International Journal of Research in Advent Technology, Vol.7, No.4S, April 2019
E-ISSN: 2321-9637
Available online at www.ijrat.org

Hybrid Data Centric Solution to Cloud Privacy and Security Issues faced in Cloud Computing

Tanaya Ganguly
Assistant Professor, Parul University, Gujrat
tanayaganguly1a@gmail.com

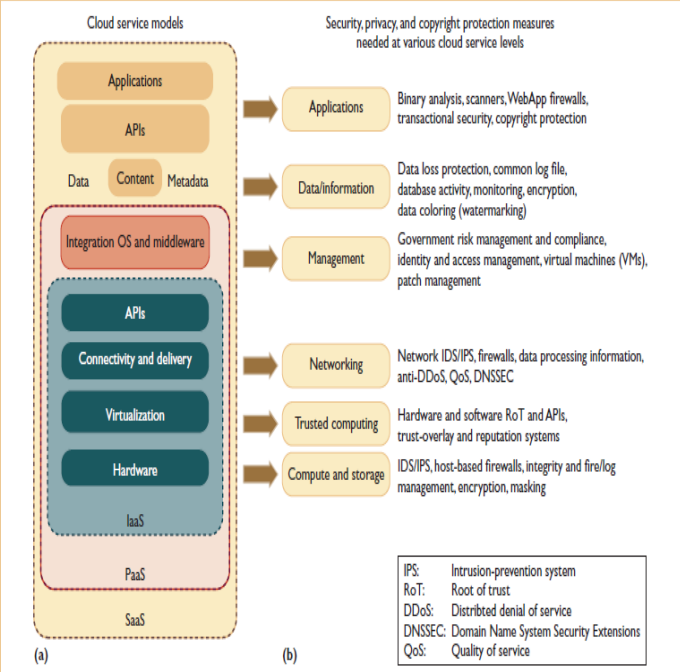
Abstract: The recent transition to \cloud computing" is changing the way people store and usedigital data. Data is more often stored remotely (on a cloud server) and accessed byvery weak devices over the internet (e.g. smartphones). In addition to storage, thecloud is expected to manipulate and process the data per the user's requests, since localprocessing on the end user's device is infeasible. This allows for great exibility in theuse of data, but also means new challenges for data privacy. To answer these challenges, we need to add new tools to our cryptographic toolbox.We want to store our data in the cloud in an encrypted form, for privacy purposes,but still want the cloud to process the data for us. We need a fast local decryptionsolution that can be executed securely in the presence of side channel attacks. We needto store cryptographic keys in a secure manner to utilize cloud services securely, whichnecessitates the ability to encrypt the cryptographic keys themselves.

Keywords: Cloud Computing, Denial-of-Service (DoS) Attack, Network Security, AuthenticationProtocol.

1. INTRODUCTION

Cloud computing enables a new business model that supports on-demand, pay-for-use, and economies-of-scale IT services over the Internet. The Internet cloud works as a service factory built around virtualized data centers.1 Cloud platforms are dynamically built through virtualization with provisioned hardware, software, networks, and datasets. The idea is to migrate desktop computing to a service-oriented platform using virtual server clusters at data centers. However, a lack of trust between cloud users and providers has hindered the universal acceptance of clouds as outsourced computing services. To promote multitenancy, we must design the cloud ecosystem to be secure, trustworthy, and dependable [1].

In reality, trust is a social problem, not a purely technical issue. However, we believe that technology can enhance trust, justice, reputation, credibility, and assurance in Internet applications. To increase the adoption of Web and cloud services, *cloud service providers* (CSPs) must first establish trust and security to alleviate the worries of a large number of users. A healthy cloud ecosystem should be free from abuses, violence, cheating, hacking, viruses, rumors, pornography, spam, and privacy and copyright violations. Both public and private clouds demand “trusted zones” for data, *virtual machines* (VMs), and user identity, as VMware and EMC3 originally introduced.



2. COMPARISONS WITH OTHER TECHNOLOGIES

Cloud users are most concerned about whether data-center owners will abuse the system by randomly using private datasets or releasing sensitive data to a third party without authorization. Cloud security hinges on how to establish trust between these service providers and data owners. To address these issues, we propose a reputation-based trust-management scheme augmented with data coloring and software watermarking.

Information about related trust models is available elsewhere

Cloud Computing vs. Utility Computing

In utility computing, software and hardware resources are concentrated in large data centers, andusers pay per use for storage and communication services.

