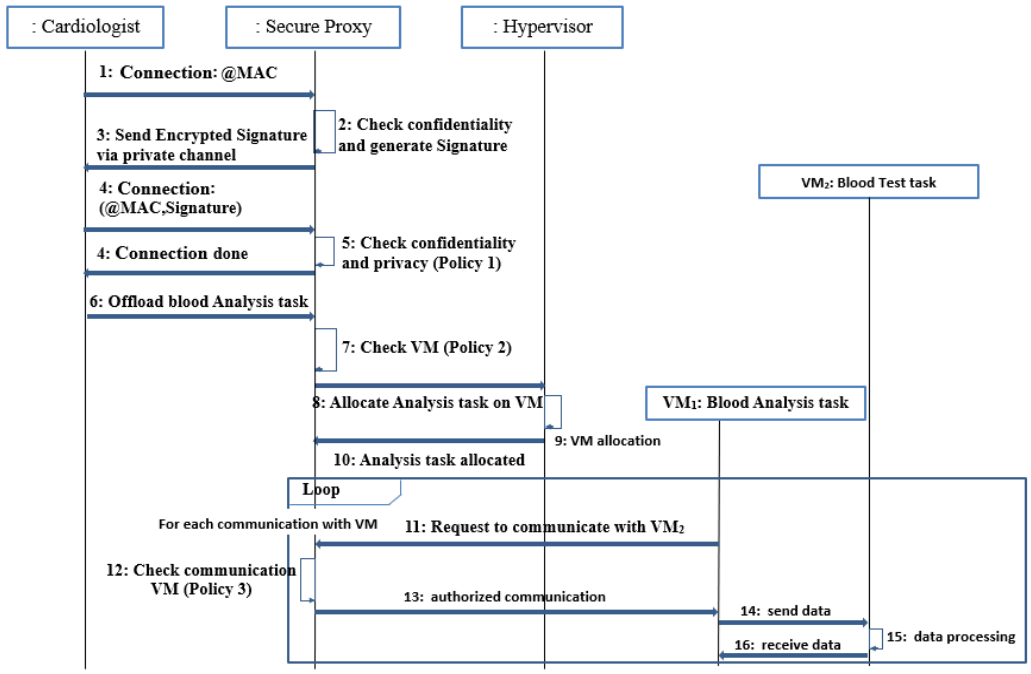

Figure 6 Applying three security-based policies on a healthcare cased study

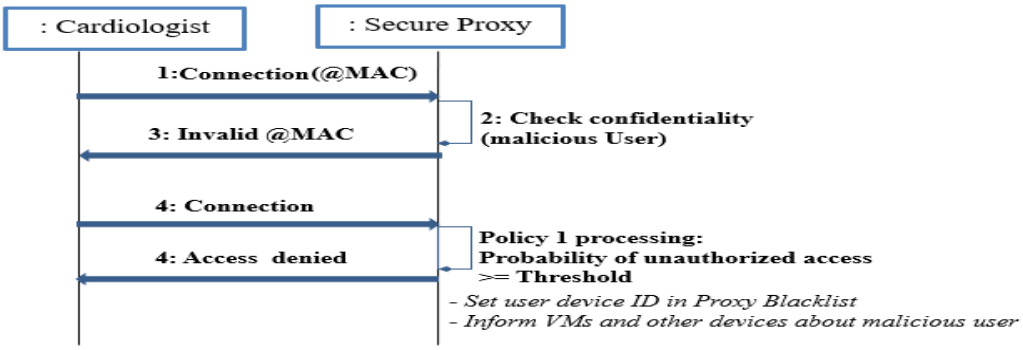

Figure 7 Detection of malicious access on a healthcare case study

4.2Detection of VMs malicious communication on the cloud

Figure 8 ensures the detection of VMs malicious communication on the cloud, according to the response of the third policy. Once the proxy detects VMs malicious communication, it puts the detected VMs in proxy's VM blacklist and informs all about detecting attacker.

5.Prototyping and evaluation

In this section, we present a practical implementation of the hash and Diffie-Hellman key exchange technique in the proposed policies: user authentication, VMs deployment and communication policies. This is improving the security isolation at the software level from external attacks. Therefore, this is very helpful to answer the required VM's data integrity of different distributed mobile applications.

Figure 9 shows the result of secure user authentication with hash Diffie-Hellman schema. The access of the mobile device to the cloud service requires the authentication process by providing the MAC address device.

