SECURITY POLICY ENFORCEMENT IN CLOUD INFRASTRUCTURE

Arijit Ukil[1], Ajanta De Sarkar[2] and Debasish Jana[3]

[1] Innovation Lab, Tata Consultancy Services, Kolkata, India
[2,3] Birla Institute of Technology, Mesra Kolkata Campus, Kolkata, India
[1] arijit.ukil@tcs.com, [2] adsarkar@bitmesra.ac.in,
[3]djana@alumni.uwaterloo.ca

ABSTRACT

Cloud computing is a computing environment consisting of different facilitating components like hardware, software, firmware, networking, and services. Internet or a private network provides the required backbone to deliver the cloud services. The benefits of cloud computing like "on-demand, customized resource availability and performance management" are overpowered by the associated security risks to the cloud system, particularly to the cloud users or clients. Existing traditional IT and enterprise security are not adequate to address the cloud security issues. In order to deploy different cloud applications, it is understood that security concerns of cloud computing are to be effectively addressed. Cloud security is such an area which deals with the concerns and vulnerabilities of cloud computing for ensuring safer computing environment. This paper explores the challenges and issues of security concerns of cloud computing through different standard and novel solutions. This paper proposes architecture for incorporating different security schemes, techniques and protocols for cloud computing, particularly in Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) systems. The proposed architecture is generic in nature, not dependent on the type of cloud deployment, application agnostic and is not coupled with the underlying backbone. This would facilitate to manage the cloud system more effectively and provide the administrator to include the specific solution to counter the threat.

KEYWORDS

Cloud computing; security; PaaS; IaaS; authentication.

1. INTRODUCTION

Cloud computing provides a distributed computing environment comprising of heterogeneous facilitating components like hardware, software, firmware, networking as well as services. Challenges arise when access through the cloud infrastructure is done from a public domain like internet. Even when privately held, security challenges prevail. Internet or even a private network provides the required backbone to deliver the cloud services. Common cloud services are: IaaS, PaaS, and Software-as-a-Service (SaaS), and may include other overlayed services on top of these basic service models. The model of metered usage of infrastructure, application, data and services bring about economy of scale, reduced computing and storage cost. However, without adequate assessment of the capability, benefit, vulnerability and optimality, cloud computing may pose severe challenges and threats, which can transform the immense advantages to massive risk and catastrophic loss. The unorthodox architecture and operation of cloud operation bring in different security and privacy vulnerabilities. Cloud security helps in delivering the resilience for different attacks to disrupt the confidentiality, integrity and availability of cloud information and user data.

David C. Wyld (Eds) : ICCSEA, SPPR, CSIA, WimoA - 2013
pp. 01–09, 2013. © CS & IT-CSCP 2013 DOI : 10.5121/csit.2013.3501

It is worthy to find trustworthiness of cloud service providers based on some parameters like system update frequency, mean down time, previous attack history [1].

In this paper, we explore the above-mentioned challenges and issues of security concerns of cloud computing through different standard and novel solutions. Our discussion on cloud security is independent of the type of cloud deployment. We propose a security-enabled cloud environment which significantly protects client's interest and security concerns over its data based on user or application's requirement, which helps in mitigating the scalability issues.

This paper is organized as follows. In Section 2, related work done by several researchers is documented. In Section 3, we discuss about the security in cloud infrastructure, its key issues and open challenges. Section 4 depicts proposed architecture for implementing cloud system security, and the Security-as-a-Service in a cloud system. Finally, In Section 5 we conclude the paper citing our future work.

2. RELATED WORK

Conner et al [1] have presented an effective reputation management system with associated trust establishment through multiple scoring functions and implemented the security service on a realistic application scenario in distributed environments. Privacy issue in cloud computing is dealt in [2]. In [3], a nice scheme for handling data protection in terms of confidentiality through amalgamation of identity management with hierarchical identity-based cryptography is described. Trust needs to be established means for better security of cloud platforms. In [14], trust and reputation based scheme in collaborative computing is presented. With this backdrop, we present our proposed architecture and security model towards better protection of confidentiality, privacy in a public cloud infrastructure.

3. SECURITY IN CLOUD COMPUTING

Security is a big challenge in cloud system due to its nature of outsourced computing. Mainly, confidentiality, integrity and authentication are the primary pain areas. Unless robust security scheme and user-centric security policy is implemented, cloud system would be vulnerable to susceptible to different attacks.

