Enhanced Keyword Search for Encrypted Data Files Guarantees in Public Infrastructure Clouds

[1] N. Jyoshna, [2] Dr. M. Rudra Kumar

[1] M.Tech.,(PG Scholar), [2]Professor & Head of the Department
[1]Dept of CSE, [2]Dept of CSE,
[1] Dept of CSE,Annamacharya Institute Of Technology & Sciences, Rajampet, Kadapa,
[2] Dept of CSE,Annamacharya Institute Of Technology & Sciences, Rajampet, Kadapa,

Abstract : In this paper, we describe a framework for data and operation security in IaaS, consisting of protocols fortrusted launch of virtual machines and domain-based storage protection. The protocols allow trust to be established byremotely attesting host platform configuration prior to launching guest virtual machines and ensure confidentiality ofdata in remote storage, with encryption keys maintained outside of the IaaS domain. The protocols allow trust to beestablished by remotely attesting host platform configuration prior to launching guest virtual machines and ensureconfidentiality of data in remote storage, with encryption keys maintained outside of the IaaS domain. Presentedexperimental results demonstrate the validity and efficiency of the proposed protocols. The framework prototype wasimplemented on a test bed operating a public electronic health record system, showing that the proposed protocols canbe integrated into existing cloud environments.

IndexTerms **- Mobile ad hoc networks, query processing, routing, traffic, data replacement attack, node grouping**

1. INTRODUCTION

Cloud computing has progressed from a bold vision to massive deployments in various application domains. However the complexity of technology underlying cloud computing introduces novel security risks and challenges. A core enabling technology of IaaS is system virtualization [8], which enables hardware multiplexing and redefinition of supported hardware architectures into software abstractions. This redefinition is performed by the hypervisor, a software componentthat abstracts the hardware resources of the platform and presents a virtualized software platform Where guest virtual machine (VM) instances can be deployed. In addition, the hypervisor also manages the I/Ocommunication between VM instances and external components, including storage devices allocated to the VMinstance. This is one of thevulnerable areas of IaaS environments since, as demonstrated in [6], improper allocationofblock storage can lead to a breach of data confidentiality. There is a clear need for usable and cost-effective cloudplatform security mechanisms suitable for organizations that rely on cloud infrastructure. One such mechanism is platform integrity verification for compute hosts that support the virtualized cloud infrastructure several large cloud vendors have signalled practical implementations of this mechanism, primarily to protect the cloud infrastructure from insider threats and advanced persistent threats. We see two major improvement vectors regarding these implementations. First, details of such proprietarysolutions are not disclosed and can thus not be implementedand improved by othercloud platforms. Second,to the best of our knowledge, none of the solutions providecloud tenants a proof regarding theintegrity of computehosts supporting their slice of the cloud infrastructure.In this project, we present DBSP (domain-based storage protection), a virtualdisk encryption mechanismwhere encryption of data is done directly on the compute host, while the key material necessary for re-generatingencryption keys is stored in the volume metadata. This approach allows easy migration of encrypted data volumes andwithdraws the control of the cloud provider over disk encryption keys. In addition, DBSP significantly reduces the riskof exposing encryption keys and keeps a low maintenance overhead for the tenant– in the same time providingadditional control over the choice of the compute host based on its software stack.The relevant security mechanism is encryption of virtual disk volumes, implemented and enforced atcomputehost level. While support data encryption at rest is offered by several cloud providers and can be configured by tenantsin their VM instances, functionality and migration capabilities of such solutions are severely restricted. In mostcases cloud providers maintain and manage the keys necessary for encryption and decryption of data at rest. Thisfurther convolutes the already complex data migration procedure between different cloud providers, disadvantagingtenants through a new variation of vendor lock-in. Tenants can choose to encrypt data on the operating system (OS)level within their VM environments and manage the encryption keys themselves. Cloud computing offers an important techniquethat is platform integrity verification that support thevirtualized cloud infrastructure for hosts. Many of the cloudvendors have assembled and the judicious implementations ofthis mechanism. Cloud storage provides us with convenient,huge, and scalable storage at low cost, but data privacy is amajor problem that prevents users from storing files on thecloud trust worthy. One way to improve privacy from dataowner point of view is to encrypt the files before storing themonto the cloud and decrypt the files after downloading them.To safeguard the cloud infrastructure from corporateexecutive threats and advanced persistent threats, we tend tosee a vast improvement vectors pertaining theseimplementations. Secondly, to the most effective of ourinformation, none of the solutions provides cloud tenants asymbol concerning the integrity of figure hosts supporting their way of looking forward towards the cloud infrastructure.