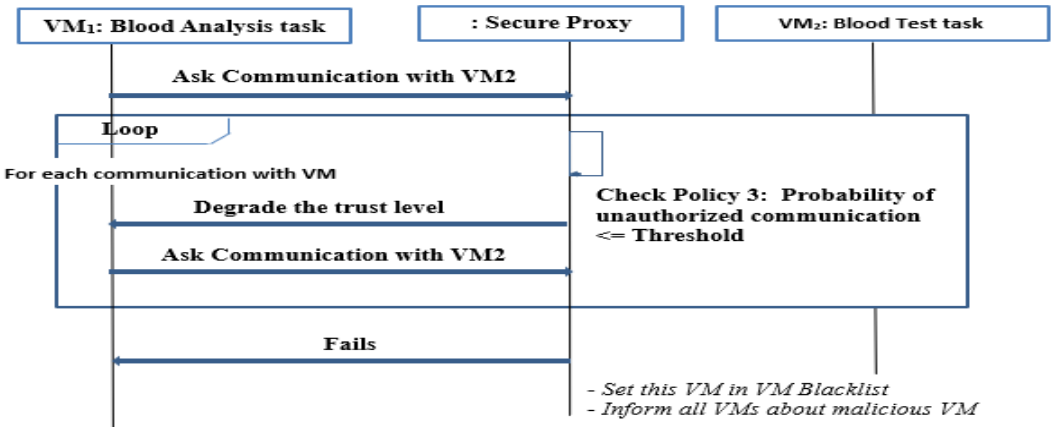

Figure 8 Detection of VM malicious communication with a healthcare case study

Line 1	User Address MAC: **1234.5628.1234.5678**
Line 2	Hash of the Mobile device MAC address:
Line 3	**949f411e20378b55b2d0bb1d17bb32b3b932bdf059ca2d2126406831cca38c72**
Line 4	Encryption step....
Line 5	Encryption signature.... [B@233c0b17
Line 6	Decryption step....
Line 7	Final result....
Line 8	**949f411e20378b55b2d0bb1d17bb32b3b932bdf059ca2d2126406831cca38c72**

Figure 9 Results of secure user authentication with hash Diffie-Hellman schema

6.Conclusion

This paper has proposed a new architecture, proxy-based with three security-based policies (i.e., co-resident attacks, hypervisor attacks and distributed attacks) to support the sensitive data protection that located on deployed VMs. A novelty in this paper was the protection of data either it is hosted on the same or different servers in order to enhance performance when ensuring the secure interaction between communicated VMs, which enabled our approach to provide high confidentiality during the exchanging of sensitive data among VMs.

The proposed approach was investigated on different techniques for generating the secret keys among the VMs while they exchange the information. The performance of the proposed approach and its resistance to cloud co-residency attacks for sensitive data was then demonstrated. Experimental results had shown that the proposed method was robust to a set of malicious attacks while maintaining accurate attack identification. Future enhancements to this work involve, reducing the complexity of our approach for easy use and practical to integrate it on current cloud platforms.

Acknowledgment

This research is funded by the Fundamental Research Grant Scheme (14174). The authors would like to thank the Ministry of Education Malaysia and Universiti Utara Malaysia for supporting and funding this research.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] 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.

[2] Zhou B, Buyya R. Augmentation techniques for mobile cloud computing: a taxonomy, survey, and future directions. ACM Computing Surveys (CSUR). 2018; 51(1).

[3] Vaezi M, Zhang Y. Cloud mobile networks. Springer; 2017.

[4] Ristenpart T, Tromer E, Shacham H, Savage S. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In proceedings of the 16th ACM conference on computer and communications security 2009 (pp. 199-212). ACM.