Similarities: There are many similarities between utility computing and cloud computing.Utility computing often requires a cloud-like infrastructure, but its focus is on the business modelfor providing computing services. Utility computing involves a straightforward rental offacilities to users (so they are in full control of these facilities).

Differences: In contrast, in cloud computing users still pay for what they use but the serviceutilization is much more complex in terms of infrastructure and software. The facilities arecontrolled by the cloud owners and managers.

Cloud Computing vs. Grid Computing

Grid computing is a network with distributed resources, which can divide and farm out pieceshardware and software facilities to a great number of users, and may be owned by diverseorganizations (unlike a cloud owned by a single owner). Users are obliged to provide theirhardware and software to other users on a schedule managed by the grid managers.

Similarities: Cloud computing has several similarities with grid computing. Theoretically, theconcept behind both models is to group up various computing resources together and share theircapabilities in a scalable form in order to accomplish one or more complex tasks that are difficultor even impossible to accomplish with one single resource [2]. The computing resources of gridcomputing may include processing cycles, memory disk spaces, networks, printers, scanners,software licenses, remote devices, etc. Grid computing is commonly used for academic andscientific purposes to process computationally intensive tasks faster and cheaper [17].

In a business model, every client negotiates with the providers for its use of grid resources byproviding a detailed proposal for the scope of his research study and anticipated amount ofnecessary resources [18]. The aim of development of grid computing was to facilitate users toremotely utilize idle computing power within other computing centers when the local one is busyor unable to perform the task alone.

Differences: Grid resources are generally free for using the computing resources but insteadmust agree to avail their own computing resources to be used by others at any time needed [19].

In contrast, cloud computing is commercially offered by providers for public use at anaffordable cost for organizations that are unable or unwilling (possibly due to economic factors)to develop and manage their own computing solutions [20].

From a technical perspective, the purpose of grid computing is to integrate resources fromvarious organizations forming a uniform resource pool which can provide the computing abilitythat is impossible to be achieved by a single computing center [18]. These organizations aredistributed geographically and have their own rights in determining vendors of their resources.

The aim of cloud computing is to divide resources into small pieces and deliver them to users according to their preferences.

3. CRYPTOGRAPHIC MECHANISMS IN CLOUDS

Modern cryptography provide much more flexible decryption mechanisms, and explicitly allow malleability on ciphertexts, namely search over encrypted data, Proofs of DataPossession (PDP) and Proofs of data Retrievability (PoR). These promoting approachesare greatly interesting in a multi-tenant cloud environment. PDP and PoR concepts willbe investigated.

Identity Based Cryptography

In 1984, ID-Based Cryptography (IBC) was introduced by Shamir [Sha85] with theoriginal idea to provide public and private key pairs with no need for certificates and CAdeployment. Shamir assumes that each entity uses one of its identifiers as its public key.These identifiers have to be unique. In addition, he assigns the private key generation functionto a special entity called the Private Key Generator (PKG). That is, before accessingthe network, every entity has to contact the PKG to get its private key. This private keyis computed so as to be bound to the public key of the entity. During the last decade,

IBC has been enhanced by the use of the Elliptic Curve Cryptography (ECC) [HMV03].As a consequence, new ID-based encryption and signature schemes emerged. These newschemes differ from Shamir approach relying on smart cards to store the private keys ofusers and the ciphering information.In 2001, Boneh and Franklin [BF01] proposed the first ID-based encryption scheme, relying on the use of bilinear pairing functions to bind elliptic curve points to a number of amultiplicative group.We note that certificates may be considered as an identity based feature, as they map theuser's public key to his identity. In this dissertation, we focus on identity based schemes

Issues, challenges and concerns

We identified a number of issues in the literature relating to technological and legalchallenges confronting privacy, security and trust posed by cloud computing. Regardingthe challenges in the technological underpinnings of cloud computing, we note evidence stemming from: virtualisation (e.g. vulnerabilities in hypervisors could have potentialwidespread effects on data integrity and confidentiality); whether grid computing modelscan afford the appropriate level of interoperability ; if Web Services will be effective foridentity management in the cloud; establishing trust when using Service OrientatedArchitectures and web application frameworks and finally whether current technicalmethods of encryption will remain viable to achieve confidentiality. There are a number ofchallenges posed by a range of legal and regulatory frameworks relevant to cloudcomputing. These include the viability of legal regimes which impose obligations based onthe location of data; the ex-ante definition of different entities (such as distinguishingbetween data controllers and processors); establishing consent of the data subject; theeffectiveness of breach notification rules; the effectiveness of cyber-crime legislation indeterring and sanctioning cyber-crime in the cloud and finally difficulties in determiningapplicable law and jurisdiction. From an operational perspective, the study uncoveredissues relating to the effectiveness of existing risk governance frameworks, whether cloudcustomers can meet their legal obligations when data or applications are hosted overseas,how to be compliant and accountable when incidents occur; whether data will be lockedinto specific providers; the complexities in performing audit and investigations; how toestablish the appropriate level of transparency and finally measuring security of cloudservice provision.

