ISSN 2394-739X

International Journal for Research in Science Engineering and Technology

A PROTOCOL FOR PREVENTING INSIDER ATTACKS IN UNTRUSTED INFRASTRUCTURE-AS-A-SERVICE CLOUDS

[1] F. LYNDA-DE-JASON ME
[1] DR. M. NITYA M.E, PH.D..,
[1] COMPUTER SCIENCE AND ENGINEERING
[1] VMKV ENGINEERING COLLEGE

ABSTRACT: Recent technical advances in utility computing have allowed small and medium sized businesses to move their applications to the cloud, to benefit from features such as auto-scaling and pay-as-you-go facilities. Before clouds are widely adopted, there is a need to address privacy concerns of customer data outsourced to these platforms. In this paper, we present practical approach for protecting the confidentiality and integrity of client data and computation from insider attacks such as cloud clients as well as from the Infrastructure-as-a-Service (IaaS) based cloud system administrator himself. We demonstrate scenario of how the origin integrity and authenticity of health-care multimedia content processed on the cloud can be verified using digital watermarking in an isolated environment without revealing the watermark details to the cloud administrator. Finally to verify that our protocol does not compromise confidentiality and integrity of the client data and computation or degrade performance, we have tested a prototype system using two different approaches. Formal verification using ProVerif tool shows that cryptographic operations and protocol communication cannot be compromised using a realistic attacker model. Performance analysis of our implementation demonstrates that it adds negligible overhead.

1. INTRODUCTION

CLOUD Computing is an exciting and promising new paradigm that allows clients to outsource storage and computational resources on demand. While cloud computing bases on current technologies such as virtualization and service oriented architecture, the major driving factors of this technology are the advancement in machine architecture, the requirement to process and/or maintain large data sets and high bandwidth network channels. Additionally, features such as multi-tenancy, auto-scaling and low cost enable cloud computing to flourish more successfully than its predecessor- the Grid. One third of the IT company respondents in a recent cloud computing survey, stated that they are already using cloud based services. An additional 40% companies are in a transitionary phase towards adopting cloud based services. Recently iCloud has played the role of a crime fighter, serving to track down the iPhone of a passenger which was stolen on a cruise ship. In this work, our focus is on the Infrastructure as a Service (IaaS) based cloud model. As IaaS resides at the lowest level, it allows the development of verifiable security solutions and then layer the software stack on top of it.

Companies are adopting cloud based IT solutions as public clouds become the source of a rich and novel range of IT solutions ranging from massive online collaborative content storage to health-care workflow management systems. At the converse, the wide adoption of cloud based services is badly suffering due to confidentiality and security concerns especially from insider attacks. One way to ensure confidentiality in the cloud environment is to constantly store customer data in encrypted form and decrypt it on the cloud platform on the fly when being retrieved or being operated on. However this approach is not practical due to its high computational cost and in case of a untrusted cloud platform the confidentiality of the data can be compromised at the point the data is decrypted for computation. Researchers have proposed homomorphic encryption schemes, that allow computations to be carried out on encrypted content, producing an encrypted result which, when decrypted, matches the result of operations performed on the plaintext. However so far only primitive operations are supported and there is a large amount of overhead. Moreover there is a strong requirement to make the operations of the IaaS based cloud transparent to clients. That means that clients be able to verify the underlying cloud platform and services, to ensure that the platform owner is not compromising the integrity and confidentiality of their data and computation. In current research work, on cloud platforms security has predominantly focused either on protecting these platforms from malicious cloud clients or on protecting cloud clients from each other's unwanted activities. The problem of protecting clients from the possible malicious acts of insiders such as cloud providers is not adequately addressed. There are organizations, for instance health-care and military, which are hesitant to move to cloud based services due to confidentiality concerns. Therefore practical solutions in this direction are required for wide adoption of cloud based services. In this paper, we propose an approach to ensure the confidentiality and integrity of client data and computation on the cloud platform. This is to ensure that private data is not exposed to internal parties such as the cloud administrator and other cloud clients. Our approach makes use of remote attestation, and a late launch based technique, called Flicker, to verify the integrity of the cloud platform. This technique secures the virtual machine (VM) launch operation and further allows the launched VM to perform operations on sensitive data in full isolation. To test our approach, we have implemented a prototype by extending a popular open source cloud computing solution known as Eucalyptus. The extra integrity verification processing overhead of our approach is found to be minimal. To illustrate the practicality of our proposed protocol, we have demonstrated how it can be used to verify presence of a hidden watermark in a health-care multimedia context. This is done in a manner that preserves the confidentiality of the watermark contents and the integrity of the verification process.