[5] Sgandurra D, Lupu E. Evolution of attacks, threat models, and solutions for virtualized systems. ACM Computing Surveys (CSUR). 2016; 48(3).
[6] Zhang J, Zheng L, Gong L, Gu Z. A survey on security of cloud environment: threats, solutions, and innovation. In third international conference on data science in cyberspace (DSC) 2018 (pp. 910-6). IEEE.
[7] Wang Z, Lee RB. New cache designs for thwarting software cache-based side channel attacks. ACM SIGARCH Computer Architecture News. 2007; 35(2):494-505.
[8] Wang Z, Lee RB. Covert and side channels due to processor architecture. In 22nd annual computer security applications conference (ACSAC'06) 2006 (pp. 473-82). IEEE.
[9] Aviram A, Hu S, Ford B, Gummadi R. Determinating timing channels in compute clouds. In proceedings of the ACM workshop on cloud computing security workshop 2010 (pp. 103-8). ACM.
[10] Vattikonda BC, Das S, Shacham H. Eliminating fine grained timers in Xen. In proceedings of the 3rd ACM workshop on cloud computing security workshop 2011 (pp. 41-6). ACM.
[11] Wu J, Ding L, Lin Y, Min-Allah N, Wang Y. Xenpump: a new method to mitigate timing channel in cloud computing. In fifth international conference on cloud computing 2012 (pp. 678-85). IEEE.
[12] 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. 2017; 14(1):95-108.
[13] Idrissi H, Ennahbaoui M, Souidi EM, Hajji SE. Mobile agents with cryptographic traces for intrusion detection in the cloud computing. Procedia Computer Science. 2015; 73:179-86.
[14] Zhang Y, Li M, Bai K, Yu M, Zang W. Incentive compatible moving target defense against VM-colocation attacks in clouds. In IFIP international information security conference 2012 (pp. 388-99). Springer, Berlin, Heidelberg.
[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] Ferretti L, Marchetti M, Andreolini M, Colajanni M. A symmetric cryptographic scheme for data integrity verification in cloud databases. Information Sciences. 2018; 422:497-515.
[17] Hu F, Qiu M, Li J, Grant T, Taylor D, McCaleb S, Butler L, Hamner R. A review on cloud computing: design challenges in architecture and security. Journal of Computing and Information Technology. 2011; 19(1):25-55.
[18] Islam MM, Razzaque MA, Hassan MM, Ismail WN, Song B. Mobile cloud-based big healthcare data processing in smart cities. IEEE Access. 2017; 5:11887-99.
[19] Sahoo J, Mohapatra S, Lath R. Virtualization: a survey on concepts, taxonomy and associated security issues. In second international conference on computer and network technology 2010 (pp. 222-6). IEEE.
[20] Shi J, Song X, Chen H, Zang B. Limiting cache-based side-channel in multi-tenant cloud using dynamic page coloring. In IEEE/IFIP 41st international conference on dependable systems and networks workshops (DSN-W) 2011 (pp. 194-9). IEEE.
[21] Han Y, Chan J, Alpcan T, Leckie C. Virtual machine allocation policies against co-resident attacks in cloud computing. In international conference on communications (ICC) 2014 (pp. 786-92). IEEE.
[22] Bates A, Mood B, Pletcher J, Pruse H, Valafar M, Butler K. Detecting co-residency with active traffic analysis techniques. In proceedings of the ACM workshop on cloud computing security workshop 2012 (pp. 1-12). ACM.
[23] Yu S, Xiaolin G, Jiancai L, Xuejun Z, Junfei W. Detecting VMS co-residency in cloud: using cache-based side channel attacks. Elektronika ir Elektrotechnika. 2013; 19(5):73-8.
[24] Sundareswaran S, Squcciarini AC. Detecting malicious co-resident virtual machines indulging in load-based attacks. In international conference on information and communications security 2013 (pp. 113-24). Springer, Cham.
[25] Yu S, Gui X, Lin J. An approach with two-stage mode to detect cache-based side channel attacks. In the international conference on information networking (ICOIN) 2013(pp. 186-91). IEEE.
[26] Azar Y, Kamara S, Menache I, Raykova M, Shepard FB. Co-location-resistant clouds. CCSW. 2014; 14:9-20.
[27] Annane B, Ghazali O. Virtualization-based security techniques on mobile cloud computing: research gaps and challenges. International Journal of Interactive Mobile Technologies. 2019; 13(4):20-32.

Boubakeur Annane received his bachelor degree in Computer Science in 2011 from Ferhat Abbas Setif-1 University, Setif, Algeria, and his Master in Fundamental Computer Science in 2014 from Kasdi Merbah Ouargla University, Ouargla, Algeria. Currently, he is a Ph.D. student in School of Computing, Universiti Utara Malaysia, Malaysia. He is a member of the InterNetworks Research Laboratory. He is also a member of the IEEE Computer Society. His research interests are Mobile Cloud Computing, Cloud Computing, Data Security and Privacy, Virtualization, Network and Distributed System Security.
Email: annane_boubakeur@ahsgs.uum.edu.my

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

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 Post-Doc at the 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, Pervasive 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 Ph.D. and Master Students. Dr. Alti has published a number of books' chapters, and articles for international journals and conferences. He is a member of IEEE Computer Society.
Email: alti.adel@univ-setif.dz

View publication stats