3.1 Key Issues

Confidentiality prevents intentional (malicious) or unintentional disclosure of sensitive information. In cloud systems, confidentiality incorporates data encryption to minimize vulnerability due to covert channels, traffic analysis, and sensitive inference. In, [3] federated identity management in the cloud is described. For guaranteeing data integrity at rest or storage, particularly in IaaS and PaaS systems, trusted infrastructure [8] needs to be incorporated. In fact, traditional security techniques for enterprise and home computing systems cannot address the cloud server security problems [10].

3.2 Open Challenges

One of the primary focuses to provide cloud security is to have one integrated solution enabling the required security primitives like confidentiality, authentication and integrity. In [2, 13], it is described that cloud specific security solutions like confidentiality-enabled computing, user-defined authentication and access control, atomic data integrity are the main issues to be addressed.

4. PROPOSED SECURITY MODEL AND IMPLEMENTATION ARCHITECTURE

We propose a framework for satisfying cloud security ensuring the main primitives: confidentiality, integrity and authentication (with access control). Then we integrate the individual proposals to provide an integrated cloud security which would be offered as a security service.

4.1 Confidentiality in Cloud Infrastructure

With the ownership of client's sensitive data at cloud service provider, it becomes highly unlikely to protect data from the respective service provider while there are well-established techniques available to resist the external threats [2, 5]. One of the solutions is to introduce the concept of data analysis and processing at the provider without the content of client's data gets revealed. Client's data needs to be processed and analysed in original or raw form at the cloud to enable meaningful applications. This defeats the confidentiality of user's data. In order to retain confidentiality as well as deriving services out of data by third party application, processing on encryption domain is required. This is termed as homomorphic encryption in [6, 7]. Suppose, cloud service provider requires to compute some arbitrary function *f* on client's (one or many in number) data d_1, … , $d_{N..}$ This can be done two ways:

- $f(d_1, d_2, ...d_N)$
- $f(E(d_1), E(d_2), ...E(d_N))$

Homomorphic encryption scheme allows to efficiently compute arbitrary functions over encrypted data i.e., given encryptions E(d_1), …, E(d_N) of d1, … , d_N for any computable function *f*. In order to ensure client data security from cloud service provider where cloud service provider needs to compute on client data, homomorphic encryption is the only available option. Though it is in developing stage and incurs high computational cost for sophisticated functions, we propose the following algorithm to balance between the security and usability:

```
                    Security-utility balancing algorithm
Begin
        Find the confidentiality requirement from client
        Repository of trust scores of the cloud service provider is
        supplied
           If the specific cloud service provider $\in$ "Blacklisted cloud
           service providers" $\vee$ "Sensitive application" (like finance
           data)
                   Use functional encryption (homomorphic encryption)
           Elseif client data $\subset$ sensitive $\wedge$ "statistical meaning is of
           importance
                   Negotiate with privacy primitives like perturbation,
                   randomization, and generalization
           Else
                   Use standard on-transit TLS/SSL encryption
 End
```

4.2 Authentication Architecture and Policy in Cloud Infrastructure

For providing identity management to warrant authentication and authorization, OpenID and OAuth standards are defined using cloud specific security and privacy policy [8]. On the other hand, XACML (eXtensible Access Control Markup Language), an OASIS-ratified, is a declarative access control policy language. XCAML is suited for policy-based access control and authorization services. A trusted third party or the cloud service provider hosts the XACML decision engine consisting of decision implementation by Policy Decision Point (PDP) and policy based enforcement by Policy Enforcement Point (PEP). In Fig. 1, we describe a simplified architecture of XACML based access control.

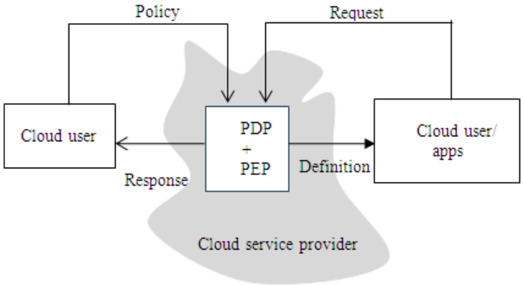

Fig. 1.Architecture of XACML based cloud authentication

The proposed protocol for XACML-based cloud authentication is described below, where we depict an activity diagram for better understanding of the protocol for XACML based cloud authentication. In this case, we consider cloud service provider as a reliable (trusted) third party.