II LITERATURE SURVEY

The infrastructure cloud (IaaS) service model offers tenantswith a improved assets flexibility and availability, wherethey are encased from the trivial details of hardwaremaintenance, rent computing resources to be utilized andoperate complex systems. Many organizations work ondelicate data to avoid relocation and replication ofoperations to IaaS platforms due to defense concerns. In thispaper we use Order-preserving encryption (OBP) to achieveefficiency and security of data stored in a cloud, we also useanother techniques like auditing protocols and third partyassistance for the key management updates into a cloud bywhich the accessing becomes easier and the security isguaranteed and the violation of the data decreases. Theindustry has invested for strict security and they

suggest best practices [5].The main aim of this project is to through light on IaaS. It is in its simplified form, and exposes to its users that it is coherent platform as it supports the hosts ofclouds who operates VM guests can communicate by a virtual network by providing the basic requirements that are identified when an deployment of Distributed Electronic Health Record (EHR) system for an IaaS computing platform. In these years for IaaS the threats and migration has been under the intensive security [1][2][3]. At first, details of such principal solutions are not closed totally and may there fore not be enforced and enhanced by alternative cloud platforms[3].

Nuno Santos Krishna P. Gummadi Rodrigo Rodrigues.[6]given a mechanism reliably detects whether or not the host is running a platform implementation that the remote partytrusts. These platforms will effectively secure a VM runningin a single host. Antonis Michalas, Nicolae Paladi andChristian Gehrmann.[7] aimed for a paperless medicalsystem where patients and doctors are able to bookappointments via the Internet, create electronicprescriptions and store their medical history in a centraldatabase, easily accessible from anyone with appropriateaccess rights. Patrick McDaniel, Kevin ButlerRadu Sion, ErezZadok, Kui Ren and Marianne Winslett.[8] There are longstandingconcerns beginning in large-scale systems. A recentreport ready for the chairman and ranking member of thesenate Committee on independent agency andenvironmental Affairs [8] highlighted beginning united of 3key future technologies for securing our national crucialinfrastructure.

Towards trusted cloud computing

The design of atrusted cloud computing platform (TCCP). TCCP enables Infrastructure as a Service (IaaS) providerssuch as Amazon EC2 to provide a closed box execution environment that guarantees confidential execution ofguestvirtual machines. Moreover, it allows users to attest to the IaaS provider and determine whether or not the serviceis secure before they launch their virtual machines [1].

Seeding Clouds with Trust Anchors

In this paper, we identify three main challenges that cloud providers face when generating proofs that can placate a user's concerns:

1) That cloud vendors provide a proof of data security protection of their hosts and customer processing; 2) That such proofs have a clear meaning to cloud customers; and
3) That such proofs can be generated effectively and efficiently in a cloud computing environment [2].

Domain Based Storage Protection with Secure Access Control for the Cloud

Despite the variety of available open source cloud management platforms (e.g. Open Stack, Eucalyptus, Open Nebula), allocation of read-write permissions for shared data between collaborating tenants still remains an open problem. In this paper we address the outlined gap. We improve and extendprevious work by adding capabilities to both grant access to data to other IaaS cloud clients and assign access permissions [3].