The case studies identified a number of challenges relating to cloud service provision fromrecent real-world instances. These include the immature and exploratory nature of cloudcomputing deployments; the necessity that those using cloud services should be versed intheir tolerance for risk prior to migrating to the cloud; how to balance the business benefitsof cloud computing with achieving security and privacy obligations; the need to integratecloud security into existing security measures; the importance of understanding untowarddependencies created by cloud computing deployments and finally that tailored andspecific security agreements can be achieved but only if the cloud user has sufficientnegotiating power.

These identified real-world concerns were supplemented by additional material gathered atan Expert Workshop. Participants commented that it was difficult to achieve a highdegree of accountability or transparency in the cloud; that there was little awareness raisingfor either cloud customers or private citizens; little established guidance on expectations forcloud users in meeting their legal obligations and finally lack of harmonisation of relevant legal and regulatory frameworks, potentially presenting an impediment to realising the economic and social benefits of cloud computing for Europe.

4. CRYPTOGRAPHY IN CLOUD DATA STORAGE ENVIRONMENTS

The public key is computationally derived from the user identity. This public key isgenerally considered as the output of hash function that takes as input the identity of theuser.In the following sections, we first present the pairing functions that were widely usedin modern cryptographic systems, thanks to its interesting properties.Then, we introduce the key generation process for ID-based schemes, which are based onpairing functions.

C. Security Issues Faced By Cloud Computing

Cloud allows users to achieve the power of computing which beats their own physical domain. It leads to manysecurity problems. The cloud service provider for cloud makes sure that the customer does not face any problem such asloss of data or data theft. Cloud computing infrastructures use new technologies and services, most which haven't beenfully evaluated with respect to security. There is also a possibility where a malicious user can penetrate the cloud byimpersonating a legitimate user, there by infecting the entire cloud. This leads to affects many customers who are sharingthe infected cloud. The security issues faced by cloud computing are discussed below.

1. Data Access Control: Sometimes confidential data can be illegally accessed due to lack of secured data accesscontrol. Sensitive data in a cloud computing environment emerge as major issues with regard to security in a cloudbased system. Data exists for a long time in a cloud, the higher the risk of unauthorized access [10].

2. Data Integrity: Data integrity comprises the following cases, when some human errors occurs when data is entered.Errors may occur when data is transmitted from one computer to another , otherwise error can occur from somehardware malfunctions, such as disk crashes. Software bugs or viruses can also make viruses. So at the same time,many cloud computing service consumer and provider accesses and modify data. Thus there is a need of some dataintegrity method in cloud computing.

3. Data Theft: Cloud computing uses external data server for cost affective and flexible for operation. So there is achance of data can be stolen from the external server.
4. Data Loss: Data loss is a very serious problem in Cloud computing. If banking and business transactions, researchand development ideas are all taking place online, unauthorized people will be able to access the information shared.Even if everything is secure what if a server goes down or crashes or attacked by a virus, the whole system would godown and possible data loss may occur. If the vendor closes due to financial or legal problems there will be a loss ofdata for the customers. The customers won't be able to access those data's because data is no more available for thecustomer as the vendor shut down.
5. Data Location: Consumers do not always know the location of their data. The Vendor does not reveal where all thedata's are stored. Cloud Computing offers a high degree of data mobility. The Data'swon't even be in the samecountry of the Customer, it might be located anywhere in the world. They may also wish to specify a preferredlocation (e.g. data to be kept in the USA) then requires a contractual agreement between the Cloud service providerand the consumer that data should stay in a particular location or reside on a given known server [11].