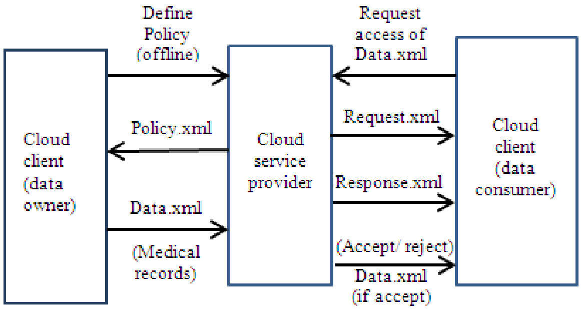

Fig. 2. XACML based cloud authentication protocol

It is to be noted that Policy.xml is a very sensitive and an important file maintaining the access and authorization policy for different applications and cloud users and should be stored in encrypted or hardware-secured method. Another important requirement is to ensure higher usability such that client users with multiple application subscription. Cloud accounts should easily access data while security is safeguarded. One of the striking usability features is to provide Single-Sign-On (SSO) based authentication so that the user can maintain only single authentication credential for accessing different applications, even different cloud service providers. Following architecture can be conceptualized as depicted in fig. 3, where a cloud user authenticates through a cloud SSO hosted by a particular cloud service provider to access other cloud apps, other (owned) cloud service provider accounts, even authorized data of other cloud user.

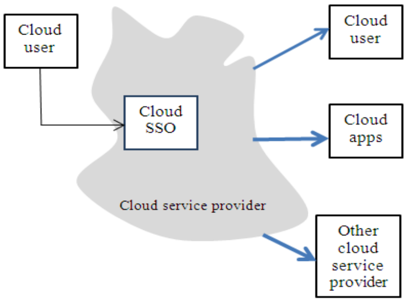

Fig. 3. SSO- based cloud authentication

4.3 Integrity Architecture in Cloud Infrastructure

Cloud service is very much prone to non-invasive side channel attacks like software attacks (malware, virus), statistical attacks (password guess) due to its distributed nature. Trusted Computing Group (TCG) is engaged in formulating a separate layer of hardware security within cloud infrastructure [10, 12]. Ensuring trusted hardware (like Trusted Platform Module) secure booting, public key based integrity checking along with frequent system validation and consequent application access control helps to build a trusted cloud platform as shown in Fig. 4. The main objective is to provide secure execution of the application by employing application access control through software and hardware level security. It can be observed that through this integrity-ensured trusted cloud, an end-to-end trust (from hardware layer to application layer) chain of trust can be established. When the client is capable of moderate processing power and transacting sensitive records like financial data, medical reports, the proposed trust establishment is necessary to ensure reliability for data at rest.

4.4 Integrated Cloud Security Architecture

To ensure the cloud ecosystem capable of handling the security aspects, discrete components for countering specific attack may not be manageable. An interesting and unique feature of cloud security is that security can be provided as a service like software, platform or infrastructure. Security-as-a-service has potential because of two reasons. The concept of security as a top-up on different applications may not suffice the requirement of cloud system. In cloud system, application developer needs to incorporate the security APIs to the application and cloud administrator has to check the required security primitives. Another important feature is to provide on-demand security like on-demand storage or on-demand computation. This means that the cloud user or cloud application based on requirement can subscribe the particular security components and thus introducing security as a service. On the other hand this feature can be handy to create an adaptive-secure cloud system, where based on applications or users context certain security primitives or APIs will be called to defend from possible threats. We envision the architecture as:

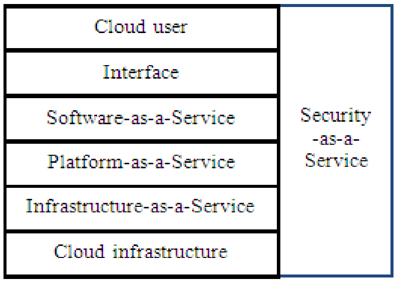

Fig 4. Conceptual cloud service model with security-as-a-service

"Security-as-a-Service" consists of different components like PaaS consists of service, compute components; IaaS consists of storage, network components. The main components of "Security-as-a-Service" are shown in Table 1. Based on the requirements, these components can be incorporated on demand basis. For example, for storage security or data at rest integrity data integrity components can be used; cloud users can negotiate with cloud service provider for homomorphic encryption such that user's data is processed in encrypted domain. In a similar way, this security primitive can be integrated in a proactive or adaptively to different rendered services for seamless protection against possible attacks. For example, when SaaS is handling request for financial transactions more security primitives (like HTTPS, XACML, digital signature) are used while handling request for chat applications, HTTPS, digital signature are not needed.