The contribution of our work is as follows:

We propose a protocol for secure launch of a client VM on a trusted cloud node. Other than secure launch, our second proposed protocol enables a client to protect the confidentiality and integrity of its data and computation from other client applications in the cloud and from the cloud system administrator.

In our proposed protocol architecture, the Trusted Computing Base (TCB) is reduced to the size requirement of the Flicker based code executed and its input and output. The software stack from the BIOS up to the virtual machine monitor (VMM) level is thus removed from the suggested TCB of client sensitive code executed on the cloud platform.

In a virtualized cloud environment, past system configuration cannot guarantee current or future trustworthiness of a system. We have shown how to provide assurance to clients in such an environment. We have verified the confidentiality and integrity security properties of our proposed protocols using the

ProVerif automatic cryptographic protocol verifier. We have also verified that our proposed protocols are secure against man-in-the-middle attacks.

2. LITERATURE REVIEW

Computation outsourcing is one of the largest possibilities that the cloud enables. Clients with limited resources can utilize any necessary computing resources to outsource large-scale computations to the cloud. Despite the benefits of cloud computing, protection of the customers' confidential data is a major concern. This work deals with secure outsourcing of linear computations into the cloud and also solving it securely. Using the direct methods like Gaussian Elimination to large-scale linear computations is very expensive. Therefore, iterative method such as the Jacobi method is used to solve these linear equations, which is easier to implement. This method enables customers to find successive approximations to the linear equation solution iteratively and securely, where the sensitive input and output of the computation are kept private. For the method of detecting a malicious server, an efficient result verification mechanism is proposed.

We present a flexible architecture for trusted computing, called Terra, that allows applications with a wide range of security requirements to run simultaneously on commodity hardware. Applications on Terra enjoy the semantics of running on a separate, dedicated, tamper-resistant hardware platform, while retaining the ability to run side-by-side with normal applications on a general-purpose computing platform. Terra achieves this synthesis by use of a *trusted virtual machine monitor* (TVMM) that partitions a tamper-resistant hardware platform into multiple, isolated virtual machines (VM), providing the appearance of multiple boxes on a single, general-purpose platform. To each VM, the TVMM provides the semantics of either an "open box," i.e. a general-purpose hardware platform like today's PCs and workstations, or a "closed box," an opaque special-purpose platform that protects the privacy and integrity of its contents like today's game consoles and cellular phones. The software stack in each VM can be tailored from the hardware interface up to meet the security requirements of its application(s). The hardware and TVMM can act as a trusted party to allow closed-box VMs to cryptographically identify the software they run, i.e. what is in the box, to remote parties. We explore the strengths and limitations of this architecture by describing our prototype implementation and several applications that we developed for it.

Eucalyptus, Open Nebula and Nimbus are three major open-source cloud-computing software platforms. The overall function of these systems is to manage the provisioning of virtual machines for a cloud providing infrastructure-as-a-service. These various open-source projects provide an important alternative for those who do not wish to use a commercially provided cloud. We provide a comparison and analysis of each of these systems. We begin with a short summary comparing the current raw feature set of these projects. After that, we deepen our analysis by describing how these cloud management frameworks relate to the many other software components required to create a functioning cloud computing system. We also analyse the overall structure of each of these projects and address how the differing features and implementations reflect the different goals of each of these projects. Lastly, we discuss some of the common challenges that emerge in setting up any of these frameworks and suggest avenues Of further research and development. These include the problem of fair scheduling in absence of money, eviction or preemption, the difficulties of network configuration, and the frequent lack of clean abstractions.