Security aspects of e-health systems migration to the cloud
In this paper, we will present current state of the art research in this field. We focused of several shortcomingscurrent healthcare solutions and standards, particularly for platform security, privacy aspect and requirements which is a crucial aspect for the overall security of healthcare IT systems. [5]

A decentralized approach to integrity attestation is adoptedby Schiffman et al. [2] to address the limited transparency ofIaaS platforms and scalability limits imposed by third partyintegrity attestation mechanisms. The authors describe atrusted architecture where tenants verify the integrity ofIaaS hosts through a trusted cloud verifier proxy placed inthe cloud provider domain. Tenants evaluate the cloudverifier integrity, which in turn attests the hosts. Once theVM image has been verified by the host and countersignedby the cloud verifier, the tenant can allow the launch. Ourprotocol maintains the VM launch traceability andtransparency without relying on a proxy verifier residing inthe IaaS. Furthermore, the TL protocol does not requireadditional tenant interaction to launch the VM on a trustedhost, beyond the initial launch arguments.Platform attestation prior to VM launch is also applied in[7], which introduces two protocols – "TPM-basedcertification of a Remote Resource" (TCRR) and "VerifyMy VM". With TCRR a tenant can verify the integrity of aremote host and establish a trusted channel for furthercommunication. In "Verify My VM", the hypervisorrunning on an attested host uses an emulated TPM to verifyon-demand the integrity of running VMs. Our approach is inmany aspects similar to the one in [7] in particular withregard to host attestation prior to VM instance launch. Weovercome this limitation and generalize the solution byadding a verification token, created by the tenant and injected on the file system of the VM instance only if it is launched on an attested cloud host.
In [8], the authors described a protocol for trusted VM launch on public IaaS using trusted computing techniques.

To ensure that the requested VM instance is launched on ahost with attested integrity, the tenant encrypts the VMimage (along with all injected data) with a symmetric keysealed to a particular configuration of the host reflected inthe values of the platform configuration registers (PCR) ofthe TPM placed on the host. The proposed solution issuitable in trusted VM launch scenarios for enterprisetenants as it requires that the VM image is pre-packaged and encrypted by the client prior to IaaS launch. However,similar to [7], this prevents tenants from using commodityVM images offered by the cloud provider to launch VMinstances on trusted cloud hosts. Furthermore, we believethat reducing the number of steps required from the tenantcan facilitate the adoption of the trusted IaaS model. Weextend some of the ideas proposed in [8], address the abovelimitations – such as additional actions required fromtenants – and also address the requirements towards thelaunched VM instance and required changes to cloud platforms.

III. Proposed Model

When providers are offering security enhancements suchas protection of data at rest, end-users have limited or nocontrol over such mechanisms. There is a clear need forusable and cost-effective cloud platform securitymechanisms suitable or organizations that rely on cloudinfrastructure. Traditional public auditing protocols, anotherimportant task of the Third-party assistance (TPA) is tocheck the integrity of the client's files stored in cloud. TheTPA does not know the real secret key of the client forIn this proposed system a "Trusted Cloud Compute Platform"(TCCP) to ensure VMs are running on a trustedhardware and software stack on a remote and initially un-trusted host. To enable this, a trusted coordinator storesthe list of attested hosts that run a "trusted virtual machine monitor" which can securely run the client's VM.Trusted hosts maintain in memory an individual trusted key use for identification each time a client launches aVM. The paper presents a good initial set of ideas for trusted VM launch and migration, in particular the use of atrusted coordinator. A limitation of this solution is that the trustedcoordinator maintains information about all hostsdeployed onwhile support data encryption at rest is offered by several cloud providers and can be configured by tenantsin their VM instances, functionality and migration capabilities of such solutions are severely restricted. In most casescloud providers maintain and manage the keys necessary for encryption and decryption of data at rest. This furtherconvolutes the already complex data migration procedure between different cloud providers, disadvantaging tenantsthrough a new variation of vendor lock-in. Tenants can choose to encrypt data on the operating system (OS) levelwithin their VM environments and manage the encryption keys themselves. However, this approach suffers fromseveral drawbacks: first, the underlying compute host will still have access encryption keys whenever the VM performscryptographic operations; second, this shifts towards the tenant the burden of maintaining the encryption software in alltheir VM instances and increases the attack surface; third, this requires injecting, migrating and later securelywithdrawing encryption keys to each of the VM instances with access to the encrypted data, increasing the probabilitythan an attacker eventually obtains the keyProposed system presents experimental results todemonstrate the validity and efficiency of the proposedprotocols to overcome the drawbacks of existing system. Abasic structure underlying a system, concept, prototype isimplemented on a transparent and replicable testing ofscientific theories, computational tools, and newtechnologies, operating a public electronic health recordsystem, showing that the proposed protocols can beintegrated into existing cloud environments. Threats andmitigation is another technique where its Blinding techniquewith homomorphic property to form the encryptionalgorithm to encrypt the secret keys held by the TPA. Itmakes our protocol secure and the decryption operationefficient. Meanwhile, the TPA can complete key.