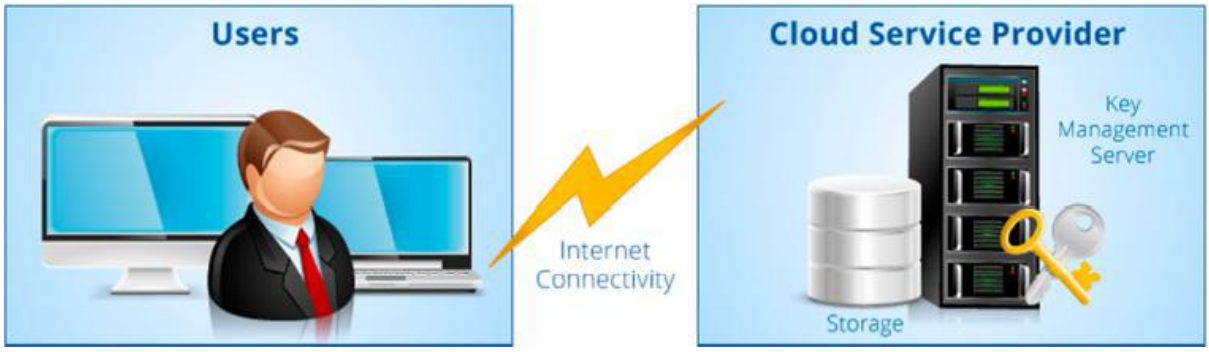


Figure 1: Cloud key management service

A Data Centric Solution to Cloud Privacy and Security Issues:
This section describes the proposed solution that addresses the main researchquestions of this study. The proposed solution is based on the Data Centric Security(DCS) approach discussed in previous section. The aim of this chapter is to develop asolution that makes an original research contribution to the DCS concept which isbelieved to be an adequate approach to address privacy and security issues in cloudcomputing. The solution is designed to satisfy the following desired requirements forapplications in a cloud computing environment:

- The data are encrypted and can be accessed by authorized users only.
- The data are searchable without compromising their privacy.
- The data are self-protected and contain the required security parameters.
- The access control parameters are hidden from cloud server providers andother users.
- The server provider does not know the number or the identity of users whoare authorized to access the data.
- Unauthorized entities, including service providers, cannot gain access to thedata or derive information about the data from authorized operations carriedout on the data.
- The data contain all the necessary information for proving their integrity andauthenticity to the authorized users who access the data.
- Interactions between owners and authorized users should be minimal,especially for key management purposes.

These requirements are specified by a set of modules each one of which specifies atleast one of the requirements. All parameters required for accomplishing the securityfunctions are attached to the data file and the result is a file called a DCS file. Thesecurity functions include privacy protection as well as integrity and authenticityverifications. This chapter starts with a background description about the ChineseRemainder Theorem (CRT) which is the core algorithm used in the proposedsolution. Then, Section describes the module that is used to provide and manageparameters required for access control and key sharing using the CRT.

Enhancing Keys and Files Security
In terms of enhancing security in the proposed solution, a data owner must use aunique symmetric key, Ks, to encrypt each file before sending it for storing in thecloud. According to the DCS approach, all the security requirements are attached

tothe actual data hence each symmetric key is attached to its file in a secure manner.From Equation (4.3), the symmetric key Ks is protected by two levels: first byencrypting it with an authorized user, then by the CRT to find the shared value Xr.Only authorized users can calculate the Ks from the Xr using Equation (4.4) which required the related ni and private key of an authorized user.

5. FRAMEWORK IMPLEMENTATION

Implementation Design

This section presents the prototype design of the privacy monitoring framework in the form of Unified Modeling Language (UML), the modelling language for software design. This design details the use case diagram, activity diagram, class diagram and entity relationship diagram.

Theoretical Performance Analysis

In this section, we present a theoretical performance analysis, while taking into consideration computation, communication and storage costs.

Computation Cost Evaluation

On the basis of the requirements of a data possession proofsystem, we choose four different PDP schemes ([ABC+07,DVW09,SW08,EKPT09]), thatare most closely-related to our context.

On the server side, SHoPS distributes the processing overhead over the multiple storingnodes. The cloud gate computes only i multiplications, where i is the number of therequested nodes, in an aggregated proof. Therefore, contrary to the other approaches,SHoPS achieves a O(logn) server computation complexity.

On the verifier side, we brought additional computation cost, in order to perform a publicverifiability. That is, the public verification procedure can also be performed by authorizedchallengers without the participation of the data owner. As such, this concern can behandled in practical scenarios, compared to private schemes ([DVW09,EKPT09]) whichhave to centralize all verification tasks to the data owner. In our scheme, the authorizedverifier has to generate two random scalars c 2]0;R[and k 2 [1; q], in order to conducthis challenge request. Then, he checks the received proof from the cloud server, whileperforming three pairing computations, regardless the number of data blocks. Thus, thepublic verifiability introduces a O(nlogn) processing cost at the verifier side.