Cloud computing has emerged as a popular model in computing world to support processing large volumetric data using clusters of commodity computers. It is the latest effort in delivering computing resources as a service. It is used to describe both a platform and a type of application. A cloud computing platform dynamically provisions, configures, and deprivations servers as needed. Cloud computing also describes applications that are extended to be accessible through the Internet. Data security and access control is one of the most challenging ongoing research work in cloud computing, because of users outsourcing their sensitive data to cloud providers. Existing solutions that use pure cryptographic techniques to mitigate these security and access control problems suffer from heavy computational overhead on the data owner as well as the cloud service provider for key distribution and management. This paper addresses this challenging open problem using capability based access control technique that ensures only valid users will access the outsourced data. This work also proposes a modified Diffie-Hellman key exchange protocol between cloud service provider and the user for secretly sharing a symmetric key for secure data access that alleviates the problem of key distribution and management at cloud service provider. The simulation run and analysis shows that the proposed approach is highly efficient and secure under existing security models.

3. EXISTING SYSTEM

In our existing system, One way to ensure confidentiality in the cloud environment is to constantly store customer data in encrypted form and decrypt it on the cloud platform on the fly when being retrieved or being operated on. However this approach is not practical due to its high computational cost and in case of a untrusted cloud platform the confidentiality of the data can be compromised at the point the data is decrypted for computation. Researchers have proposed homomorphism encryption schemes, that allow computations to be carried out on encrypted content, producing an encrypted result which, when decrypted, matches the result of operations performed on the plaintext. However so far only primitive operations are supported and there is a large amount of overhead. Moreover there is a strong requirement to make the operations of the IaaS based cloud transparent to clients. That means that clients be able to verify the underlying cloud platform and services, to ensure that the platform owner is not compromising the integrity and confidentiality of their data and computation. In current research work on cloud platforms security has predominantly focused either on protecting these platforms from malicious cloud clients or on protecting cloud clients from each other's unwanted activities. The problem of protecting clients from the possible malicious acts of insiders such as cloud providers is not adequately addressed. There are organizations, for instance health-care and military, which are hesitant to move to cloud based services due to confidentiality concerns. Therefore practical solutions in this direction are required for wide adoption of cloud based services.

4. PROPOSED SYSTEM

In our proposed system, we propose a protocol for secure launch of a client VM on a trusted cloud node. Other than secure launch, our second proposed protocol enables a client to protect the confidentiality and integrity of its data and computation from other client applications in the cloud and from the cloud system administrator. In our proposed protocol architecture, the Trusted Computing Base (TCB) is reduced to the size requirement of the Flicker based code executed and its input and output. The software stack from the BIOS up to the virtual machine monitor(VMM) level is thus removed from the suggested TCB of client sensitive code executed on the cloud platform. In a virtualized cloud environment, past system configuration cannot guarantee current or future trustworthiness of a system. We have shown how to provide assurance to clients in such an environment. We have verified the confidentiality and integrity security properties of our proposed protocols using the Prove if automatic cryptographic protocol verifier. We have also verified that our proposed protocols are secure against man-in-the-middle attacks.

5. MODULE

- Cloud group formation
- Trusted platform module
- Remote attestation
- Prove if cryptographic protocol

Cloud Group Construction

In This module, we allocate Identity numbers to each and every user while registering into our group. In that we can collect information regarding the users present in the group. We can also send and receive files from the user in our group or individual. An individual or group entity, which owns its data stored in the cloud for online data storage and computing. Different users may be affiliated with a common organization, and are assigned with independent authorities on certain data fields.

Trusted platform module

In this module, a secure storage area where cryptographic keys and other secure data can be stored. The key and data stored inside the TPM is protected from malicious alteration. The data stored inside the TPM normally includes platform configuration status. The platform status stored inside TPM can then be provided to external entities, through a process called Remote Attestation, to convey platform trustworthiness. The Trusted Computing Base (TCB)of a system is the collection of all hardware, firmware, and/or software modules that are vital for the security of the overall system. Any vulnerabilities occurring inside the TCB can compromise the security of the entire system.