IV METHODOLOGY

We now describe two protocols that constitute the core of this papers contribution. These protocols are successively applied to deploy a cloud infrastructure providing additional user guarantees of cloud host integrity and storage security. For protocol purposes, each domain manager, secure component and trusted third party has a public/private key pair (pk/sk).

The private key is kept secret, while the public key is shared with the community. We assume that during the initialization phase, each entity obtains a certificate via a trusted certification authority. We first describe the cryptographic primitives used in the proposed protocols, followed by definitions of the main protocol components.
Cryptographic Primitives The set of all binary strings of length n is denoted by{0,1}n, and the set of all finite binary strings as ,0,1-∗ . Given a set U, we refer to the ith element as vi. Additionally, we use the following notations for cryptographic operations throughout the paper:

Protocol Components Disk encryption subsystem:

a software or hardware component for data I/O encryption on storage devices, capable to encrypt storage units such as hard drives, software RAID volumes, partitions, files, etc. We assume a softwarebased subsystem, such as dm-crypt, a disk encryption subsystem using the Linux kernel Crypto API. 4.3 Trusted Launch Construction We now present our construction for the TL, with four participating entities: domain manager, secure component, trusted third party and cloud provider (with the „scheduler" as part of it). TL comprises a public-key encryption scheme, a signature scheme and a token generator.

We now analyse the TL and DBSP protocols in the presence of an adversary. We prove the security of both schemes 4 Key retrieval is currently not covered in the security analysis due to space limitations through a theoretical analysis, showing that our protocols are resistant to the attacks presented in Section

Option a can only succeed if ADV can break the mutual authentication in the secure channel setting. Given that the selected secure channel scheme is sound and τ is sufficiently long and selected using a sound random generation process, the ADV fails to break the last protocol step. Hence, as long as the secure channel protocol is sound, the overall protocol construction is also sound against this attack option. Option b can only succeed if the adversary either managestoguessavalueτ0 = τ when launching vm or manages to either obtain τ when DMi launches vmi l or replace the association between τ and vmi l with an association between τ and vm when DMi launches vmi l, by attacking any of the protocol steps preceding the final mutual authentication step. A successful attack in this case has the probability τ0 = τ equals to 1/2n, where n is the length of the token value and is infeasible if n is large enough. Below, we show why the adversary also fails with respect to the last option. 6. IMPLEMENTATION AND RESULTS We next describe the implementation of the TL and DBSP protocols followed by experimental evaluation results.

Test bed Architecture We describe the infrastructure of the prototype and the architecture of a distributed EHR system installed and configured over multiple VM instances running on the test bed.

Performance evaluation DBSP Processing time: Table 1 shows a breakdown of the time required to process a storage unlock request, an average of 10 executions. Processing a volume unlock request on the prototype returns in≈2.714 seconds; however, this operation is performed only when attaching the volume to a VM instance and does not affect the subsequent I/O operations on the volume. A closer view highlights the share of the contributing components in the overall overhead composition. Table 1 clearly shows that the TPM unseal operation lasts on average ≈2.7 seconds, or 99.516% of the execution time. According to Section

In this prototype we use TPMs v1.2, since a TPM v2.0 is not available on commodity platforms at the time of writing. Given that the vast majority of the execution time is spent in the TPM unseal operation, implementing the protocol with a TPM v2.0 may yield improved results.