Table 1. Security-as-a-service for other cloud services and stakeholders

Services/ Stakeholders	Security primitives of Security-as-a-service
Cloud user	Homomorphic encryption, TPM
Cloud infrastructure	TPM, SSO
SaaS	OpenID, OAuth, XACML, HTTPS
PaaS	Homomorphic encryption, OpenID, OAuth, XACML
IaaS	TPM

4.5 Cloud Computing with Security-As-A-Service

Security-as-a-service, as defined earlier is to be availed as a horizontal service in a cloud service model. In this section, we describe a use case of an e-health system using security-as-a-service. There are different parties in the e-health system like medical practitioner, patient, hospital, medicine retailer, nursing staff, insurance agency, medical researcher, so on and so forth designated as $\tau = [\tau_i]$, i= medical practitioner, patient, medicine retailer, nursing staff, hospital, insurance agency, medical researcher… The e-health system is hosted in a cloud service provider C with PaaS model. We denote the sensitive medical record of the patient as D. The patient intends to share $D = [D_p, D_s]$, where p stands for public, s stands for sensitive. The cloud client with medical record (patient) D is hosted in C with following security constraints S :

1. For τ_i, where i = medical researcher, only aggregated result on D_s would be shared.
2. For τ_i, where i= medical retailer only medicine part of D_s is to be shared.
3. For τ_i, where i= nursing staff, only medicine and some related part of D_s is to be shared.
4. For τ_i, where *i*= insurance agency, cost, primary investigation and medicine part of D_s is to be shared.
5. All τ_i is to be authenticated.
6. D_s is to be stored securely in C, D_s is to be shared to τ_i through C in a secure channel, i.e. $C \xrightarrow{D_s \text{sec} ured} \tau_i$.

When the cloud client, the owner registers to the cloud C for allowing C to host D, client $\tau_{patient}$ gets registered and authenticates to C using OpenID. When $\tau_{patient}$ avails the service of e-health application, it posts its medical record D to C undersigning with the constraints S. There can be a negotiation process between $\tau_{patient}$ and C such that C accepts a subset of S. For sake of simplicity, we do not consider the negotiation phase. In fig. 5, we show the initial data hosting and constraint sharing between $\tau_{patient}$ and C.

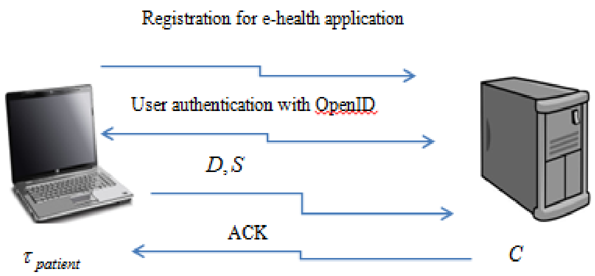
Registration for e-health application
User authentication with OpenID
D, S
ACK
$\tau_{patient}$
C

Fig 5. Registration and security-constraint sharing

After $\tau_{patient}$ registers in C, shares D and S, it is the responsibility of C to ensure the security requirements S as per when acknowledgement is made. It is to be mentioned that service and business model does also participate as the amount of D and S directly impact the pricing of rendering the service.

After $\tau_{patient}$ registers in C, shares D and S, it is the responsibility of C to ensure the security requirements S as per when acknowledgement is made. It is to be mentioned that service and business model does also participate as the amount of D and S directly impact the pricing of rendering the service.

Let us consider that medical researcher intends to avail some information from D through query function Q, which can be searching for a piece of data, aggregated result etc. So, $\tau_{medical\_researcher}$ queries C on D for Q. In order to retain secrecy, C negotiates with $\tau_{medical\_researcher}$ for homomorphic key exchange, public and private key (K_{pu}, K_{pr}) and installing homomorphic encryption agent (if already not present) on $\tau_{medical\_researcher}$. C performs homomorphic encryption on D with K_{pu} and $\tau_{medical\_researcher}$ decrypts with K_{pr}.The decrypted content is Q on D. For example, D may consist of medical investigation data of $\tau_{patient}$ and Q requires information on the investigation data that is higher than reference range. We depict the protocol in fig. 6. Our proposal is to address this issue through functional encryption. However, other cryptographic primitives can be used.