Remote Attestation

In this module, remote attestation, the platform (firmware and software) configuration is captured and stored in a tamper resistant and cost effective chip called a TPM. Confidential information is held inside the TPM and is then signed and reported to a remote entity for verification and attestation purposes. store platform integrity in the form of hashes of loaded software in data registers called Platform Configuration Registers (PCRs). Quote operation is used to attest the values of TPM PCRs.TPM Quote comprises of a subset of PCRs values together with a nonce all signed by a TPM Endorsement Key (EK). The private part of the EK is used for signing purposes during Quote generation and is used to convince remote verifiers that assertions in the TPM Quote have been signed by a trusted TPM.

Proverif Cryptographic Protocol

In this module, the client first verifies the platform configuration before launching his VM in the cloud. After VM launch, the client computation on normal data is performed as usual in the cloud environment. However, when the client wants some computation on highly sensitive data then it cannot simply rely only on Level I security. As the client has previously verified cloud platform during VM launch then according to Level I security it can trust the platform for sensitive computation as well. However, the problem is that the cloud system administrator can run an arbitrary process in domo after initial verification and hence can compromise client confidentiality and integrity. Therefore, we propose Level II security whereby computation on client sensitive data is performed in full isolation from the cloud system administrator. Such assurance is achieved through our proposed approach based on late launch and the Intel Trusted execution Technology (TXT) hardware based mechanism, Flicker.

CONCLUSION

In the last few years, cloud computing has experienced very high growth rates and is showing great prospects. One of the biggest challenges to the wide adoption of cloud based services is client confidentiality and integrity concerns. In this paper, we have presented and formally verified a practical solution to address this problem. Our solution includes a protocol for secure VM launch which enables clients to verify cloud platform configuration before launching their VMs on the cloud. In addition, a protocol for performing sensitive computations in a cloud environment is presented. We have formally verified the security properties of our proposed protocols using ProVerif. Currently our implementation is for Intel based systems but it can easily be adapted to AMD. Evaluation results show that our solution is practical in terms of performance. In the future, we are planning to perform rigorous penetration testing of our protocol using an actual deployment.

REFERENCES

[1]. N. Kroes. “Setting up the European Cloud Partnership”. World Economic Forum, 2012.

[2]. M. Naehrig, K. Lauter, and V. Vaikuntanathan. “Can homomorphic encryption be practical?”. In Proceedings of the 3rd ACM workshop on Cloud computing security workshop, pp. 113-124, New York, USA, 2011.

[3]. Advanced Micro Devices. AMD64 virtualization: Secure virtual machine architecture reference manual. AMD Publication no. 33047 rev. 3.01, May 2005.

[4]. G. Coker, J. Guttman, P. Loscocco, A. Herzog, J. Millen, B. OHanlon, J. Ramsdell, A. Segall, J. Sheehy, and B. Sniffen. “Principles of remote attestation”. International Journal of Information Security, Volume 10, Issue 2, pp. 63-81, 2011.

[5]. X. Lei, X. Liao, T. Huang, H. Li and C. Hu. “Outsourcing Large Matrix Inversion Computation to A Public Cloud”. IEEE Transactions on Cloud Computing, Volume 1, Issue 2, pp. 78-89, 2013.

[6]. Trusted-Java: Jsr321: Trusted computing api for java(tm) (2009) Available at: http://jcp.org/en/jsr/detail?id=321. Accessed on 06/09/2013.

[7]. P. Tysowski and M. Hasan. “Hybrid Attribute- and Re-Encryption- Based Key Management for Secure and Scalable Mobile Applications in Clouds”. IEEE Transactions on Cloud Computing, Volume 1, Issue 2, pp. 172-186, 2013.

[8]. S. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi and P. Samarati.“ Integrity for Join Queries in the Cloud”. IEEE Transactions on Cloud Computing, Volume 1, Issue 2, pp. 187-200, 2013.

[9]. X. Leroy. “Formal certification of a compiler back-end, or: programming a compiler with a proof assistant”. In 33RD Proceedings of ACM Symposium on Principles of Programming Languages, 2006.

[10]. F. Krautheim, D. Phatak, and A. Sherman. “Introducing the trusted virtual environment module: a new mechanism for rooting trust in cloud computing”. In Proceedings of the 3rd international conference on Trust and trustworthy computing, 2010.