V. CONCLUSION

In this paper, we have proposed an system architecture about providing user security guarantees in public infrastructure clouds and single keyword search scheme tosearch the encrypted data files efficient and also the data security over the cloud. However, some extensions are still possible of our current work remaining. In future, We wouldlike to propose a multi-keyword search scheme as our OPEalgorithm is a simple one, another extension is to find apowerful algorithm which will not harm the efficiency. The cloud security model does not yet hold against threat models developed for the traditional model where the hostsare operated and used bythe same organization. However, there is a steady progress towards strengthening the IaaSsecurity model. In thiswork we presented a framework for trusted infrastructure cloud deployment, with two focuspoints: VM deploymenton trusted compute hosts and domain-based protection ofstored data. We described in detail thedesign, implementation and security evaluation of protocols for trusted VM launch and domain-based storageprotection. The solutionsare based on requirements elicited by a public healthcareauthority, have been implemented ina popular open-sourceIaaS platform and tested on a prototype deployment of adistributed EHR system. In the securityanalysis, we introduceda series of attacks and proved that the protocols holdin the specified threat model.This work hascovered only a fraction of the IaaS attack landscape. The additional concept is also implementing attribute based file sharing system.

REFERENCE

[1] N. Santos, K. P. Gummadi, and R. Rodrigues, “Towards trustedcloud computing,” in Proceedings of the 2009 Conference on HotTopics in Cloud Computing, HotCloud’09, (Berkeley, CA, USA),USENIX Association, 2009.

[2] J. Schiffman, T. Moyer, H. Vijayakumar, T. Jaeger, and P. McDaniel,“Seeding Clouds With Trust Anchors,” in Proceedings of the 2010ACM Workshop on Cloud Computing Security, CCSW ’10, (NewYork, NY, USA), pp. 43–46, ACM, 2010.

[3] N. Paladi, A. Michalas, and C. Gehrmann, “Domain based storage protection with secure access control for the cloud,” in Proceedingsof the 2014 International Workshop on Security in Cloud Computing,ASIACCS ’14, (New York, NY, USA), ACM, 2014.

[4] M. Jordon, “Cleaning up dirty disks in the cloud,” Network Security,vol. 2012, no. 10, pp. 12–15, 2012.

[5] Cloud Security Alliance, “The notorious nine cloud computing topthreats 2013,” February 2013.

[6] A. Michalas, N. Paladi, and C. Gehrmann, “Security aspects ofe-health systems migration to the cloud,” in the 16th InternationalConference on Ehealth Networking, Application & Services (Healthcom’14), pp. 228–232, IEEE, Oct 2014.

[7] B. Bertholon, S. Varrette, and P. Bouvry, “Certicloud: a novel tpm based approach to ensure cloud IaaS security,” in Cloud Computing, 2011 IEEE International Conference on, pp. 121–130, IEEE, 2011.

[8] M. Aslam, C. Gehrmann, L. Rasmussen, and M. Bj ¨orkman, “Securely launching virtual machines on trustworthy platforms in apublic cloud – an enterprise’s perspective.,” in CLOSER, pp. 511–521, SciTePress, 2012.

[9] A. Cooper and A. Martin, “Towards a secure, tamper-proof gridplatform,” in Cluster Computing and the Grid, 2006. CCGRID 06.Sixth IEEE International Symposium on, vol. 1, pp. 8–pp, IEEE, 2006.

[10] W. Wang, Z. Li, R. Owens, and B. Bhargava, “Secure and efficientaccess to outsourced data,” in Proceedings of the 2009 ACM workshopon Cloud computing security, pp. 55–66, ACM, 2009.

[11] D. Song, E. Shi, I. Fischer, and U. Shankar, “Cloud data protectionfor the masses,” IEEE Computer, vol. 45, no. 1, pp. 39–45, 2012.