6. CONCLUSION

The common issue and challenge for cloud computing is the security of the cloud environment, many different approaches and models have already been proposed by many researchers. Cloud services providers are now searching for the proper security and privacy mechanisms which would make the cloud atmosphere safe and protected place for their customers and they keep full faith on the cloud service provider. This paper survey the cryptographic storage technology in cloud computing the techniques, the benefits and drawbacks.

REFERENCE

[1] Bijeta Seth, SurjeetDalal, Addressing Security in Cloud Federation: A Review, International Journal of Research in Electronics and Computer Engineering (IJRECE), Vol. 6 Issue 3, July - September 2018, pp. 1746-1755

[2] Dac-Nhuong Le, Bijeta Seth, SurjeetDalal, A Hybrid Approach of Secret Sharing with Fragmentation and Encryption in Cloud Environment for Securing Outsourced Medical Database: A Revolutionary Approach, Journal of Cyber Security and Mobility, Vol. 7, Issue 4, pp. 379-408, 2018

[3] M. Shoaib, H. Garudadri, Digital pacer detection in diagnostic grade ecg, e-HealthNetworking Applications and Services (Healthcom), 2011 13th IEEE InternationalConference on, IEEE, 2011, pp. 326–331.

[4] H. Alemdar, C. Ersoy, Wireless sensor networks for healthcare: a survey, Comput.Networks 54 (15) (2010) 2688–2710.

[5] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee,D. Patterson, A. Rabkin, I. Stoica, et al., A view of cloud computing, Commun. ACM53 (4) (2010) 50–58.

[6] M.-R. Ra, R. Govindan, A. Ortega, P3: toward privacy-preserving photo sharing,NSDI, (2013), pp. 515–528.

[7] L. Zhang, T. Jung, P. Feng, K. Liu, X.Y. Li, Y. Liu, Pic: enable large-scale privacypreserving content-based image search on cloud, IEEE Trans. Parallel Distrib. Syst.PP (99) (2017), http://dx.doi.org/10.1109/TPDS.2017.2712148 . 1–1

[8] L. Zhang, K. Liu, X.Y. Li, C. Liu, X. Ding, Y. Liu, Privacy-friendly photo capturingand sharing system, ACM International Joint Conference on Pervasive andUbiquitous Computing, (2016), pp. 524–534.

[9] Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, K. Ren, A privacy-preserving and copydeterrencecontent-based image retrieval scheme in cloud computing, IEEE Trans.Inf. Forensics Secur. 11 (11) (2017) 2594–2608.

[10] D.L. Donoho, Compressed sensing, Inf. Theory, IEEE Trans. 52 (4) (2006)1289–1306.

[11] N. Zhou, H. Li, D. Wang, S. Pan, Z. Zhou, Image compression and encryption schemebased on 2d compressive sensing and fractional mellin transform, Opt. Commun.343 (2015) 10–21.
[12] C. Wang, B. Zhang, K. Ren, J.M. Roveda, Privacy-assured outsourcing of imagereconstruction service in cloud, IEEE Trans. Emerg. Top Comput. 1 (1) (2013)166–177.
[13] C. Wang, B. Zhang, K. Ren, J.M. Roveda, C.W. Chen, Z. Xu, A privacy-aware cloudassistedhealthcare monitoring system via compressive sensing, INFOCOM, 2014Proceedings IEEE, IEEE, 2014, pp. 2130–2138.
[14] W. Chen, X. Chen, C.J. Sheppard, Optical image encryption based on diffractiveimaging, Opt. Lett. 35 (22) (2010) 3817–3819.
[15] Z. Liu, L. Xu, C. Lin, J. Dai, S. Liu, Image encryption scheme by using iterativerandom phase encoding in gyrator transform domains, Opt. Lasers Eng. 49 (4)(2011) 542–546.
[16] Y. Wang, K.-W. Wong, X. Liao, G. Chen, A new chaos-based fast image encryptionalgorithm, Appl. Soft Comput. 11 (1) (2011) 514–522.
[17] R.B. Candès E J, Exact matrix completion via convex optimization, Found. Comput.Math. 9 (6) (2009) 717–772.
[18] Y.-C. Chen, L. Qiu, Y. Zhang, G. Xue, Z. Hu, Robust network compressive sensing,Proceedings of the 20th Annual International Conference on Mobile Computing andNetworking, ACM, 2014, pp. 545–556.
[19] Y. Zhang, M. Roughan, W. Willinger, L. Qiu, Spatio-temporal compressive sensingand internet traffic matrices, ACM SIGCOMM Computer Communication Review,39 ACM, 2009, pp. 267–278.