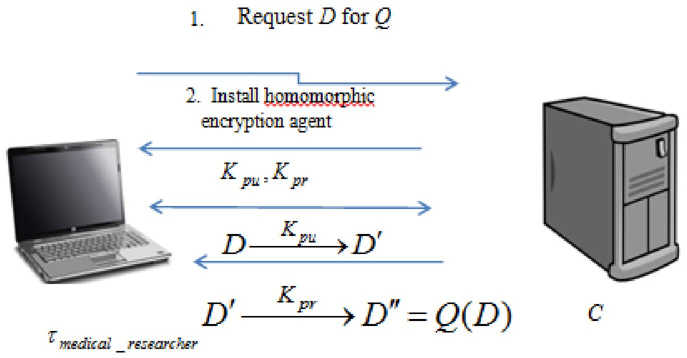
1. Request D for Q
2. Install homomorphic encryption agent
K_{pu}, K_{pr}
$D \xrightarrow{K_{pu}} D'$
$D' \xrightarrow{K_{pr}} D'' = Q(D)$
$\tau_{medical\_researcher}$
C

Fig 6. Functional confidentiality in cloud computing

In order to satisfy other constraints primitives from security-as-a-service needs to be incorporated. For example, satisfying 6 requires HTTPS channel set up among $\tau_{patient}$, D and $\tau_{medical\_researcher}$ for data sharing. For 5, OpenID and OAuth primitives need to be set up.

5. Conclusion And Future Work

In this paper, we have analyzed the problem of security in cloud computing. This paper provides security architecture and necessary support techniques for securing cloud computing infrastructure. It assumes to address following challenges to provide data confidentiality cloud users, to enable cloud information integrity and authentication. We have emphasized that the problem of network security or security of data at transit can be handled by the present state-of-the-art solution. We have provided solutions to counter these threats for securing cloud user's data when exchanged with the cloud service provider (and processed at the cloud service provider), among different cloud service providers and between other cloud users. We have proposed "Security-as-a-Service" as a horizontal service model to support the security requirements of cloud users as well as other service models like IaaS and PaaS. However, cloud security research has just started its journey and it is long way to go before ensuring full-fledged cloud security. For example, computation on encrypted data is very much essential to provide data confidentiality from cloud security provider while allowing computation. To enable such feature, homomrphic encryption [5, 6] is a good candidate. However, fully homomrphic encryption incurs high computational cost and is not feasible with existing state-of-the-art cloud hardware. There exists immense scope of research to introduce light-weight homomorphic encryption scheme.

References

1. Conner, W., Iyengar, A., Mikalsen, T.,Rouvellou, I., and Nahrstedt, K. A Trust Management Framework for Service-Oriented Environments. In *Proceedings of the WWW Conference*, 891- 900, 2009
2. Ukil, A. Security and Privacy in Wireless Sensor Networks. In *Smart Wireless Sensor Networks*, 395 – 418, 2010
3. Yan, L., Rong, C., and Zhao, G. Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based Cryptography. In *Proceedings of CloudCom*, 167–177. 2009
4. Yau, S., S., and Ho G. Protection of users' data confidentiality in cloud computing. In *Proceedings of the 2nd Asia-Pacific Symposium on Internetware*, 2010
5. Rivest, R. L., Adleman, L., and Dertouzos, M., L. On data banks and privacy homomorphisms. In *Foundations of Secure Computation*, 1978

6. Gentry, C. Fully Homomorphic Encryption Using Ideal Lattices. In *Proceedings of 41st ACM Symposium on Theory of Computing*, 169 – 178, 2009
7. Leiba, B. OAuth Web Authorization Protocol. *IEEE Internet Computing*, 16, 1, 74-77, 2012
8. Ukil, A. Secure Trust Management in Distributed Computing Systems. IEEE DELTA, Newzealand, 116 – 121, 2011
9. Ukil, A., Sen, J., and Koilakonda, S. Embedded Security for Internet of Things. In *Proceedings of 2nd IEEE National Conference on Emerging Trends and Applications in Computer Science*, 1-6, 2011
10. Van Dijk, M., Juel, A. On the impossibility of cryptography alone for privacy-preserving cloud computing. In Proceedings of *USENIX Hotsec*, 2010.
11. http://www.trustedcomputinggroup.org (accessed on 27 Aug, 2012)
12. Ukil, A.,Sen, J. Secure multiparty privacy preserving data aggregation by modular arithmetic. In Proceedings of *IEEE International Conference on Parallel Distributed and Grid Computing*, 344 – 349, 2010
13. Mather, T., Kumaraswamy, S., and Latif, S. *Cloud Security and Privacy: An Enterprise perspective of Risks and Compliance*. O'Reilly Media, Inc., 2009
14. Ukil, A. Trust and Reputation Based Collaborating Computing in Wireless Sensor Networks. In *Proceedings of IEEE International Conference on Computational Intelligence, Modelling and Simulation*, 464 – 469, 2010